Thursday, February 1. 2018

NBN And Emergency Lift Phones, Alarms, And Other Fixed Diallers

Emergency phones like those in Lifts, and Security Alarm Systems with back to base monitoring are also affected by the NBN changeover and cut-offs, therefore building owners and managers need to start considering what action they need to take, even if the NBN is not as yet active in your area, it likely wont be that far off, so you'll need to start planning for the changeover, it's also beneficial to change earlier, cheap PAYG mobile plans are more economical for standby emergency and idle telecommunications than PSTN line rental. As for Alarms, many B2B providers supply you with a SIM that includes all signal calls in your monthly B2B plan.

This process is not as daunting or expensive as it might sound, for example, with Lifts, you're not going to need lengthy and costly service calls, or have downtime to change over the panels, because the system stays the same, it's only the external part, on how it talks to the outside world, that changes. These systems are intelligent, with a lot of electronics behind them, as part of that, the system is pre programmed by the Lift company on who to call in the event of emergency call button activation. These systems usually have a phone lead from them plugged into a telecommunications outlet on a normal PSTN phone line, just like your home phone, as this example shows
In the current set up, when the call button is pressed, it automatically dials the pre determined phone number which usually is the Lift or Security company, it's exactly like if you pick up a normal phone and hit a stored number memory button. Most Alarm Systems with B2B monitoring operate the same way, all you need do is make sure it's plugged into a working PSTN line.

And therein lies the problem, the PSTN line, it is the existing copper telecommunications network, which gets completely switched off 18 months after the area is formerly NBN ready. To get around this we need to go wireless - with a 3G or 4G dialler gateway - please, do not consider using VoIP for such critical infrastructure, somebody's life, maybe your own, may one day depend on that call button on a Lift, or panic button on your Alarm getting through to someone, help can't come if you're internet is down, or high jitter because your Internet is lagged out, or worse, it's on FTTN technology.

NBN (see PDF) recommends cellular (3G, 4G etc) diallers be used for Lifts, Security, and Fire Alarmed Systems, as there is no battery backup on FTTN/FTTB/FTTC, and very limited backup on only some FTTP installs. Reliability is key, and WH&S Laws covering Lifts and Fire must also be consulted.

To overcome the PSTN line problem you first need to purchase a 3G dialler, the most commonly used unit is the Ness 106-249 3G single line dialler, this unit ranges in cost from around $160 to $200, so shop around. At around 18*12*4 cm, it's small enough to fit inside most Lift Control units, it also includes a backup battery capable of powering the unit for two or so hours, which although not appearing to be very long, should be ample time - lets face it, if you're stuck in a Lift, you're not really going to sit around for a couple of hours before calling for help This unit also has an operating temperature range of 0-50Â°c, and is suitable for humid environments, making it the perfect fit for all Australian climates. Larger capacity multiple line units are also available from other manufacturers such as Aristel.

Next, purchase a SIM Card compatible with a 3G network, choose a cheap minimum value PAYG plan with a well established provider (so you know they'll still be around in years to come), you could use pre-paid, but I don't advise it, you don't want to be cut off for out of credit or past expiry if you didn't activate auto-renew, and most Telcos don't send warning Emails, just SMS's, which is pretty pointless since nobody gets them. There are however established companies that specialise in M2M (Machine to Machine) SIMs that are very well suited for Lifts and Alarms, one such example is M2Mone who at time of writing have very cheap PAYG plans at $1.50 per month, plus per second timed calls, works out to be around 69c a minute - perfect for Lifts and Alarm Systems that mostly sit idle. As touched on earlier, for a B2B Security Alarm, talk to your B2B company first, most have special SIMs and deals.

Setting up the Ness device is as easy as inserting the SIM into the dialler, plugging in its external antenna, then unplugging the phone lead coming from your Lift Control unit from the phone wall outlet, and plugging it into the phone socket at the rear of the 3G dialler, power it up, and you're good to go.

Your new 3G set up now looks something like this...

A few side notes...

Make a note of the date the dialler was installed, as with everything with batteries, they need to be replaced eventually, so at the very least, get them tested every twelve months.
Some Lift systems may have their phone cabling hard wired, in this case, you'll need to seek out a Registered Cabler to sort it out for you.
The dialler doesn't have to be located in or even next to the Lift Control system, if the existing phone line is currently wired to an MDF, the dialler can be connected down there, or anywhere in between, for convenience and/or security.
If this is for a Security Systems, before you go out and get any of this, it's possible your system is already capable of 3G services, either right now, or through purchase of a module or licence upgrade (yeah, I too despise these licence upgrade paths, someone's always out to rip us off every way they can).
If you're considering replacing or upgrading your entire Security System, you need to ensure it's 3G or 4G capable, if you need, or think one day you might need, back to base monitoring.
As for monitored Fire Alarms, you need to talk to your Fire Alarm Service Provider, your equipment may be under maintenance contract to be replaced by them, else discuss using a 3G or 4G dialler, such as above.

Hope this explains what needs to change for your Lifts and B2B Alarms. If you have other fixed dialler uses, like Doors, or Taxi phones, you may get away with using VoIP/SIP, but don't take any chances with services that may potentially save a life.

Usual Disclaimer: I have no direct relationship with any equipment manufacturer or cellular provider, I offer suggestions and examples based on what is known to work, and at fair and reasonable prices.

Posted by NoelB at 17:53

Friday, December 1. 2017

Why I Hate Commercial Control Panels

Whether it's DirectAdmin, cPanel, Plesk, or some other commercial hosting control panel, I pretty much dislike them all. They do their best to present an eye candy appealing image to help for good customer experiences, and I guess most of them do that well, probably far more appealing than the cobbled together scripts that I use allowing my hosts to manage their websites, but I guarantee you mine are probably more secure, efficient, scalable and redundant - capability beats looks any day!

In a few weeks time it'll be 2018, yet they still treat us like it's the 90's, limiting us to what daemons we can use on our own servers, limiting us to their choices of Linux distros, if it runs on RedHat, Debian, and FreeBSD, it'll run on SuSE, Slackware, Gentoo and others, but the biggest gripe of all, is they continue putting everything on one server. The process is along the lines of your customers sign up online, probably using Hostbill or WHMCS, it then shoots off to the current new hosts server's telling the Control Panel to set up the domain, its DNS, Email, Databases and Website structure - all on that one single machine, putting all your eggs in one basket, I guess they think hardware is infallible, where the truth is far from it.

The wheels do move ever so slowly though, back around 2010, some of these Control Panels started to introduce what they call multi server, or clustering - for DNS at least. How they seem to work though, means it still creates your DNS data on that one server, but then pushes out to the external DNS servers - which by the way for this to work, also needs your Control Panel installed, yep, more paid licences (some CP's do offer free DNS only licences and they are to be commended for that), either way, it's hardly an efficient method or true multi server, why bother creating records on the original host server in the first place, though still better than nothing I suppose, so when your host server is down for hardware failure, you should still at least have DNS.

But in web hosting, there are three critical components, DNS, WWW, and Email, so picture this, you're machines unresponsive, firefox and Outlook are both telling you it's DNS records can be found, but they just can't connect, what's the point if no-one can get to your website or email you, so your other two critical components, displaying your website or shopping cart etc, and Email, are kaput.

In 2017 there is no excuse for such archaic design, if your Website is down, your Mail shouldn't be, if Mail is down, your Website shouldn't be. Hosts, your customers wont care about blaming your Control Panel company, they will blame you, because it's your business and you decided how you are running it.

The situation doesn't have to be this bad though, but it will likely take making lots of noise to bring about change.

It's not hard, an ISP I worked for as far back as 2002, yes, 15 years ago, was able to do this right with complete separation of services, independent dedicated primary, secondary, and off-site tertiary DNS servers, we had multiple WWW servers which provided Web, MySQL and FTP for, at the time around 1200 customers each server, and we had a dedicated Mail server which stored all customers domains mail on RAID based disk array.

The way it should be done is very easy, instead of the Control Panel writing to corruptible flat, plain text files for Email virtual domains and users, a few simple SQL INSERT statements into a master database is all that's needed to have a highly scalable and efficient mail system, no need to edit text files for adding or closing domains, users, and suspension handling is as simple as setting a 0 or 1 in an "active" or "status" enum column.

I use the Postfix, Dovecot, MySQL (now days MariaDB) combination, I have used most MTA's over the years and found Postfix to be far superior in speed and resource niceness over Exim (which the CP companies tend to favour for some unknown reason), Qmail, and Sendmail, the great thing is Postfix and Dovecot work well together, using dovecot-lda for delivery is simple to configure, yes it does mean that if using multiple mail servers dovecot runs on all of them, even dedicated SMTP's (for delivery only) - but of course it only accepts connections for whatever the particular server is doing (truth be told every one of them can still do all protocols if you really wanted - some ISP's actually do it that way), and NFS to a NAS for the back end storage like EMC or NetApp, best using separate ethport on a private LAN, so mail storage flows go nowhere near the live network (but you could run it that way if you wanted to).

Separating Mail from Web also removes some of the loading issues that can be experienced during peek periods, it's

not so much the mail delivery itself, it's all the necessary stuff like anti virus and anti spam checks in particular that induce load, couple that with a bunch of heavy poorly written CGI scripts and a lot of very active sites, and the machines response times become at times noticeably lagged, and that's not what you, your customers, or your customers customers want to see.

You can see from the above diagram how simple this is, your HostBill/WHMCS Server sets up customer for billing, then talks to the allocated customer Web Server Control Panel via an API which adds your domain/host etc on that server, it also fires off to external DNS servers to add records and then it creates domain/user entries in your master Mail DB located back on your Billing Server which in turn replicates out to the mail server(s).

Depending upon your size and mail flow, you may need multiple SMTP, POP3 servers (like above image), you could do it all on one Mail server - at least you've separated it from the Websites serving, or one server for each protocol, whatever you like, but redundancy is cheap in the long run, having multiple servers for each protocol, and behind a load balancer though just gives better resiliency and performance, and allows you to perform maintenance without affecting users.

Using a database makes it efficient, it allows multiple servers to access the same auth details, it's fast, especially with writes, and mysqldump's ease of backing them up, which I do and recommend hourly. I've done it that way for over ten years never having had a single corruption from MySQL or MariaDB and never needing a database backup, unlike the many times I and others have had to restore plain passwd files that were periodically only half written, even the old vpopmail cdb files were a problem at times, fast reads, but terrible with writes.

Does this all cost more? Of course it does, you're using more hardware, but it doesn't have to be the latest and greatest, eBay often has decent cheap server and networking hardware as do many refurbished tech dealers, and lets not forget that Google's Gmail runs on many cheap "home-type" PC boards, in much the same sort of design.

Local media has over the years covered many outages from providers who just stacked everything together with major SAN failures, although not to scale, the end result here is the same, all those Web, Mail, DNS services unreachable, one provider I recall had over 10K angry customers without any service for two days with their SAN failure. Sometimes you just have to care enough to outlay a little bit more for long term benefit.

So if we on a shoe string budget could do this way back in 2002, why, in almost 2018, do the mass produced commercial Control Panel companies treat us all like it's still the 90's and make life more difficult than it needs to be for Host providers.

Well cPanel, Plesk, DA and co? Balls in your court, it's time you got your arses into gear and bring your software into the modern era. I'm sure there's a buck to be made for a true mutli-server operation, do I hear you say new product? I certainly hope so.

Posted by NoelB at 09:11

Wednesday, November 8. 2017

NBN And PABX Phone Systems

So your business is running an old analog multi-line PABX that you've used and trusted for years, you've also just been letter dropped that the NBN is ready for service in your area, ok, so that means you have 18 months to migrate to an NBN service before Telstra cuts off your existing copper services, you know it's wise to move sooner rather than later because you don't want to get caught out and be without a phone service when everyone waits till the last minute, and there's not enough techs to go round.

You decide you better start talking to some RSP's (Retail Service Providers), a fancy new name NBN has dreamt up for an ISP (apparently someone thinks they were clever [slow clap]), or worse - you get one of those pesky door to door sales people, either way, during your conversations all of a sudden your ears prick up because you've just been told that your trusty existing PABX wont work, it's incompatible with the NBN and you need to replace it. There is a tiny bit of truth in that, and I do mean tiny, like it wont work as is, but If you think it sounds more like a rort, you're probably right.

Some RSP's and Phone shops are telling businesses they need entire new phone systems (since NBN is a SIP or IP based service) when in fact they don't. These SIP PBX devices start at a little over $400 odd for a pretty comprehensive device suitable for SMB's such as a Grandstream 6202, but you can bet your bottom dollar the brands they are pushing are in the thousands, yet they all do pretty much the exact same thing and based on asterisk, most likely with freepbx or elastix, or a slight variation of.

Then there's the new phones they say you need, IP Phones, pretty basic handsets can be bought for under $100, a Grandstream 3 line handset will set you back around to $130-$140, I have little doubt the handsets they try to sell you are closer to costing several times that. Although cheaper, they are just as reliable and feature rich as the pricey ones, even the world renowned Linksys/Cisco SPA series (I've owned an SPA942 for going on 10 years now and its performed flawlessly, its comparative model today is about $190) and Grandstream, who have been around for a long time, and both substantially cheaper than say Avaya, LG, and other brands you're more used to associating with traditional phone systems, not to mention they are well known and respected in the VoIP world.

Then the RSP's will likely tell you, for once a truthful point, that it's more than likely your existing phone cabling wont work and needs replacing because it's the old 2 pair Cat3 cabling designed for analog phone systems, not the 4 pair Cat5/6 Ethernet cabling needed by IP Phones, and then there's the new PoE (Power over Ethernet) Switch that makes powering the phones plug and play, however most IP Phones are sold with AC adaptors (make sure you verify) so not completely essential, though you will need a decent switch anyway, the $29 things from eBay wont cut it in the long run.

See how easy it is for the costs to keep quickly adding up, it could very easily exceed $5000, closer to $10000, depending upon how many phones, cables and outlets have to be replaced.

I've been hearing horror stories of some SMB's quoted $5000 just for the PBX and a few phones - without new cabling. Some, but not all RSP's are sprouting this crap almost daily to unsuspecting business people who just need their phones to keep working. Sadly, the number of SMB's who fall for this will end up being high in the long run unless a lot of people get educated. I'd like to think this isn't all deliberate tactics, and is mostly because the sales people themselves, have no idea, but I wont be so naive to think some are not out to make a quick buck through any means.

In reality, your existing PABX will continue to work just as it does today with only a small modification, most modern PABX's are modular and have option for a plugable SIP module (that may already be installed), or a simple licence upgrade to activate SIP, and as for the systems that don't, like very basic systems, or old systems - which there are a lot of still in use today (I've worked with one that dates back 30 or so years) because they just work, can be made to work with the NBN via an external device called an ATA (Analog Telephone Adapter) for only a tiny fraction of the cost compared to replacing your entire system, a 2 line ATA (Grandstream HT802 or Cisco SPA 112) will set you back around $60, a 4 line (Grandstream HT814) for under $130, and an 8 line (Cisco SPA8000) for under $270, thus eliminating the need to replace your entire phone system, saving you countless thousands of dollars.

Rather than falling for these sales droids drivel, talk to your IT consultant or a Registered Cabling Provider who should be able to tell you if your system can do SIP, or if not, recommend, supply and install a suitable ATA for your PABX to hook into.

Currently, your PABX is likely wired into an IDC termination block, or directly to several wall sockets, basically to move to NBN - SIP based, rather than terminate in a terminal block or wall socket they are plugged into the ATA's FXS ports which uses ethernet data from your FTTx network to talk to your phone service provider via SIP, making it transparent.

An example of how NBN and an ATA with your old PABX works is

If you are considering a new phone system anyway, perhaps this would be a good time to consider a fully VoIP system, as it is the way of the future, but shop around, talk to your IT consultant or a Registered Cabling Provider for advice, as mentioned earlier, you can do a system for under $1000 (assuming you have compatible cabling), but most sales types will want you to buy a mega priced system - when you don't need it. This type of setup involves extra equipment on top of the PBX itself such as a PoE (Power over Ethernet) Switch, IP Phones, and you'll also need a decent Router with QoS, much like this example

A smaller business or shop, with a single line would likely be configured similar to a Household NBN Service like this

And to do away with a local PBX altogether, using a hosted PBX solution like

Hosted VoIP Services might suit a single person office, much like a personal VoIP service for home, but it is not a solution recommended for use with multiple phone requirements, there are plenty who say this works, but I've always found those people to have vested interests, your biggest problem is if there's no internet, you wont be able to call any other extension, not your sales guy in the office next to you, not your reception or front counter, not your warehouse storeman downstairs, nobody, all your phones are useless with no internet, and we've all seen the nightmare stories on the nightly news services about small businesses struggling with NBN outages.

If you decide you are going to replace your aging phone system with a brand new SIP based PBX, and require new or extra cabling, remember, Phone and Data Cabling can only be done by a Registered Cabler, NOT yourself, not even an Electrician unless they also have a current Open Cablers Registration and applicable endorsements ("S" as a minimum), so if you use an Electrician, just like any person claiming to be a authorised to conduct such work, you should ask to see their Cablers Registration Card, if they can not produce it for ANY reason, they must not be allowed to perform such work until they can produce it, an Electrician licence is not sufficient and does not authorise a sparky to do any phone or data work.

My advice here is, they are both specialised fields, so seek out a Registered Cabler, as that's all they do, day in, day out - phone and data, Electricians do what they do extremely well, but most of them don't do much phone or data as a rule, and most of them are not ACMA approved Registered Cablers.

*** WARNING: It is a criminal offence in Australia to tamper with, alter, or perform any phone or data work if it is, or even if it can be, used on or over a telecommunications or data network, including behind air-gaped WiFi devices, unless you are a Registered Cabling Provider with appropriate endorsements.

Existing penalties such as on-the-spot fines of $2040 for very minor breaches, or in more serious cases, court imposed fines of $90,000 and criminal conviction recorded is a real probability, as well as the likelihood of the removal of all illegal cabling.

Other things you need to be aware of are, using a non Telco provider (Telstra, Optus etc) SIP service, you will need to have your router enforce QoS for SIP, in reality this has rarely been a problem, some VoIP "experts" go over hypo when hearing people using anything without QoS, but perhaps they should just turn off their torrents instead

Also of note is, if you have an NBN connection with voice service from for example Telstra, they will make life extremely difficult in obtaining your own SIP details to use in third party equipment, they mostly will deny you access to that forcing

you to use their hardware, there are ways around this for some modem models, but frankly, why you'd continue to use their over priced voice services instead of established VoIP providers is another question you need to ask yourself. Most of them allow you to port over (keep) your existing phone numbers too, but take care if you have 13, 1300, or 1800 numbers, talk to your prospective SIP provider to ensure they can handle all that as well.

No matter which way you opt for when moving to the NBN, you will have minor downtime when NBN change you over, it can be hard to get NBN to keep an appointment time, delays happen, and can throw their entire days schedule out (try get a first up appointment), and your IT consultant or Cabling Provider should be there at the same time to minimise any disruptions. If you can, try to move only half your lines at a time, that way you wont be totally without a service, especially if your business relies upon the phone service.

Lastly, regardless of which system you opt for, ensure you have a dedicated half decent UPS with surge protection powering your NBN Modem, Router, PoE Switch, PABX, and ATA, for at least 2 to 4 hours.

I hope this article has helped to show you what happens with NBN and SMB phone systems, and that there is no reason to throw out your perfectly good working reliable existing analog PABX system when you're forced onto the NBN, no matter how old it is.

Disclaimer: I have no direct affiliation with any company linked to in this article, I use them as product/price examples only, I may however be a customer of some, and offer no guarantee that they are authorised agents or the prices they provide are the best available. Please review any store policies before considering any online purchases.

Posted by NoelB at 17:29

Tuesday, October 31. 2017

NBN With Multiple Phone Outlets

Australia's NBN, how it will affect your existing landline phones when you are migrated depends on how your home is currently wired and how many phones you have.

There's been a bit of rubbish being spread by RSP (Retail Service Provider - AKA: ISP) sales type people telling you your existing phones wont work when you're moved to the NBN. There is some truth to this, but no you likely do not need to re-wire your entire house or some such rot, or buy dect phones as only means of more phones, as many are being told, and despite other rhetoric from these sales geniuses, you can have more than one fix wired phone.

There are issues with leaving multiple active outlets in place on your original phone line when NBN connects your new service with their VDSL modem that's for certain, they can and do create issues that result in poor performance with your service, that's one of the few things NBN chief Bill Morrow and I actually agree on

There are typically two wiring layouts of a home with multiple outlets and ADSL, the first and most common is daisy chained, that sort of looks like this

(if any diagrams look incomplete, click on them for full size)

If you have such a setup, NBN may or may not (but should) disconnect the rest of the sockets from that first socket, also known as NBP (Network Boundary Point) in the chain, if they don't, you'll need to have a Registered Cabler do it for you (I heard recently that to stop many trivial NBN connection and speed complaints, that NBN techs are now doing this), and, if you want your other phone points to work again, you will need a Registered Cabler to come and make those changes anyway, in most cases, it's a matter of doing a little bit of wiring work at the first outlet, changing over the face plate and popping a couple more sockets in, much like figure 2 below

Another, less common wiring setup would be what's known as star wiring, this is where multiple cables are run from a central point, usually the Telstra (or now NBN) NTD (Network Termination Device), a big brownish looking box on side of your house next to your power box, as shown below

In this case, your costs will be a bit more because the Registered Cabler will need to do a lot more work, in most cases they can still re-use some (if not all) of your existing phone cabling, to give you a system much like Figure 2 daisy chaining from that first NBN socket.

Also, just because you have the big NTD box on your wall outside, doesn't mean you have star wiring, you may still have a daisy chained system, since early 2017 Telstra, and now NBN, will only install and cable lead-in to an NTD rather than a wall box and first outlet, on all new installations, this means the builder, or home owner, will need a Registered Cabler to do the actual wiring of the home and connect that to the NTD.

These are not all the wiring configuration possibilities, but they are the most common, so all in all, no, you don't need to re-wire your entire home.

The above is pretty much also applicable if you want to use an independent VoIP provider, rather than the VDSL voice - which is just an ATA output using the modems inbuilt SIP capabilities, just like many ADSL modems with VoIP ports, that's all it is, nothing special.

To use a private VoIP service, such as MyNetfone for example, using your own ATA (Analogue Telephone Adapter), you'll be running its phone-out FXS port into that new voice-in wall socket at the first outlet. Most RSP's are not divulging the SIP logins they provide on those voice ports, and personally I'd be using my own VoIP account and not an

RSPs over priced voice service anyway.

Trying to use your own VoIP account on their modems likely wont work, because they control that part, with you unable to even access that section of some providers modems, apart from any updates, resets etc, that will likely wipe yours out.

Whether using an over priced voice inclusive plan an RSP offers, or using an ATA with your own private VoIP service, I hope you're now more informed on what happens to your house wiring and what changes you might have to have made.

*** WARNING: It is a criminal offence in Australia to tamper with, alter, or perform any phone or data work if it is, or even if it can be, used on or over a telecommunications or data network, including behind air-gaped WiFi devices, unless you are a Registered Cabling Provider with appropriate endorsements.

Existing penalties such as on-the-spot fines of $2040 for very minor breaches, or in more serious cases, court imposed fines of $90,000 and criminal conviction recorded is a real probability, as well as the likelihood of the removal of all illegal cabling.

Phone and Data Cabling can only be done by a Registered Cabler, NOT yourself, not even an Electrician unless they also have a current Open Cablers Registration and applicable endorsements ("S" as a minimum), so if you use an Electrician, just like any person claiming to be a authorised to conduct such work, you should ask to see their Cablers Registration Card, if they can not produce it for ANY reason, they must not be allowed to perform such work until they can produce it, an Electrician licence is not sufficient and does not authorise a sparky to do any phone or data work.

My advice is they are both specialised fields, so seek out a Registered Cabler, as that's all they do, day in, day out - phone and data, Electricians do what they do extremely well, but most of them don't do much phone or data as a rule, and most of them are not ACMA approved Registered Cablers.

Posted by NoelB at 17:47

Tuesday, September 5. 2017

Ipv6 2017 Check Update

In 2015, we ran a test on our most commonly used sites for IPv6 responses which yielded pathetic 8% results, so this is a quick update to the article I wrote back then - IPv6 Reality Checks, but it seems here we are two and a half years later, only a handful of the previously IPv4 only hosts have managed to graduate to IPv6.

These hosts have since IPv6:

www.9news.com.au
bbc.co.uk
cnn.com
www.yourtv.com.au
mypolice.qld.gov.au
www.webhostingtalk.com
www.datacenterknowledge.com
techdirt.com
planefinder.net
comlaw.gov.au

However the following, the over whelming vast majority, still have yet to add IPv6 -
twitter.com
www.theguardian.com
www.abc.net.au
www.cbs.com
theplayer.platform.com
abc.com
www.tmr.qld.gov.au
www.foxtel.com.au
www.broadcastify.com
www.afl.com.au
www.bom.gov.au
itnews.com.au
blogs.crikey.com.au
slashdot.org
exchangewire.com
www.buzzfeed.com
arstechnica.com
techrepublic.com
gizmodo.com
mashable.com
wired.com
pcmag.com
www.helinews.com
www.airservices.gov.au
flightradar24.com
flightaware.com
www.msq.qld.gov.au
amsa.gov.au
ptwc.weather.gov
ebay.com.au
www.wia.org.au
sourceforge.net
github.com
www.apc.com

www.eaton.com
h10010.www1.hp.com
www.hp.com
www.dell.com
australia.emc.com
www.emc.com
www.netapp.com
irc.undernet.org
www.energex.com.au
tatts.com
www.seek.com.au
eway.com.au
www.lookout.com
www.marriott.com
www.hoyts.com.au

So there ya go, many still to wake up, yet this is not really a surprise as most the ISP's still do not provide native IPv6, TPG certainly don't. I have removed bigpondmusic, since they ceased to exist.
The financial institutions I use I also retested, none of them have upgraded yet either.

My original thoughts it'll be 2020 before things are really IPv6, sure looks like coming true

Posted by NoelB at 20:48

Saturday, September 10. 2016

NSA v Facebook - Who's More Evil

With all the Edward Snowden revelations about the extent of activities of the U.S.A's N.S.A, we are all like oh how dare they the privacy invading bastards, we all attack and condemn them - rightly so! We now realise how far out of control they and other Five Eyes member nations really are, so we tend to take more steps to protect our privacy from their prying eyes, make no mistake they are privacy invading power tripping scum who spend more time spying on friendly nations and their own law abiding citizens - than terrorists.

Yet, I'm betting pretty much all of those outraged over the NSA's actions, spend most of their days on feciesbook facebook, probably an unhealthy amount of time too, revealing everything about their life, now, I wrote some time ago about what I think of the privacy invading POS that is facebook, but recently, information on what they collect by their own admission, came to life, and it would make even the most seasoned operative at the U.S.A.'s NSA and U.K.'s GCHQ jaw drop in puddles of drool...

Facebook goes to great lengths to track you across the web, 98, yes, that's ninety eight data points they use that is or can be linked to you, they probably know more about your life than you do, and most certainly more then you'd like them to.

But then thereâ€™s creepier stuff that definitely isnâ€™t submitted voluntarily, such as the number of credit lines you have, whether youâ€™re an investor, what you invest in, whether you carry a balance on your credit card, whether you use coupons

Facebook knows every time you visit a page with a â€œlikeâ€• or â€œshareâ€• button whether you hit that button or not, its part of their tracking your every move. Remember back in 2014 or so when that was made public there was an outcry, well, little did we really know what was going on when you visit those sites, and other sites that have nothing to do with facebook.

So what is it exactly these facebook perverts collect on you directly and indirectly? (remember - this is from their own admission and not from some paranoid conspiracy newsgroup) Go get a coffee, it's a long list...

Location
Age
Generation
Gender
Language
Education level
Field of study
School
Ethnic affinity
Income and net worth
Home ownership and type
Home value
Property size
Square footage of home
Year home was built
Household composition
Users who have an anniversary within 30 days
Users who are away from family or hometown
Users who are friends with someone who has an anniversary, is newly married or engaged, recently moved, or has an upcoming birthday
Users in long-distance relationships
Users in new relationships
Users who have new jobs
Users who are newly engaged

Users who are newly married
Users who have recently moved
Users who have birthdays soon
Parents
Expectant parents
Mothers, divided by â€œtypeâ€• (soccer, trendy, etc.)
Users who are likely to engage in politics
Conservatives and liberals
Relationship status
Employer
Industry
Job title
Office type
Interests
Users who own motorcycles
Users who plan to buy a car (and what kind/brand of car, and how soon)
Users who bought auto parts or accessories recently
Users who are likely to need auto parts or services
Style and brand of car you drive
Year car was bought
Age of car
How much money user is likely to spend on next car
Where user is likely to buy next car
How many employees your company has
Users who own small businesses
Users who work in management or are executives
Users who have donated to charity (divided by type)
Operating system
Users who play canvas games
Users who own a gaming console
Users who have created a Facebook event
Users who have used Facebook Payments
Users who have spent more than average on Facebook Payments
Users who administer a Facebook page
Users who have recently uploaded photos to Facebook
Internet browser
Email service
Early/late adopters of technology
Expats (divided by what country they are from originally)
Users who belong to a credit union, national bank or regional bank
Users who investor (divided by investment type)
Number of credit lines
Users who are active credit card users
Credit card type
Users who have a debit card
Users who carry a balance on their credit card
Users who listen to the radio
Preference in TV shows
Users who use a mobile device (divided by what brand they use)
Internet connection type
Users who recently acquired a smartphone or tablet
Users who access the Internet through a smartphone or tablet
Users who use coupons
Types of clothing userâ€™s household buys
Time of year userâ€™s household shops most
Users who are â€œheavyâ€• buyers of beer, wine or spirits
Users who buy groceries (and what kinds)
Users who buy beauty products
Users who buy allergy medications, cough/cold medications, pain relief products, and over-the-counter meds
Users who spend money on household products
Users who spend money on products for kids or pets, and what kinds of pets

Users whose household makes more purchases than is average
Users who tend to shop online (or off)
Types of restaurants user eats at
Kinds of stores user shops at
Users who are â€œreceptiveâ€• to offers from companies offering online auto insurance, higher education or mortgages, and prepaid debit cards/satellite TV
Length of time user has lived in house
Users who are likely to move soon
Users who are interested in the Olympics, fall football, cricket or Ramadan
Users who travel frequently, for work or pleasure
Users who commute to work
Types of vacations user tends to go on
Users who recently returned from a trip
Users who recently used a travel app
Users who participate in a timeshare

Read the full Washington Post article for more.

So... what do you think about your beloved facebook now... huh? Remember, this is the company that you trust your details with, that wants to know so much about you it tracks you even when you're not on facebook , you trust them with your privacy? The same company who's founder and CEO had some accounts hacked because he used a simple password, that being dadada ...

I'm betting you'll still condemn the NSA, again, rightly so, but I'm also betting you still continue to give facebook your life's every little detail...

footnote: when I typed feciesbook at the start of this post (just like now) , Firefox's spell checker recommended I change it, yep, you guessed it, to facebook... ahhh pity it didn't work the other way round

In more facebook rot... The Guardian reports on facebook's farces.

In the weeks since Facebook fired the humans who curated its â€œtrendingâ€• news feed, its algorithmic floodgates opened up for fake stories, conspiracy theories and internet bile. This week, the company insisted it is a â€œneutralâ€• platform that needs no editors, even while it censored art, spread false news and deleted a post by Norwayâ€™s prime minister because it included a Pulitzer-winning photo from the Vietnam war. The leader had called for Facebook to â€œreview its editing policyâ€•, and the company eventually restored the post.

In a semi-regular column, weâ€™ll highlight what Facebook doesnâ€™t want to: the bogus stories, clickbait and disinformation being framed as legitimate news by one of the most powerful tech companies on Earth.

Read the full story over at The Guardian...

Posted by NoelB at 08:34

Saturday, July 2. 2016

Slackare 14.2 Released

Yyyyyyyiiiiiippppppppiiiiiieeeeeeee

Friday July 1 sees the release of version 14.2 of the most reliable and oldest Linux distro, Slackware!

Of course, http project which lately has gone into distro-clone-suckup-mode, that is, to try follow the likes of unstable distros like fedora and ubuntu and release often, are about to release 2.2.23, we have a vote ending this weekend that likely will pass. The attempt at speedily and stupidly pushing out stuff even if garbage saw the votes of 2.2.21 and 2.2.22 withdrawn because of one thing on each, showing the release often mentality is dumb arsed, it should be quality not quantity, more time should be given and RC's used, I've voiced my concern before, but the release-often fanbois tend to shout you down, and well, look at whats happened in past week alone, so Slackware's httpd package is out of date already...

The following is from email...

We are sure you'll enjoy the many improvements. We've done our best to bring the latest technology to Slackware while still maintaining the stability and security that you have come to expect. Slackware is well known for its simplicity and the fact that we try to bring software to you in the condition that the authors intended.

Slackware 14.2 brings many updates and enhancements, among which you'll find two of the most advanced desktop environments available today: Xfce 4.12.1, a fast and lightweight but visually appealing and easy to use desktop environment, and KDE 4.14.21 (KDE 4.14.3 with kdelibs-4.14.21) a stable release of the 4.14.x series of the award-winning KDE desktop environment. These desktops utilize eudev, udisks, and udisks2, and many of the specifications from freedesktop.org which allow the system administrator to grant use of various hardware devices according to users' group membership so that they will be able to use items such as USB flash sticks, USB cameras that appear like USB storage, portable hard drives, CD and DVD media, MP3 players, and more, all without requiring sudo, the mount or umount command. Just plug and play. Slackware's desktop should be suitable for any level of Linux experience.

Slackware uses the 4.4.14 kernel bringing you advanced performance features such as journaling filesystems, SCSI and ATA RAID volume support, SATA support, Software RAID, LVM (the Logical Volume Manager), and encrypted filesystems. Kernel support for X DRI (the Direct Rendering Interface) brings high-speed hardware accelerated 3D graphics to Linux.

There are two kinds of kernels in Slackware. First there are the huge kernels, which contain support for just about every driver in the Linux kernel. These are primarily intended to be used for installation, but there's no real reason that you couldn't continue to run them after you have installed. The other type of kernel is the generic kernel, in which nearly every driver is built as a module. To use a generic kernel you'll need to build an initrd to load your filesystem module and possibly your drive controller or other drivers needed at boot time, configure LILO to load the initrd at boot, and reinstall LILO. See the docs in /boot after installing for more information. Slackware's Linux kernels come in both SMP and non-SMP types now. The SMP kernel supports multiple processors, multi-core CPUs, HyperThreading, and about every other optimization available. In our own testing this kernel has proven to be fast, stable, and reliable. We recommend using the SMP kernel even on single processor machines if it will run on them. Note that on x86_64 (64-bit), all the kernels are SMP capable.

Here are some of the advanced features of Slackware 14.2:

- Runs the 4.4.14 version of the Linux kernel from ftp.kernel.org. The 4.4.x series is well-tested, offers good performance, and will be getting long term support from kernel.org. For people interested in running the latest Linux kernel, we've also put configuration files for

Linux 4.6 in /testing.

- System binaries are linked with the GNU C Library, version 2.23.
  This version of glibc also has excellent compatibility with
  existing binaries.

- X11 based on the X.Org Foundation's modular X Window System.
  This is X11R7.7 with many improvements in terms of performance and
  hardware support.

- Installs gcc-5.3.0 as the default C, C++, Objective-C,
  Fortran-77/95/2003/2008, and Ada 95/2005/2012 compiler.

- Also includes LLVM and Clang, an alternate compiler for C, C++,
  Objective-C and Objective-C++.

- The x86_64 version of Slackware 14.2 supports installation and booting
  on machines using UEFI firmware.

- Support for NetworkManager for simple configuration of wired and
  wireless network connections, including mobile broadband, IPv6, VPN,
  and more. Roam seamlessly between known networks, and quickly set
  up new connections. We've retained full support for the traditional
  Slackware networking scripts and for the wicd network manager,
  offering choice and flexibility to all levels of users.

- Support for fully encrypted network connections with OpenSSL,
  OpenSSH, OpenVPN, and GnuPG.

- Apache (httpd) 2.4.20 web server with Dynamic Shared Object
  support, SSL, and PHP 5.6.23.

- USB2, USB3, IEEE 1394 (FireWire), and ACPI support, as well as legacy
  PCMCIA and Cardbus support. This makes Slackware a great operating
  system for your laptop.

- The udev (eudev) dynamic device management system for Linux 4.x.
  This locates and configures most hardware automatically as it is added
  (or removed) from the system, loading kernel modules as needed. It
  works along with the kernel's tmpfs filesystem to create access nodes
  in the /dev directory.

- New development tools, including Perl 5.22.2, Python 2.7.11,
  Ruby 2.2.5, Subversion 1.9.4, git-2.9.0, mercurial-3.8.2,
  graphical tools like Qt designer and KDevelop, and much more.

- Updated versions of the Slackware package management tools make it
  easy to add, remove, upgrade, and make your own Slackware packages.
  Package tracking makes it easy to upgrade from Slackware 14.1 to
  Slackware 14.2 (see UPGRADE.TXT and CHANGES_AND_HINTS.TXT).
  The slackpkg tool can also help update from an older version of
  Slackware to a newer one, and keep your Slackware system up to date.
  In addition, the slacktrack utility will help you build and maintain
  your own packages.

- Web browsers galore! Includes KDE's Konqueror 4.14.13, SeaMonkey 2.40
  (this is the replacement for the Mozilla Suite), Mozilla Firefox ESR 45.2.0,
  as well as the Thunderbird 45.1.1 email and news client with advanced
  junk mail filtering. A script is also available in /extra to repackage
  Google Chrome as a native Slackware package (Chrome is only available for
  x86_64).

- The KDE Software Compilation 4.14.21 (KDE 4.14.3 with kdelibs-4.14.21),
  a complete desktop environment. This includes the Calligra productivity
  suite (previously known as KOffice), networking tools, GUI development
  with KDevelop, multimedia tools (including the Amarok music player and
  K3B disc burning software), the Konqueror web browser and file manager,
  dozens of games and utilities, international language support, and more.

- A collection of GTK+ based applications including pidgin-2.10.12,
  gimp-2.8.16, gkrellm-2.3.7, hexchat-2.12.1, xsane-0.999, and pan-0.139.

- A repository of extra software packages compiled and ready to run
  in the /extra directory.

- Many more improved and upgraded packages than we can list here. For
  a complete list of core packages in Slackware 14.2, see this file:

    ftp://ftp.slackware.com/pub/slackware/slackware-14.2/PACKAGES.TXT

Downloading Slackware 14.2:

The full version of Slackware Linux 14.2 is available for download from the central Slackware FTP site hosted by our friends at osuosl.org:

ftp://ftp.slackware.com/pub/slackware/slackware-14.2/

If the sites are busy, see the list of official mirror sites here:

http://mirrors.slackware.com

We will be setting up BitTorrent downloads for the official ISO images. Stay tuned to http://slackware.com for the latest updates.

Instructions for burning the Slackware tree onto install discs may be found in the isolinux directory.

Purchasing Slackware on CD-ROM or DVD:

Or, please consider purchasing the Slackware Linux 14.2 six CD-ROM set or deluxe dual-sided DVD release directly from Slackware Linux, and you'll be helping to support the continued development of Slackware Linux!

The DVD release has the 32-bit x86 Slackware 14.2 release on one side, and the 64-bit x86_64 Slackware 14.2 release on the other. Both sides are bootable for easy installation, and includes everything from both releases of Slackware 14.2, including the complete source code trees.

The 6 CD-ROM release of Slackware 14.2 is the 32-bit x86 edition. It includes a bootable first CD-ROM for easy installation. The 6 CD-ROMs are labeled for easy reference.

The Slackware 14.2 x86 6 CD-ROM set is $49.95 plus shipping, or choose the Slackware 14.2 x86/x86_64 dual-sided DVD (also $49.95 plus shipping).

Slackware Linux is also available by subscription. When we release a new version of Slackware (which is normally once or twice a year) we ship it to you and bill your credit card for a reduced subscription price ($32.99 for the CD-ROM set, or $39.95 for the DVD) plus shipping.

For shipping options, see the Slackware store website. Before ordering express shipping, you may wish to check that we have the product in stock. We make releases to the net at the same time as disc production begins, so there is a lag between the online release and the shipping of media. But, even if you download now you can still buy the official media

later. You'll feel good, be helping the project, and have a great decorative item perfect for any computer room shelf.

Ordering Information:

You can order online at the Slackware Linux store:

http://store.slackware.com

Other Slackware items like t-shirts, caps, pins, and stickers can also be found here. These will help you find and identify yourself to your fellow Slackware users.

Order inquiries (including questions about becoming a Slackware reseller) may be directed to this address: info@slackware.com

Have fun! :^) I hope you find Slackware to be useful, and thanks
very much for your support of this project over the years.

Oh well, now to go buy that new disk, most my current boxes have been upgrades after upgrades after upgrades, time to have a rolling clean install me thinks

BTW I know I haven't posted much in past year, time has been tight, I will get to my revised ipv6 tests soon.. promise!

Posted by NoelB at 11:31

Sunday, March 29. 2015

IPv6 Reality Checks

*** Update A revised entry for 2017 can be found here.

Recent statements made on an Australian industry mailing list about how well IPv6 was doing, with some people reporting their traffic is split 50/50 between IPv4 and IPv6, raised my eyebrows, I was not entirely convinced about those figures, so decided to put that 50/50 to the test to see how it applies in my situation.

One of these gentleman told me that my test was flawed, setting it up to fail even, well, I disagree with that, since if 50% of the traffic is favoured as IPv6, it still stands to reason that if I disable IPv4, about 50% of my traffic should still work - albeit slower at times for local sites since I'm limited to a tunnel provided by Hurricane Electric in California, U.S.A, so I expect a bit of lag using local sites, anyway, getting back on point, that should then result in the remaining 50% or so of traffic to actually fail, which is kind of the point if one wants to test the theory of half of the sites working or not via IPv6.

Another gentleman said to me that many IPv6 sites might fail because they still need IPv4 to lookup their AAAA (IPv6) records, I found this true in only one case (noted), however, the fact remains that it should not need an IPv4 address to lookup an IPv6 address, after all, the entire point of this is, IPv6 needs to completely replace IPv4, so why have a reliance upon it? If you are offering up IPv6 addresses, it makes sense to ensure your own DNS servers respond to those queries on IPv6, just as it is now, and has been for decades, with IPv4. (view my test script)

Now, it would be foolish to think that the data usages are all the same, in fact, probably vastly differs greatly between all of us, so we'll assume the results should still be roughly in that 50/50 to 40/60 vicinity, or so one would think.

Update: A small number of people have criticized these tests, nit picking and splitting hairs on data/traffic/sites, lets be realistic, they do go hand on hand, if you want to be a hero and claim actual data, you can claim 100% over IPv6 if you just used youtube and nothing else - but the world doesn't work that way. So consider this an overall test of IPv6 usability/accessibility/reachability/whatever_else_you_want_to_call_it. because unless you have a more sheltered life than me, you do visit more than just one site.

You will soon see that I'm a rather boring individual when it comes to online activities, I'm sure I've been responsible for putting many an NSA operative to sleep on the job. I have decided there is pretty much no risk to my privacy in publishing the sites I frequent, anyone who's read more than one of my posts knows I'm into IT, and most of us use Social Media and online entertainment, but I have withheld listing some sites for privacy reasons as they involve financial transactions, everything else listed is used by tens of thousands plus others and are very common sites, so I don't consider them an invasion of my privacy or able to be used in any nefarious ways against me (sorry Senator Brandis). You will notice I do not list faecesbook facebook, I don't use the pervert stalker infested ID-Theft crime gang privacy invading P.O.S, you'll notice I don't list Skype, I do use it, but neglected to test it - my bad, so I wont count it in either pool.

Time to get started, IPv6 was upped, and IPv4 was downed, DNS tested, works good, I don't include my VPS's in Frankfurt or L.A. since I set them up and know they work, but they were the baseline test, the fact I could ping, trace, and ssh into both of those boxes located on two entirely different networks, confirms my DNS and routing of IPv6 is good to go.

So I started testing the usual sites I go to daily, and to ensure I didn't leave any (or hopefully many) out, I checked my browsers history and even grabbed the ones I only use every once in a while - like buying music which I might do once every month or two, banking/paying bills (the suppressed sites), and hardware sites to check out the latest server and storage stuff, so all kind of irregular stuff as well as the almost required daily rituals.

The results were far far worse than I anticipated, so much so that I had to check that IPv6 didn't drop! Nope, still there, still access my VPS's, still access Google and Youtube, but I could pay no bills, nor buy any music, couldn't buy my lotto entry for Saturdays 21mil or Thursdays 30mil jackpots, I couldn't do much at all...

As most of the world knows, Australia has the most pathetic TV network programming, it's why we are known as the worlds largest copyright infringer's of TV shows. Australian TV networks treat Australians with utter contempt, we end up waiting months at times for hit shows to appear or return to our little screens, and all TV networks are guilty of this (I do applaud the ABC for same time as UK airing of Doctor Who though!), so of course people don't want to wait 3 or more months after the rest of the world has seen them, the internet is instant - forums, newsgroups and chat rooms fill with discussions of what just aired, so most Australians take matters into their own hands by torrenting to see it at the pretty much the same time as the U.S. and Europe so they don't feel ostracised.

But a small number of people like myself don't go down that road, we opt for either Geoblock bypass add-ons, or VPN's, the latter is my favourite since I have a VPS in the U.S., enabling a VPN on the VPS to watch catchup TV is trouble free, this way I can sit down on a Saturday or Sunday and log into the U.S. networks websites and watch episodes on catchup... but alas, not today, one site, NBC, actually did respond on IPv6, but then to watch the stream, it called an IPv4 only service, so, scrub that out too.

It's no surprise however that Youtube and Google Search worked because everyone knows Google is IPv6 ready, so my morning was not totally lost and it was surprisingly not that much slower than if I had gone direct with IPv4.

A large number of IT and Tech related sites also failed, in fact the only one to respond was Heise - the most popular IT professionals site in Germany, not overly surprised since Germany has an overall IPv6 takeup of around 19% from what I have seen, that's the best in the world, that betters the U.S that sits around 17%, of course most of these are probably end-user IP ranges being enabled, because as the checked list below shows, there aren't too many websites that I view that are IPv6 capable.

In concluding, the results were horrific for IPv6, I have absolutely no idea what these other guys are doing, but 50%? My results here are only 6 sites accessible, with 63 sites unreachable, that's more like a measly few 8 percent of sites accessible via IPv6.

Sites Accessible
google
youtube
www.heise.de
aussiescanners.com
pch.net
en.wikipedia.org

Sites Not Reachable
twitter.com
www.theguardian.com
www.9news.com.au
www.abc.net.au
www.cbs.com
nbc.com (yes, but failed streaming because of - theplayer.platform.com)
abc.com
www.tmr.qld.gov.au
www.foxtel.com.au
bbc.co.uk
cnn.com
www.broadcastify.com
www.yourtv.com.au
bigpondmusic.com.au
www.afl.com.au
www.bom.gov.au
mypolice.qld.gov.au
itnews.com.au
www.webhostingtalk.com
www.datacenterknowledge.com
blogs.crikey.com.au
slashdot.org
exchangewire.com
techdirt.com

www.buzzfeed.com
arstechnica.com
techrepublic.com
gizmodo.com
mashable.com
wired.com
pcmag.com
www.helinews.com
www.airservices.gov.au
flightradar24.com
planefinder.net
flightaware.com
www.msq.qld.gov.au
amsa.gov.au
comlaw.gov.au (This site requires IPv4 to lookup its IPv6 address)
ptwc.weather.gov
ebay.com.au
sourceforge.net
github.com
www.apc.com
www.eaton.com
h10010.www1.hp.com
www.hp.com
www.dell.com
australia.emc.com
www.emc.com
www.netapp.com
irc.undernet.org
www.energex.com.au
tatts.com
www.seek.com.au
eway.com.au
www.lookout.com
www.marriott.com
www.hoyts.com.au
Four sites not listed since they are related to financial/bill transactions.

Perhaps if people had not been crying wolf about running out of IPv4 addresses in two years time, every two years, from around 1992 onwards, and only cried about it when it was really only two years or so off, maybe CSP's might today have a stronger IPv6 uptake.

Either way we have run out of IPv4 now, yet many CSP's have warehouses of spare addresses to dish out still - they weren't all totally asleep at the wheel like some think. Yes, we do need to move to IPv6 now, and yes, Australia is amongst the worst offenders for rolling it out at about 0.01% uptake, but given my tests, it isn't any real surprise that our Service Providers see no urgency.

In the mean time, if you want to play around with IPv6 at home, locate a tunnel broker, there are a few free ones around, and although based in the U.S. I highly recommend Hurricane Electrics free tunnelbroker.net service, the latency isn't that bad at all, and since most international traffic goes via the U.S., you may not even notice the difference.

Posted by NoelB at 22:57

Sunday, November 16. 2014

Metadata

Update: March 29, 2015

Metadata, just the latest annoyance by the Australian Government to spy on our Internet use, they couldn't screw us over with the failed mandatory filtering attempt, so they'll try get us another way. Not sure what all the fuss is about however since we now know the United States's NSA and UK's GCHQ has been doing this a long time thanks to the Snowden Releases, so all Canberra need do is pick up the phone and call head office

Now, I'm not going to go into all the bungling of them trying to sell this to us, Bumbling George Brandis's comedy show has been doing the rounds for a while now, when he came out with his and Woger Wabbott's , I mean Tony Abbott's version, it was like the two stooges Larry and Moe, without curly - Malcolm Turnbull, who finally did have to join the duo and fix up their diabolical mess, sending relief down peoples spines knowing the Government did not want to know what websites you went to, just who had what IP on what date. Much more different to voice, since they do want to know who you called, and when and from where.

When this came about I was in two minds about it, didn't have strong objections, my IP's static so wont be too hard to find me in radius, and I've had it for nearly five years at home, so there's no doubting its accuracy, as for phone, well, I make/get SFA phone calls, I rarely use 3G data because it's about the same price as pure gold in Australia. Most of my communications from home is by IRC, IM (Jabber/Skype - so the U.S.'s NSA already know who I talk to anyway), Email, ramblings on Twitter, or this strange thing called ...
"in real life".

With Email, I've used PGP (actually GPG) digital signatures for well over a decade, I think I've only ever used encryption a couple of times, mostly just to piss off the U.S.'s NSA. I don't deal with sensitive material much these days, so I ask myself, despite being a very private person, is it really such a big deal? They are just going to keep this stuff for a couple of years, and to be honest I can pull Email server logs going back to around 2007, saying who at what IP, sent to who, but contrary to the Governments belief - no, we don't log subjects, because the Subject is in the DATA segment of a messages transaction, it has nothing to do with envelope header details which is all mail servers log (or need to know), basically this means the Subject is actually part of content, and no one logs that, but not that that's really much of a problem, since if I was a terrorist going to blow up some building, I'd hardly put in the subject "Re: that building we're gunna blow up"... All I can do is... shake my head... seriously, where do Governments get these ideas from, clearly pen pushers that have no clue.

The most common Mail Server software's, or more precisely, Mail Transport Agents (MTA) - the part of mail servers that accept inbound and outbound mail - postfix, exim, sendmail, and to much lesser extent other MTA's do not log anything other than envelope sender, recipient, size, time, message-id - stuff like that.

Updated Nov 16, because I've had a number of emails asking to show what a typical ISP/WebHost type mail server actually logs, I am adding a lightly sanitized copy (to protect the recipient from spambots), and for those confused about it loading twice, the second injection is to amavisd which handles all anti spam and virus detection...

Nov 16 11:38:14 valhalla postfix/smtpd[8807]: connect from omp.email.flybuys.com.au[12.130.139.106]
Nov 16 11:38:15 valhalla postfix/smtpd[8807]: 76D3EC0EBCA: client=omp.email.flybuys.com.au[12.130.139.106]
Nov 16 11:38:15 valhalla postfix/cleanup[8814]: 76D3EC0EBCA: message-id=
Nov 16 11:38:16 valhalla postfix/qmgr[5996]: 76D3EC0EBCA: from=, size=83006, nrcpt=1 (queue active)
Nov 16 11:38:16 valhalla postfix/smtpd[8807]: disconnect from omp.email.flybuys.com.au[12.130.139.106]
Nov 16 11:38:19 valhalla postfix/smtpd[8818]: connect from localhost[127.0.0.1]
Nov 16 11:38:19 valhalla postfix/smtpd[8818]: 12A55C0EBCB: client=localhost[127.0.0.1]
Nov 16 11:38:19 valhalla postfix/cleanup[8814]: 12A55C0EBCB: message-id=
Nov 16 11:38:19 valhalla postfix/qmgr[5996]: 12A55C0EBCB: from=, size=87818, nrcpt=1 (queue active)
Nov 16 11:38:19 valhalla postfix/smtpd[8818]: disconnect from localhost[127.0.0.1]
Nov 16 11:38:19 valhalla amavis[979]: (00979-05) Passed SPAMMY {RelayedTaggedInbound}, [12.130.139.106]:43915 [12.130.139.106] -> , Queue-ID: 76D3EC0EBCA, Message-ID: , mail_id: uvPRGJls45Du, Hits: 3.302, size: 82970, queued_as: 12A55C0EBCB, dkim_sd=flybuys2:edm.flybuys.com.au, 2572 ms
Nov 16 11:38:19 valhalla postfix/smtp[8817]: 76D3EC0EBCA: to=, relay=127.0.0.1[127.0.0.1]:10024, delay=4.2,

delays=1.6/0.02/0/2.6, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 12A55C0EBCB)
Nov 16 11:38:19 valhalla postfix/qmgr[5996]: 76D3EC0EBCA: removed
Nov 16 11:38:19 valhalla postfix/pipe[8819]: 12A55C0EBCB: to=, relay=dovecot, delay=0.43, delays=0.19/0.01/0/0.22, dsn=2.0.0, status=sent (delivered via dovecot service)
Nov 16 11:38:19 valhalla postfix/qmgr[5996]: 12A55C0EBCB: removed

..Dovecot logs show nothing more:
Nov 16 11:38:19 lda(deletethis@ausics.net): Info: sieve: msgid=: from=flybuys@edm.flybuys.com.au: stored mail into mailbox 'INBOX'

So no, I'm sorry Mr's Brandis, Abbott, and Turnbull (who should know better given his ISP background), there is no logging of subjects for the very reason given above - it's in the DATA (content) component, but to sprout that ISP's already log subjects (as in your claims ISP's already log all this stuff) is plain wrong, in fact, one could say an outright lie, but perhaps Windows MTA's might log subjects, however since they are in use in in only about 6% of the worlds mail servers, pretty much all of which would be corporate (private) organisations and not ISP's, they are irrelevant and can not be used as an example of an existing industry standard.

Anyway, I then thought more about it, as has been clearly shown in news articles around the globe that you don't need content to build a persons profile, the metadata is all about names, dates, and locations. Think about it, a trend as to who my friends are, where we meet, do we go out on the same day(s) every week or weekend, after a while they can tell where I shop, what my favourite restaurant is, what sports I like, and what my hobbies may be and where, so they don't need to read the content of my Email's or listen to my phone calls to learn enough to build a picture of me, this is recently supported by comments made by United Nations German ambassador Harald Braun:

"Metadata can be as privacy sensitive as the content of communications," said Braun, who raised concerns about how easy it is to compile personal profiles by collecting metadata.

Updated Dec 20, 2014, an example on what can be found out, and a very small example was demonstrated in this SMH article, remember, what was found here is by publicly available tools, just imagine what the government and its tools could do.

Yet another scary thought is ISP's and Telcos are going to be required to store this data, so what if they get hacked, the hacker can sell off our information to some crime gang(s), who then get the same life profile as the Government can, perfect recipe for identity theft amongst other nasty things, and don't be so naive to think once this is law, a little while down the track hackers wont be concentrating on breaking into those systems, because they will, anyone who doesn't think so, is only fooling themselves, this would still be the case even if Governments stored the data.

So, now I'm less in favour of this plan, but I want to know who has access to it all, on one hand we have the Attorney General George Brandis saying things like

The laws will apply "only to crime and only to the highest levels of crime," the attorney-general said. "Breach of copyright is a civil wrong. Civil wrongs have got nothing to do with this scheme."

But then we also have the AFP boss (Colvin) saying

the stored data of Australians could be used for a whole number of things, including anti-piracy

Confused? So are we, on one hand you have the head of legal saying no it can't be used outside serious crime, but then you have the head of the AFP saying it can, Colvin's statement was however backup up by Communications Minister Malcolm Turnbull who admitted that the stored data would be accessible through the court process, and the mandatory data-retention legislation would not prevent that from happening.

"They can through civil proceedings. Sure, as they always have done. They can go to court, and they can seek discovery of the records that disclose the account to which a particular IP address was allocated at a particular time, but they do not have warrantless access to metadata in the way the police and ASIO and Customs have," he said.

Looking at the key bits of The Bill

Schedule 2â€”Restricting access to stored communications and telecommunications data
Part 1â€”Main amendments

Telecommunications (Interception and Access) Act 1979

1 Subparagraphs 107J(1)(a)(i) and (ii)
Omit â€œan enforcement agencyâ€•, substitute â€œa criminal law?enforcement agencyâ€•.

2 Subsection 110(1)
Omit â€œAn enforcement agencyâ€•, substitute â€œA criminal law?enforcement agencyâ€•.

3 After section 110
Insert:
110A Meaning of criminal law?enforcement agency
(1) Each of the following is a criminal law?enforcement agency:
(a) the Australian Federal Police;
(b) a Police Force of a State;
(c) the Australian Commission for Law Enforcement Integrity;
(d) the ACC;
(e) the Australian Customs and Border Protection Service;
(f) the Crime Commission;
(g) the Independent Commission Against Corruption;
(h) the Police Integrity Commission;
(i) the IBAC;
(j) the Crime and Corruption Commission of Queensland;
(k) the Corruption and Crime Commission;
(l) the Independent Commissioner Against Corruption;
(m) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.

(2) The head of an authority or body may request the Minister to declare the authority or body to be a criminal law?enforcement agency.

(3) The Minister may, by legislative instrument, declare:
(a) the authority or body to be a criminal law?enforcement agency; and
(b) persons specified, or of a kind specified, in the declaration to be officers of the criminal law?enforcement agency for the purposes of this Act.

(4) In considering whether to make the declaration, the Minister must have regard to:
(a) whether the functions of the authority or body include investigating serious contraventions; and
(b) whether access to stored communications, and the making of authorisations under section 180, would be reasonably likely to assist the authority or body in investigating those serious contraventions; and
(c) whether the authority or body:
(i) is required to comply with the Australian Privacy Principles; or
(ii) is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles; or
(iii) has agreed in writing to comply with a scheme providing such a level of protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made; and
(d) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of a criminal law?enforcement agency under Chapter 3, and the obligations of an enforcement agency under Chapter 4; and
(e) whether the Minister considers that the declaration would be in the public interest; and
(f) any other matter that the Minister considers relevant.

(5) In considering whether to make the declaration, the Minister may consult such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.

(6) The declaration may be subject to conditions.

(7) Without limiting subsection (6), a condition may provide that the authority or body is not to exercise:
(a) a power conferred on a criminal law?enforcement agency by or under a specified provision in Chapter 3; or
(b) a power conferred on an enforcement agency by or under a specified provision in Chapter 4.
The authority or body is taken, for the purposes of this Act, not to be a criminal law?enforcement agency for the

purposes of that provision in Chapter 3, or an enforcement agency for the purposes of that provision in Chapter 4, as the case requires.

(8) The Minister may, by legislative instrument, revoke a declaration under subsection (3) relating to an authority or body if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force.

(9) The revocation under subsection (8) of a declaration relating to an authority or body does not affect the validity of:

(a) a domestic preservation notice given by the authority or body; or

(b) a stored communications warrant issued to the authority or body; or

(c) an authorisation made by an authorised officer of the authority or body under Division 4 of Part 4?1;

that was in force immediately before the revocation took effect.

So that says for Criminal Investigations, it doesn't say only serious crime, and after all the mumbo jumbo a civil body will likely still get access through a court, lets use Copyright infringement as one of those outside possibilities.

In rare cases Copyright infringement can be, if deemed on a commercial scale, included under the Crimes Act, so becomes a criminal offence, but who decides what is commercial scale? One person uploading a song, not for gain, knowing that song will be dissected and distributed further, maybe after a while thousands of times - that to me is of a commercial scale regardless of any monetary gain, so pretty much everyone who partakes in that activity could be included under the Criminal Code.

Let's look at it another way, the AFP tell some rights holder to sod off they are not interested (I recall last decade a Commander in the AFP saying publicly the AFP have far more important things to do than go after kids who do online sharing), so the rights holder goes to a court and says we want to know who these people are, they know the ISP will have this information stored under law, so sue the ISP for this information.

My take on this is a court shouldn't have the right to do that based on the Bill as it stands, but courts will see it that way and decide they have the right to order that data released to a civil party, it may not be copyright matters, it could be ugly divorce matters, insurance claims, the list goes on, if this does succeed in its current form, because it's so holey, it is very dangerous, oh it goes to great lengths to tighten the rope around what Government departments can access it and when, but not civilly, I do envisage a High Court challenge the moment civil use gets granted access by a lower court.

I call on the Government to amend the Bill to clear up these matters, they could easily add into the Bill conditions that tighten this up and make it clear to courts that they can only order the release for criminal investigations, or serious crimes, as the Attorney General keeps saying, or civilly up to a reasonable date.

There must be no loopholes, civil matters must not have access to the stored data past a reasonable time frame, or made available to them for discovery or for any other reason after a reasonable time frame, I'd think 28 days.

I say 28 days because it would be reasonable to expect an ISP would already keep user data handy for short periods of time, such as four weeks, for operational purposes, like billing, spam and abuse complaints, so a partition to a civil court for the users data within 28 days I think is not unreasonable.

However, it could be considered unreasonable to expect that a typical ISP would keep this data longer than four weeks and they may only then be doing so because of lawful requirement under this Metadata Bill allegedly for serious criminal investigations, so the rights of discovery, or any civil access, must end after 28 days (since courts deem one month as 28 days) for everything other than serious, criminal investigations.

I hope I'm not confusing you now, because (as written elsewhere in my blog from the iitrial days) I have always believed that rights holders should target the offenders - not ISP's, and only by means of going to a court and seeking the details of a particular user, based on an IP address at a specific date/time, and the court must approve each user/IP match - none of this blanket discovery access.

Anyway as it stands, The Bill is dangerous, so I decide I no longer support it in its current form, therefore, I would hope when it comes time, The Bill is voted down.

Updated March 29, 2015

This past week, the Senate has approved the data retention Bill, although it had some 30 odd changes from its original, it is now Law (as soon as it gets royal accent which will be soon).

Both the Liberal Govt and the sell-outs of the Australian Labor Party agreed to its passing in a major vote win, however, this was a done deal long ago, and despite many attempts to tighten it up, for instance, Sen Leyonhelm, tried to have an amendment to the Bill to ensure it was only used for serious crimes - As Sen George Brandis A.G has been telling us it would only ever be used for, but Brandis and the Libs and Sen Jacinta Collins on behalf of the ALP, both refused that amendment, later on Brandis even admitted that his promise of the serious crimes only access was false since even with PJC's recommendations, it is still very possible for courts to allow access to civil litigants. A move most of us know was deliberate, well, Brandis isn't known as the Minister for U.S. and Hollywood for the fun of it!

One thing is clear however, the Govt has learned that Subjects in Email are part of content and are exempt. not that it makes much difference since as we and despite denials, the Govt and ALP fully know that you can tell more about a person with metadata than content, so who needs that.

Posted by NoelB at 12:06

Saturday, July 5. 2014

Popular Linux Website A Threat to the USA - Apparently

In what can only be described as the most funniest thing I've read in many many years, the U.S.A.'s National Security Agency (NSA) regards The Linux Journal Website as an extremists forum, and its users as extremists, therefore logs its users, likewise with privacy site TAILS, and they also keenly, but not really unexpectedly, (try to) target the Tor network.

I just find it ridiculous on all levels that Linux users, or anyone who values their privacy, are labelled as extremists, the only extremists here, are the out of control U.S.A's NSA!

It's wrong when merely visiting privacy related websites is enough for a user's IP address to be logged into a NSA database, and become a possible target, and it's beyond dangerous scope creep when visiting a Linux website gets you thrown into the same basket, it's about time these bastards had the reigns thrown on them, from not only within the U.S.A., but from all other countries that give a damn about their citizens, the only country with any guts at present to do this seems to be Germany. Shame on our Australian government as well, who wont do squat, since they are just U.S. puppets and lap dogs who take their orders from Washington.

The line "if you got nothing to hide, you have nothing to fear" is just pure bullshit and doesn't wash.

From XKeyscore Rules

```
/ START_DEFINITION
/
These variables define terms and websites relating to the TAILs (The Amnesic
Incognito Live System) software program, a comsec mechanism advocated by
extremists on extremist forums.
/

$TAILS_terms=word('tails' or 'Amnesiac Incognito Live System') and word('linux'
or ' USB ' or ' CD ' or 'secure desktop' or ' IRC ' or 'truecrypt' or ' tor ');
$TAILS_websites=('tails.boum.org/') or ('linuxjournal.com/content/linux*');
// END_DEFINITION
```

TAILS
Tails is a privacy-focused Linux based operating system that runs entirely from an external storage device such as a USB stick or CD. It comes with Tor and other privacy tools pre-installed and configured, and each time it reboots it automatically wipes everything that is not saved on an encrypted persistent storage medium. However, pretty much any Linux distribution like Slackware, openSuSE, or Fedora, etc, are just as capable if you're slightly above a novice Linux user.

TOR
As for Tor (which incidentally was developed by the U.S. Navy Research Lab for protecting government communications), normally a user's online traffic - such as emails, instant messages, searches, or visits to websites, can be attributed to the IP address assigned to them by their internet service provider. When a user goes online over the Tor Network, their connections are relayed through a number of Tor nodes using another layer of encryption between each server such that the first server cannot see where the last server is located and vice-versa.

Please read the full five page story at http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html

Posted by NoelB at 19:38

Friday, May 16. 2014

Mozilla Does DRM Deal With Adobe Devil

So much for Mozilla's motto of openness, yet again another netizens call to action arises to make Mozilla realise what a grave error this is, remember, it was public opinion that forced the resignation of Eich over his support for organisations rife with homophobia in trying to stop marriage equality, so time to start all over again to stop them supporting DRM.

FSF condemns partnership between Mozilla and Adobe to support Digital Restrictions Management

In response to Mozilla's announcement that it is reluctantly adopting DRM in its Firefox Web browser, Free Software Foundation executive director John Sullivan made the following statement:

Only a week after the International Day Against DRM, Mozilla has announced that it will partner with proprietary software company Adobe to implement support for Web-based Digital Restrictions Management (DRM) in its Firefox browser, using Encrypted Media Extensions (EME).
The Free Software Foundation is deeply disappointed in Mozilla's announcement. The decision compromises important principles in order to alleviate misguided fears about loss of browser marketshare. It allies Mozilla with a company hostile to the free software movement and to Mozilla's own fundamental ideals.

Although Mozilla will not directly ship Adobe's proprietary DRM plugin, it will, as an official feature, encourage Firefox users to install the plugin from Adobe when presented with media that requests DRM. We agree with Cory Doctorow that there is no meaningful distinction between 'installing DRM' and 'installing code that installs DRM.'

We recognize that Mozilla is doing this reluctantly, and we trust these words coming from Mozilla much more than we do when they come from Microsoft or Amazon. At the same time, nearly everyone who implements DRM says they are forced to do it, and this lack of accountability is how the practice sustains itself. Mozilla's announcement today unfortunately puts it -- in this regard -- in the same category as its proprietary competitors.

Unlike those proprietary competitors, Mozilla is going to great lengths to reduce some of the specific harms of DRM by attempting to 'sandbox' the plugin. But this approach cannot solve the fundamental ethical problems with proprietary software, or the issues that inevitably arise when proprietary software is installed on a user's computer.

In the announcement, Mitchell Baker asserts that Mozilla's hands were tied. But she then goes on to actively praise Adobe's "value" and suggests that there is some kind of necessary balance between DRM and user freedom.

There is nothing necessary about DRM, and to hear Mozilla praising Adobe -- the company who has been and continues to be a vicious opponent of the free software movement and the free Web -- is shocking. With this partnership in place, we worry about Mozilla's ability and willingness to criticize Adobe's practices going forward.

We understand that Mozilla is afraid of losing users. Cory Doctorow points out that they have produced no evidence to substantiate this fear or made any effort to study the situation. More importantly, popularity is not an end in itself. This is especially true for the Mozilla Foundation, a nonprofit with an ethical mission. In the past, Mozilla has distinguished itself and achieved success by protecting the freedom of its users and explaining the importance of that freedom: including publishing Firefox's source code, allowing others to make modifications to it, and sticking to Web standards in the face of attempts to impose proprietary extensions.

Today's decision turns that calculus on its head, devoting Mozilla resources to delivering users to Adobe and hostile media distributors. In the process, Firefox is losing the identity which set it apart from its proprietary competitors -- Internet Explorer and Chrome -- both of which are implementing EME in an even worse fashion.

Undoubtedly, some number of users just want restricted media like Netflix to work in Firefox, and they will be upset if it doesn't. This is unsurprising, since the majority of the world is not yet familiar with the ethical issues surrounding proprietary software. This debate was, and is, a high-profile opportunity to introduce these concepts to users and ask them to stand together in some tough decisions.

To see Mozilla compromise without making any public effort to rally users against this supposed "forced choice" is doubly disappointing. They should reverse this decision. But whether they do or do not, we call on them to join us by

devoting as many of their extensive resources to permanently eliminating DRM as they are now devoting to supporting it. The FSF will have more to say and do on this in the coming days.

For now, users who are concerned about this issue should:

Write to Mozilla CTO Andreas Gal via agal_at_mozilla DOT com, and let him know that you oppose DRM. Mozilla made this decision in a misguided appeal to its userbase. It needs to hear in clear and reasoned terms from its own users who feel this as a betrayal. Ask Mozilla what it is going to do to actually solve the DRM problem that has created this false forced choice.

Join the effort to Stop EME approval at the W3C. While today's announcement makes it even more obvious that W3C rejection of EME will not stop its implementation, it also makes it clear that W3C can fearlessly reject EME to send a message that DRM is not a part of the vision of a free Web.

Use a version of Firefox without the EME code: Since its source code is available under a license allowing anyone to modify and redistribute it under a different name, we expect versions without EME to be made available, and you should use those instead. We will list them in the Free Software Directory

Most of this post is of course from FSF's Email, there is nothing I could really add to it, its quite to the point, for FSF complete statement see https://u.fsf.org/xk

Posted by NoelB at 11:04

Saturday, June 8. 2013

PRISM - The US Govt Caught Out, Yet Again

Updated Feb 28, 2014

For complete run down, please visit The Guardians NSA Files

The Prism program allows the U.S. National Security Agency (NSA), the world's largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.

With this program, the NSA (a military defined organisation) is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on users.

We have recently been hearing reports from American politicians, Embassy staff (Yes, looking at you Jeff Bleich), and U.S. cloud service providers, and security experts all claiming the worlds fear of U.S. Laws, like the Patriot Act when it comes to hosting data in the U.S., is just FUD, even as recent as two days ago I read a report from a U.S. cloud expert in Europe trying to show the world it is safe to host data in the U.S., claiming there is oversight, court orders are in fact needed (something that we have known for along time is utter rubbish - google FISA warrant), and this expose about PRISM proves it.

Prominent world renowned media organisation, The Guardian, has blown the lid after obtaining highly classified documents

The United States National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants (like Microsoft), according to a top secret document obtained by the Guardian.

The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says Read the full story at The Guardian

Only five slides from the presentation have been published. The other 36 remain a mystery. Both the Guardianâ€™s Glenn Greenwald and the Postâ€™s Barton Gellman have made it clear that the rest of the PowerPoint is dynamite stuff â€¦ which weâ€™re not going to be seeing any time soon.
Greenwald wrote on Twitter, â€œbut weâ€™re not publishing NSA tech methods.â€•
Gellman wrote on Twitter â€œIf you saw all the slides you wouldnâ€™t publish them,â€• adding â€œI know a few absolutists, but most people would want to defer judgment if they didnâ€™t know the full contents.â€•

One of the PRISM slides suggests NSA has international cable taps in South America, East Africa, and Indian Ocean (at least) offering up the rough location of NSA fiber optic taps on cables

World-wide disbelief and condemnation continues as U.S. President Obama's response to the revelations was This does not apply to US citizens and it does not apply to people living in the United States completely disregarding the privacy of the innocent citizens of the entire world who just happen to use US-based Internet services or have their traffic routed via the U.S. transiting to other parts of the world, I have long considered Asia and Europe's connecting paths favouring via the U.S. to be a horrible redundant-less idea, and more undersea cables between Asia Pacific and Europe are needed, and this is just one more example of why.

Australian Senator Scott Ludlam says â€œAustralians use these services to the point of ubiquity. Does the Australian Government believe it is appropriate that the US intelligence agencies appear to be engaged in warrantless realtime

surveillance of the entire online population?"

Opposition Communications spokesman Malcolm Turnbull has also been outspoken and demanded explanations from the U.S. Govt embassy reps in Australia saying â€œThese reports have potentially very significant commercial implications,â€• , â€œThere is a massive global trend to cloud services. The vast majority of the cloud service providers are US companies. These companies have, with US Government support and endorsement, been promoting their services globally, and have sought to allay concerns that data hosted by them would have less privacy protection than it would in Australia.â€•

â€œTodayâ€™s reports elevate those concerns to an even higher level especially since it has been alleged that foreign-owned data hosted by US Internet companies has lesser protection than data belonging to US citizens.â€•

Germany's federal commissioner for data protection said "Given the large number of German users of Google, Facebook, Apple or Microsoft services, I expect the German government... is committed to clarification and limitation of surveillance.

In addition, the reports illustrate the importance of strengthening the European data protection law. The dilatory attitude of the EU Interior and Justice Ministers towards the Privacy Policy reform package is a completely wrong signal.

The European privacy advocate, Alexander Hanff, is calling for the US's "safe harbor" status to be revoked. The European Commission's Directive on Data Protection went into effect in October of 1998, and would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU.

In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework and this website to provide the information an organization would need to evaluate -- and then join -- the U.S.-EU Safe Harbor program.

Sir Tim Berners-Lee, inventor of the World Wide Web, has released a statement about Prism on behalf of the World Wide Web Foundation calling Prism â€œdeeply concerning"

â€œTodayâ€™s revelations are deeply concerning. Unwarranted government surveillance is an intrusion on basic human rights that threatens the very foundations of a democratic society.

â€œI call on all Web users to demand better legal protection and due process safeguards for the privacy of their online communications, including their right to be informed when someone requests or stores their data. Over the last two decades, the Web has become an integral part of our lives. A trace of our use of it can reveal very intimate personal things. A store of this information about each person is a huge liability: Whom would you trust to decide when to access it, or even to keep it secure?â€•

The dissemination may also be more widespread than we first thought, the UK's electronic eavesdropping and security agency, GCHQ, has also been secretly gathering covert intelligence data shared by America's top spy agency. So, is Australia's ASIO, ASIS, or the incompetent clowns at DSD also privy to this information? Possibly not given the ties are not as strong as those with the U.K., but it does pose the question, who else?

Britain's spy agency GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA).

The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate.

One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.

GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely

innocent people, as well as targeted suspects.

This includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites â€“ all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets.

Personally I am less concerned about local authorities spying on me, hell, I pity the poor bastards if they ever decided to spy on me, they'd be bored shitless in no time, but what is a concern, far far far more of a concern is the fact a foreign government agency may also be doing the same.

I think a lot of questions need answers, and a lot of countries are now demanding them, since as you're surely aware, the likes of Google, Microsoft, and Facebook and others not only accept users from anywhere in the world, but also have data centres outside the U.S., and that data is also indeed subject to NSA surveillance since they are U.S. incorporated organisations.

We have all known for along time the U.S. government is completely out of control when it comes to demanding power and information, NSA procedures give a little insight, maybe this is why Hillary Clinton came to the aid of us aussies defending our right to not be censored when our own government tried to pull the mandatory inet filter crap, was it because it is in the U.S.'s best interest that we are not filtered, so they can see everything we are doing too, paranoia? Who the hell knows.

Is it any wonder why I don't place my users content in the U.S., I mean, sure, I might have a secondary and (not controlled by me) tertiary DNS server over there (like in EU), but good luck sniffing anything of interest out of that NSA Ohh, and no, I don't really use facebook, myspace, google+, gmail, hotmail, skype, or .... other privacy invading hordes like them. Twitter is extent of my social media really - nothing private about that, long live IRC!

I also must ask the question as to why mainstream media in Australia are not saying much about it? A 10 second snippet with Obama saying "hey we gotta do it, National Security" type bullshit, without mentioning anything about the actual affects or actions, like spying on world wide users emails and other personal content hosted in U.S. or by a U.S. company outside the U.S., kind of astounded me, not even a mention of Ludlam or Turnbulls outrage. I thought journos are supposed to rock the boat to keep the bastards honest? my bad - I must be wrong, or may it be they, like the current gutless labor government we have, are too scared to upset the bully boys in Washington.

...and to think the United States is outraged by China's attempted hackings and spying, well Obama, one thing comes to mind - POT KETTLE BLACK

Another little known Dangerous U.S. Govt Act is the Stored Communications Act, that classifies data older than 180 days as abandoned, this means it can be accessed at any time, without warrant or just reason, so if you thought those messages in your gmail or hotmail/live inbox's over 180 days old are covered by privacy, then think again, the U.S. Govt interprets this data as abandoned and can read to their hearts content.

I have previously wrote about cloud concerns before at

Avoid the cloud hype
Life without Facebook

So, maybe all those companies, governments and educational institutions conned into moving email to Gmail, or Microsofts Hotmail, Live, or 365, will now think again and do some real due diligence.

World renown security expert Kevin Mitnick has had much to say on Twitter about this, but one of evins recent tweets sums it all up nicely:

.... and I bet you though I was just another privacy paranoid, well... now who is laughing

Update
 "I don't want public attention because I don't want the story to be about me. I want it to be about what the US government is doing."

The individual responsible for one of the most significant leaks in US political history is Edward Snowden, a 29-year-old former technical assistant for the CIA and current employee of the defence contractor Booz Allen Hamilton. Snowden has been working at the National Security Agency for the last four years as an employee of various outside contractors, including Booz Allen and Dell.

The Guardian, after several days of interviews, is revealing his identity at his request. From the moment he decided to disclose numerous top-secret documents to the public, he was determined not to opt for the protection of anonymity. "I have no intention of hiding who I am because I know I have done nothing wrong," he said.

Snowden will go down in history as one of America's most consequential whistleblowers, alongside Daniel Ellsberg and Bradley Manning. He is responsible for handing over material from one of the world's most secretive organisations â€“ the NSA.

Read on for the complete story and video interview at The Guardian

Statement by Edward Snowden to human rights groups at Moscow's Sheremetyevo airport on Friday, July 12, 2013, at 15:00 UTC

Hello. My name is Ed Snowden. A little over one month ago, I had family, a home in paradise, and I lived in great comfort. I also had the capability without any warrant to search for, seize, and read your communications. Anyone's communications at any time. That is the power to change people's fates.

It is also a serious violation of the law. The 4th and 5th Amendments to the Constitution of my country, Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties forbid such systems of massive, pervasive surveillance. While the US Constitution marks these programs as illegal, my government argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair. These rulings simply corrupt the most basic notion of justice â€“ that it must be seen to be done. The immoral cannot be made moral through the use of secret law.

I believe in the principle declared at Nuremberg in 1945: "Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring."

Accordingly, I did what I believed right and began a campaign to correct this wrongdoing. I did not seek to enrich myself. I did not seek to sell US secrets. I did not partner with any foreign government to guarantee my safety. Instead, I took what I knew to the public, so what affects all of us can be discussed by all of us in the light of day, and I asked the world for justice.

That moral decision to tell the public about spying that affects all of us has been costly, but it was the right thing to do and I have no regrets.

Since that time, the government and intelligence services of the United States of America have attempted to make an example of me, a warning to all others who might speak out as I have. I have been made stateless and hounded for my act of political expression. The United States Government has placed me on no-fly lists. It demanded Hong Kong return me outside of the framework of its laws, in direct violation of the principle of non-refoulement â€“ the Law of Nations. It has threatened with sanctions countries who would stand up for my human rights and the UN asylum system. It has even taken the unprecedented step of ordering military allies to ground a Latin American president's plane in search for a political refugee. These dangerous escalations represent a threat not just to the dignity of Latin America, but to the basic rights shared by every person, every nation, to live free from persecution, and to seek and enjoy asylum.

Yet even in the face of this historically disproportionate aggression, countries around the world have offered support and asylum. These nations, including Russia, Venezuela, Bolivia, Nicaragua, and Ecuador have my gratitude and respect for being the first to stand against human rights violations carried out by the powerful rather than the powerless. By refusing to compromise their principles in the face of intimidation, they have earned the respect of the world. It is my intention to travel to each of these countries to extend my personal thanks to their people and leaders.

I announce today my formal acceptance of all offers of support or asylum I have been extended and all others that may

be offered in the future. With, for example, the grant of asylum provided by Venezuela's President Maduro, my asylee status is now formal, and no state has a basis by which to limit or interfere with my right to enjoy that asylum. As we have seen, however, some governments in Western European and North American states have demonstrated a willingness to act outside the law, and this behavior persists today. This unlawful threat makes it impossible for me to travel to Latin America and enjoy the asylum granted there in accordance with our shared rights.

This willingness by powerful states to act extra-legally represents a threat to all of us, and must not be allowed to succeed. Accordingly, I ask for your assistance in requesting guarantees of safe passage from the relevant nations in securing my travel to Latin America, as well as requesting asylum in Russia until such time as these states accede to law and my legal travel is permitted. I will be submitting my request to Russia today, and hope it will be accepted favorably.

If you have any questions, I will answer what I can.

Thank you.

Update Aug 9
If you ever needed more reason why it is dangerous to do business in or with a US firm, whilst the government of United States of America is completely out of control, and if the botched destruction of Megaupload with its vast majority of innocent users data wrongfully withheld from them, and its eventual destruction, overnight news from Lavabit must now present you with clear waters when it comes to protection of your data, including Email, and why you must never do business with a U.S. based company.

My Fellow Users,
I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know whatâ€™s going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

Whatâ€™s going to happen now? Weâ€™ve already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

So, 400,000 email accounts gone - all of them victims of the out-of-control US government.

Update Aug 19 2013

What can only be described as beyond despicably bullying, the UK Security Services, likely in direct partnership with the US Govt, has illegally detained and attempted to intimidate Greenwalds partner

At 6:30 am this morning my time - 5:30 am on the East Coast of the US - I received a telephone call from someone who identified himself as a "security official at Heathrow airport." He told me that my partner, David Miranda, had been "detained" at the London airport "under Schedule 7 of the Terrorism Act of 2000."

David had spent the last week in Berlin, where he stayed with Laura Poitras, the US filmmaker who has worked with me extensively on the NSA stories

Extreme abuse of powers

But they obviously had zero suspicion that David was associated with a terrorist organization or involved in any terrorist plot. Instead, they spent their time interrogating him about the NSA reporting which Laura Poitras, the Guardian and I are doing, as well the content of the electronic products he was carrying. They completely abused their own terrorism law for reasons having nothing whatsoever to do with terrorism: a potent reminder of how often governments lie when they claim that they need powers to stop "the terrorists", and how dangerous it is to vest unchecked power with political officials in its name.

Read the fulll report here

In his first interview since returning to his home in Rio de Janeiro early on Monday, Miranda said the authorities in the UK had pandered to the US in trying to intimidate him and force him to reveal the passwords to his computer and mobile phone.

"They were threatening me all the time and saying I would be put in jail if I didn't co-operate," said Miranda. "They treated me like I was a criminal or someone about to attack the UK â€¦ It was exhausting and frustrating, but I knew I wasn't doing anything wrong."

During that time, he said, he was not allowed to call his partner, who is a qualified lawyer in the US, nor was he given an interpreter, despite being promised one... read more...

Will it ever end...
One must wonder when this madness will ever stop, a reminder to the U.S and U.K, we have seen civil uprisings in many countries in past two years, don't think you are immune, people can see right this lame bullshit terrorism excuse, people have been seeing through it since your illegal invasion of Iraq with "they have weapons of mass destruction" bullshit we all knew to be false, so tell me, why don't other countries invade the U.S. - after all, the United States has weapons of mass destruction, who are they to be treated differently from a European or Middle Eastern country?

Lets look at history...
Hitler: Warmongering, murderer of innocent civilians, dictating, imperialist one world views.
Obama/Bush: Warmongering, murderer of innocent civilians, dictating, imperialist one world views.

So, where's the difference?

Why is the U.S govt not on trial for war crimes, as has been well published via Wikileaks, no-one forgets the video they exposed with the US military targeting civilians and having fun about it.

WHY are these U.S murderers not before the Hague? Please, someone explain it to me.

Update Oct 12 2013

U.S. Feds begged Washington Post reporter not to name companies involved with PRISM because they were worried they'd stop cooperating.

The thing that the government most wanted us to remove was the names of the nine companies. The argument, roughly speaking, was that we will lose cooperation from companies if you expose them in this way. And my reply was "that's why we are including them." Not in order to cause a certain result, or to get you to lose your cooperation but if the harm that you are describing consists of reputational or business damage to a company because the public doesn't like what it's doing or you're doing, that's the accountability we are supposed to be promoting

U.S. Patriot Act co-author says James Clapper should be fired and prosecuted and plans Law code named The Freedom Act, to stop NSA overreach.

Congressman Jim Sensenbrenner, who worked with president George W Bush to give more power to US intelligence agencies after the September 11 terrorist attacks, said the intelligence community had misused those powers by collecting telephone records on all Americans, and claimed it was time "to put their metadata program out of business".

Mike Rogers isn't overseeing the Intelligence Community, he's conspiring to cover up its activities Mike Rogers, the head of the House Intelligence Committee seems to have gone out of his way to withhold information from Congress.

Read more at The Guardian.....

Update Oct 27 2013

German spy chiefs will travel to the United States next week to demand answers following allegations that US intelligence has been tapping Chancellor Angela Merkel's mobile phone, as a row over US snooping threatened to hurt transatlantic ties. But the furore has intensified further after allegations that world leaders including the presidents of Brazil and Mexico have been among spying targets.

"Spying on friends, that's just not done," Chancellor Merkel said

Germany and Brazil are also working on a UN General Assembly resolution to highlight international anger at US data snooping in other countries, diplomats said Friday.

The resolution would not mention the United States (It should though, and should name UK's GCHQ as well) but would call for extending the International Covenant on Civil and Political Rights to Internet activities.

"The aim is to send a message to those who abuse the system," said a UN diplomat involved in the talks.

The Bavarian daily Suddeutsche Zeitung meanwhile suggested that France had an ambiguous role in international surveillance, having signed an accord with the "Five Eyes" grouping of Australia, Britain, Canada, New Zealand and the United States whose members share virtually all intelligence -- and have pledged not to spy on one another. (yeah right, like that doesnt happen)

Thousands of Americans marched Saturday, October 26, in Washington DC to protest the out of control power tripping U.S. Govt mass surveillance program, former NSA contractor and whistleblower Edward Snowden had a statement read at the â€œStop Watching Usâ€• Rally read by Justice Department whistleblower and attorney with the Government Accountability Project, Jesselyn Radack.

Snowden says:
In the last four months, weâ€™ve learned a lot about our government. Weâ€™ve learned that the US Intelligence Community secretly built a system of pervasive surveillance.

Today, no telephone in America makes a call without leaving a record with the NSA. Today, no Internet transaction enters or leaves America without passing through the NSAâ€™s hands. Our representatives in Congress tell us this is not surveillance. Theyâ€™re wrong.

Weâ€™ve also learned this isnâ€™t about red or blue party lines. Neither is it about terrorism.

It is about power, control, and trust in government; about whether you have a voice in our democracy or decisions are made for you rather than with you. Weâ€™re here to remind our government officials that they are public servants, not private investigators.

This is about the unconstitutional, unethical, and immoral actions of the modern-day surveillance state and how we all must work together to remind government to stop them. Itâ€™s about our right to know, to associate freely, and to live in an open society.

We are witnessing an American moment in which ordinary people from high schools to high office stand up to oppose a dangerous trend in government.

We are told that what is unconstitutional is not illegal, but we will not be fooled. We have not forgotten that the Fourth Amendment in our Bill of Rights prohibits government not only from searching our personal effects without a warrant but from seizing them in the first place.

Holding to this principle, we declare that mass surveillance has no place in this country.

It is time for reform. Elections are coming and weâ€™re watching you.

Update Oct 31 , 2013

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA does not keep everything it collects, but it keeps a lot.

According to a top-secret accounting dated Jan. 9, 2013, the NSAâ€™s acquisitions directorate sends millions of records every day from Yahoo and Google internal networks to data warehouses at the agencyâ€™s headquarters at Fort Meade, Md. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records â€” including â€œmetadata,â€• which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

Read the report at The Washington Post

Update Dec 2 , 2013

A senior IT official has left open the prospect that parliamentary communications in Australia could be monitored by US intelligence through a â€œback doorâ€• provided by Microsoft operating systems.

Eija Seittenranta, who is responsible for ensuring network security in Australiaâ€™s parliamentary IT systems, told the Senate finance and public administration committee on Monday that no specific action had been taken to secure the parliamentary network against surveillance by US agencies under the Prism program.

â€œNo we wouldnâ€™t have taken any specific actionâ€• Seittenranta told the committee.

Greens senator Scott Ludlam asked Seittenranta whether, given that answer, Australian MPs and staff should assume their IT communications were exposed routinely to intrusion.

She replied: â€œYes, I suppose you should be able to assume that. It probably should be noted that our network is not a protected network, it is unclassified.â€•
Full story at The Guardian

Update Dec 6 , 2013
Amongst the almost daily revelation of the American power crazed Govt and NSA, today, Ed Snowdens release shows that the United States of America's NSA considered spying on Australian citizens without the knowledge or consent of the Australian intelligence organisations it partners with, according to a draft 2005 NSA directive kept secret from other countries.

The draft directive leaked by the US whistleblower Edward Snowden reveals how the NSA considered the possibility of "unilaterally" targeting citizens and communication systems of Australia, New Zealand and Canada â€“ all "5-Eyes" partners which it refers to as â€œsecond partyâ€• countries.

Under certain circumstances, it may be advisable and allowable to target second party persons and second party communications systems unilaterally when it is in the best interests of the US

The draft 2005 directive, which was published in the Guardian in November, goes on to state that the U.S. could conduct the targeting without the knowledge of Australian, Canadian or New Zealand authorities, and even if the countries had rejected a "collaboration proposal" for the operation.

Read the full story at The Guardian

Update Feb 28 , 2014

Well, I stopped updating this because I just don't have the time to add to it every day, and since The Guardian does the

perfect job with its Edward Snowden NSA Files releases there's little point I think, but, today's release is worth a mention, the amazing story of breach of innocent users privacy, through recording data off webcams, and although this report names from intercepted Yahoo sessions, well, you know what they say, if there's one, there's a whole lot more!

Between 2008 and 2010, Britain's GCHQ, in cooperation with the U.S. National Security Agency, ran the "Optic Nerve" program which covertly intercepted and collected webcam imagery from more than 1.8 million Yahoo user accounts globally

Images were taken as often as once every five minutes, a limit issued to avoid overloading GCHQ systems, as well as to "partly comply" with human rights legislation.

As much as between 3 percent and 11 percent of the snapped imagery was considered "explicit."

Such blatant disrespect and wholesale abuse of power, puts repressive regimes in communist dictatorship led countries to shame, makes them seem like angels compared to the out of control UK and US governments and their spy agencies.

Read on over at The Guardian for full story.

Q.How many terrorist plots have been foiled by the NSA with this massive blanket surveillance?
A.None!

Posted by NoelB at 11:47

Sunday, March 3. 2013

Why Windows XP users need to dump Internet Explorer - NOW!

Here we are in the year 2013, and Microsoft's incompetence (or is it arrogance?) still continues to astound me. We are now (and have been for nearly twelve months) at a stage where the normal age-old Internet Address ranges are depleted, yes, they have now pretty much run out of IP addresses all around the world, most regions will no longer issue any more IPv4 addresses to existing organisations, and new organisations are severely restricted in how many they can obtain - because there are little to none to give out. The problem of IPv4 address depletion has been solved for some time by the new IP address scheme, called IPv6, however, at present less than 1% of the world is using IPv6, many service providers, businesses and governments are moving that way, albeit very slowly, and there is going to be serious problems in the near future.

I'm not going to go off on a tangent like many of the IPv6 fanboi's do, and lets face it, they have been crying wolf since late nineties about running out of addresses within two years, when that was never the case and time has proved that, so they have no-one else to blame but themselves for the slow take-up of IPv6 today but now it is essential that all service providers, businesses, and governments stop delaying, and start configuring their entire networks for IPv6 - especially the service providers with end users, where here in Australia,
only one of the top ISPs is doing anything about it, the top three ISP's with the vast majority of users, are not, of course when you have a million users or so it's not something you can do overnight, but there is no excuse for not having started the roll out at all, after all, it's going to be your helpdesk staff flooded with tickets about unreachable sites if you don't.

It is a known fact however that IPv4 will continue to be around for a very long time yet, I personally think it'll be perhaps mid 2020's by the time it is completely withdrawn from use, because of this, and the slow take up on IPv6, there will be a lot of reachability problems if networks don't roll it out quickly, and we'll start seeing these problems by next year.

To get around reachability problems, hosting web sites will do what's called dual stack, it means each server will have an IPv4 and an IPv6 address, in shared hosting situations (the most common method), this is fine, since you can put many thousands of websites on one single IP address, limited only by the ability of your hardware, allowing for bursts and the unexpected, two or three thousand websites per industry standard rack server would be common, some may handle less, some more.

However, even in shared hosting, this all changes with secure websites (those with https://), traditionally, SSL sites have been one host per IP address, this is because of the way the web server, SSL, and certificate matching works, it finds the first or best match, any second host attempt is regarded as a possible tampering (man in the middle attack) and results in a failure to view the website.

To get around this, in 2004 an extension to the transport layer security in OpenSSL was developed called Server Name Indication, or commonly known as SNI, this allows, identically like non secure shared hosting, one IP to host multiple secure web sites, but, for all this to work, the client software (your web browser) must also support SNI, and this is where the problem exists.

Most web browsers that have been released or had any sort of maintenance in the past 5 years or more have supported SNI, except of course for one well known, and heavily used browser, Internet Explorer. Microsoft did however resolve this for users of IE 8 onwards but only for Vista, Windows 7 and above, not XP, which is the real issue here, the most commonly used Windows operating system today by around 75% is still XP, which today, still receives updates, but apparently Microsoft would rather tell you buy an upgraded operating system like vista/win7, than fix IE on XP. The annoying thing is, SNI has been supported as general availability for more than five years, back in the days of Mozilla 2, it's even supported on old linux browsers with no support for years now like Epiphany and Galeon since 2006, even the text based browser lynx can support SNI, as well Internet Explorers prime competition - Firefox and Chrome.

What all this means is that service providers who run out of IPv4 addresses, will have to start using SNI for SSL sites to be reached by IPv4 users, resulting in XP users using IE that do not have an IPv6 address, getting failures and unable to access those SSL websites. Now, it's not entirely just Microsoft here, Apple's Safari (or perhaps this is because it links into the XP operating system the same way IE does) on XP (but not on Mac's since v3.0) will also fail, as will java prior to 1.7 (you really aren't going to admit to using that are you?).

The only way around this for XP users is, no, not to go out and spend a couple hundred dollars on a Windows OS upgrade like certain official Microsoft staff bloggers (@EricLaw) would suggest you do, but spend a minute to download and install Firefox or Google's Chrome, the cheap, as in free, and immediate resolution to the problem.

Is it a fact that Microsoft care more about their bottom line than customer loyalty? Don't think for one moment this wont affect you, what if you start a small business in two years time and want a shopping cart? You'll need SSL! What if your desperate for that one special item that can only be bought at one online shop, from a secure shopping cart, on a server using SNI. Perhaps you should let @Microsoft know you're not happy and that they should fix the XP SNI problem. Despite Microsoft's wishes, XP is not going to go away any time soon.

Posted by NoelB at 14:19

Friday, November 16. 2012

Open Letter to the Governments of the world and the ITU

In a few short weeks, from December 3 to 14, the ITU will meet to decide the Internet's as we know it today, future. They want to take over full control, deciding on regulating it, what we can see or can't see, how companies must stop supplying access in some cases (PIPA, SOPA etc anyone?) and more importantly, introducing government access fees for carriers, which will drive up the cost of Internet access for everyone, those are just some of the ideas, with censorship being the huge one of course, and dictated by communist countries, so how do people in say for example Australia, the United States, United Kingdom, and Germany like being told the type of content they can or can not access by the likes of Iran and China... The words I have for that are legally unprintable!

ITU participants (representatives of each of our own countries governments) need to hear from as many Internet users as possible to voice their opinion in stopping more madness Internet control madness.

Sign the petition here

You can watch this short video to understand more about why this is a bad thing...

Below is a copy of my submission.

Dear Sir / Madam,

At the upcoming WCIT conference in Dubai, governments will consider proposals to update the ITUâ€™s underlying treaty.

Some proposals would expand the ITUâ€™s mandate in ways that would likely threaten Internet openness and most importantly innovation, increase access costs, and erode human rights online.

Recent events of only this past year, proves how invaluable a free and open Internet is, in playing a very major part in ridding the world of more tyrant dictatorship governments to allow for their peoples to make an independent and free choice in electing a peoples government, not a countries jailer.

Having the likes of Iran, China, Russia and other certain countries, who have harsh penalties for those who disagree with or speak out against their governments, deciding on our Internet access is a grave concern to me and many others, do we really want the Great wall of China, to become the Great wall of the world? One only has to watch nightly news services to see why this is horrible and should never have been dreamt of let alone put up for a vote.

The internet is powerful tool for communication, driving economic development, and expanding human rights. The internet has got where it is today in democratic societies having been built by private companies, using private funds, only those companies have the right to decide who or how or where they send their own networks data and how they accept data.

Discussions about the future of the Internet should involve as many stakeholders as possible including government officials, technology experts, businesses leaders, civil society, and human rights organisations.

I write to ask that you:
-Reject proposals at WCIT that would expand ITU authority to areas of Internet governance especially those that affect the exercise of human rights online;
-Release to the public proposals that our country or other countries will make at the WCIT; and

-Solicit input from your citizens and experts on proposals, including by inviting a range of stakeholders to participate in our countryâ€™s delegation.

The ITU has done good in the world, and I applaud those efforts. But I join a chorus of voices from around the globe, however, who feel strongly that the Internet must always remain a free and open access to anyone, any and every where.

Posted by NoelB at 13:04

Friday, September 21. 2012

Have ICANN Lost The Plot

ICANN are considering the introduction of Dotless Domains, basically, this means, instead of, for example entering in http://blog.ausics.net, I could buy ausics and you only enter in http://blog.ausics or http://ausics

Now, some of you might think that's a cool idea, but NO, it's not! What about host names on LAN, I have a box called fox (no pun intended, well, ok, maybe) so, if I http://fox, I want my local fox, not someones domain, http://fox the use of hostname in local lookups (search lists) in place of FQDN, has been used for near eternity on PC's.

It could not be one of the more crazy and stupidest moves by the hierarchy yet, for reasons I explained in my submission (below)

I really recommend those in a system or network administrative position to have a read of ICANNS RFC, and submit their opinion on it, one of the more vocal voices against this, is more or less Mr DNS himself, Paul Vixie who wrote about it last year.

Regrettably, you have only a couple of days, submissions close Sept 24 2012....

The following is a copy of my submission.

Dear SSAC Members,

As an Email administrator, this is a horrible idea, much of the anti-spam measures in use today use this as one of the most basic of tests, given a lot of machines, mostly malware infected, connect using helo somemachinebriefname , they can be rejected outright there and then.

If dotless domains become a fact of life, MTA's, and anti spam software will become much less effective, or, and the more likely scenario, is that the legitimate dotless domain messages will be blocked, through fault of the MTA server, the anti spam measures, or the "if it aint broke don't fix it" attitude many admins and businesses alike have. Even if this was to be so, there are rightly or wrongly, many ancient unsupported mail transport agents out there that, as unsupported, will never be modified to allow dotless domains. Even those that are, may take years to do anything about it, just have a look at how many servers out there that are running such old software that barf at looking up an SPF resource record, and sadly, many of them are on large busy networks.

The affect of this will be like ISP's blocking all inbound port 25 to residential customers so they can not run a mail server, but allowing business customers to do so, whilst putting those business class customers in the residential (blocked) pool.

Another detrimental fact is with internal sites, and those who use aliasing in their hosts file, take "foo" as an example, lets assume foo may now be a new legitimate domain, foo, may also be an internal hostname of a network, as in foo.example.net, aliased in a search/domain entry in *nix, or a windows equivalent, in this case, foo is treated as local, and the external domain wont be as easily accessible , if I ssh foo, I not only want, but expect it to be that local host (foo.example.net), and not someone else's domain, where I may start setting off alarms for "why is this person trying to gain access to our machine, are they trying to hack us" etc etc etc.

The cons outweigh any possible pro's, and the only pro I see, is for a domain to grandstand, really, I mean, people do not care if its address is http://icann or http://icann.org , to use as an example.

I consider this a terrible, even ridiculous idea to consider, and ask that you keep the status quo which works very well and will not cause problems or dramas that will be felt for many years if this is approved.

Posted by NoelB at 06:31

Wednesday, September 12. 2012

How redundant is your network, really?

The well publicised GoDaddy outage on Sept 11 this year should be a huge wakeup for everyone to find out, just how good their network is designed.

So, you have multiple data links to multiple carriers, redundancy, failover, the works, even a wireless/microwave link in case someone digs up the entire block including your fibre. You've also got dual power supplies in your routers, switches, and servers, even redundant routers and switches, they are all protected by dual channel mains supplies, each with their own dedicated UPS and battery bank, both connecting into the power company by two separate diverse paths, backed up by two mega powerful diesel generators.

You can go to bed tonight and sleep easy can't you... Or, can you?

A bored shitless teenager, after getting banned from some gaming server on your network, has decided to seek revenge, so initiates a more, real life battle, he attacks the name servers that host the game server network since they may be slightly easier to take down, than the actual server.

Most kids don't care about collateral damage, then again, maybe they are smarter than many give them credit for, attacking the game server, only peeves off the gamers, attacking and taking out DNS peeves off the network admins for affecting the entire network, that would be a quick way to having the ISP kick off the game server, and with word of mouth, that game network soon becomes known as a high risk target, and may find it very hard to get another network to stick their gear in.

OK, back to our story, so, your primary DNS server 10.1.1.1 is massively DDoS'd, but wait, your secondary slave server should respond and save the day, so no problems, right?

Oh, you umm, what? You made 10.1.1.2 as your slave DNS server? So, both your primary and secondary DNS servers are in the same /24 netblock route path... and you wonder why not only is the game network status tango down, but so is your domain, and the domains of every single customer on your network, yes, every single one of them, all because you ignored DNS 101.

Lets not laugh at the above scenario, it happens all too often - as GoDaddy just found out, still, not as much as it could though, and that's mostly because most of us are not targets at all, let alone high risk targets. It is allowed to happen because some network operators just chuck it all together and hope it works and stays working, if you have two or more diverse paths, use them to your maximum advantage.

Default route and prefer for example 10.1.1.0/24 via Link A, so your primary name server along with any other critical stuff like mail servers and company web site will always use link A for internet traffic.

Then default route and prefer 10.1.2.0/24 via Link B your secondary name servers, your secondary backup MX mail server, and whatever else is secondary importance, then let BGP use best path for all other ranges.

Ideally your BGP configuration would be such that if one link is down, the other takes up slack. find a BGP expert to help you there, trust me, I'm not one

Further to this, it's also advantageous to have additional slaves (and secondary MX's) geographically located, if you're a national network with PoP's in different states, that's good enough, but personally, I prefer my external DNS slaves in another country, for instance, my private domain has slaves in the U.S. and U.K, and I have been considering adding a third slave, which will be in Frankfurt, Germany, (given it's fast becoming a European super hub), so now I'm pretty much covered.

There is no reason a service provider can not also do same, dedicated servers, in well known and reliable overseas data centres, will pay for themselves in no time.

One thing I do see a lot of these days, with VPS's becoming cheap, a lot of people go register a domain, get a VPS host which is issued with only one IP address, then in their registrars settings they set ns1 and ns2 to the same damn IP on

the same damn server, seriously? I mean, WTF? If your only copy of bind exits (because you're probably running a debian or centos image that's so old and outdated using exploitable versions of softwares), or your VPS goes belly up, even with an external secondary MX configured, how the hell do you expect DNS lookups to succeed to lookup the mail backup I'll never know. Folks, this is DNS #1, never ever do it, its worse than putting both separate servers in the same immediate IP range.

There are services out there that offer secondary NS/MX services, google them, hell, I'll even do it for you for free if we have ever met, MSN'd/IRC'd/Tweeted/emailed, or even friended on fuckbook facebook, (OK so that's not so likely given I rarely use it given my dislike of that privacy invading cesspit of a ...REDACTED FOR LEGAL REASONS...) and, of course, if you're nice to me

If you screw up your DNS, your vanished off the face of the net, and unreachable, if not immediately, within 24 hours, which is the typical TTL (time to live) for DNS records. Some however use less than 24 hours, those using cheap load balancing methods may set Zero on the record for your MX servers, and require DNS to be available at all times for mail to succeed. You should also never allow your server to be an open recursive server, serving anyone, this can introduce local cache poising risks.

DNS is not something to be taken lightly, if you do not understand it, don't touch it at all, or, be prepared to spend a good few hours and learn it, it's not really that hard, but be warned, there is much, much wrong and outdated information found via search engines, too many blogs are written by people with three hours experience, and a hell of a lot of assumptions and guesses.

Posted by NoelB at 21:14

Monday, July 30. 2012

Ethernet Cabling - It's Easy

What is contained within, may in part, in Australia, be illegal - No, I'm not talking about bomb making, I'm talking about... home ethernet data cable work, be it patch leads, or running between sockets in different rooms....

So, you're wondering, WTF? Well, yes, if you do data cabling work, even in your own, owner-occupied home, you must not only be a an open registered cabler, but you must also have structured cabling endorsements.

Where I disagree with this however is being illegal for you to cable up a couple of rooms in your own owner-occupied home for data to access the Internet, you're not going to hurt or affect anyone else, but our nanny government has decided that's tough luck, the previous Digital Data Exemption that allowed this is completely gone with a rewrite of The Rules so you can't!

That aside, if your cabling a network that doesn't, and can not have access to the telecommunications network in any way shape or form (incl wireless, 3/4G, Cable, etc), in other words is a 100% intranet, then the law does not apply, because it is not regarded as "customer cabling", and you can do what you want, and we will assume that's the case here.

So, I am going to assume you like having LAN parties and will have no internet connection for the LAN you are about to construct for those LAN parties, this way, the network cable stuff you're about to do, is actually legal Also that you are a pretty good home handyman with experience using dry wall saws, power tools, understand that electricity can kill you, you might get bitten by redbacks and have to fight off possums (among other creepies) crawling around your roof and wall spaces - If your not this type of person, best hire a registered cabler with the appropriate endorsements to do it all for you!

Again, if you have even the slightest hesitation about your ability to do the job, leave it for a professional!

Under NO circumstances are you to access, alter, tamper with, or infringe upon, the phone network! The phone network is very complicated and sensitive, the slightest wrong thing can alter the resistance and capacitance causing anything from massive broadband drop outs, to the inability to receive or make phone calls, many other factors are involved, and unlike ethernet for your home LAN, there is constant voltage on phone lines, and a zap will let you know it too, especially if someone rings you whilst your tinkering, and although not normally a fatal level of current, you'll still know you were hit (those with weak hearts or medical conditions, may however risk seriously injured or even death).

if you need another phone extension, replace a broken socket or wire, need to move your outlet, or any work with relation to the phone network including its cabling, or, you need a data network with Internet access, you must seek out a registered cabler with appropriate endorsements to do that work.

The ACMA will prosecute you for tampering with the phone or data network - you will get a permanent criminal record for life as it is a criminal offence unless you're a registered cabler

So, if you understand the risks of doing your own data cabling, and that I provide this for non Internet based purposes, read on...

If you were to google or youtube for how to make ethernet patch leads or wiring, you might be confused by the different colour code pinouts used in examples, because most, but not all examples, are from Americans, who use a different wiring pinout standard than pretty much the rest of the world does like here in Australia, the U.K., and so on.

Although both methods are technically valid, the standard type Americans and a couple of Eastern European countries tend to use is commonly known as T568B (orange wires first) pinout configuration (don't confuse T568B to be a better standard, it's not, it's just an old AT&T method, in fact, any cable installers doing cable work in any U.S. Government building even in the U.S. must comply with U.S. Federal Government publication NCS FTR 1090-1997, which only recognizes designation T568A)
The only time we would use a T568B pinouts is when we need to make a cross-over cable for directly connecting two PC's together without a switch or hub, this is where one end is T568A, and the other is T568B.

In order to do a good job, you need a decent pair of scissors, a cable crimper for the plugs, and although not necessary, a handy little gadget to have is an ethernet cable tester. I got both my current cable crimper and ethernet cable tester from Jaycar back in around mid 2006 after I parted ways with my employer at the time and found I needed to crimp a few cables, and they're still going strong, perfect for the hobbyist, and probably even the pros, the crimper especially, couldn't break that bugger if I tried!

Warning/Update: You likely have noticed that you can get these tools for only a few bucks these days from China on Ebay, from what I've seen, you get exactly what you pay for, and it aint much, peoples biggest gripes are the cheap crimpers don't work, they crimp some but not all pins, some don't even line up right, the cheap strippers mutilate more than strip, and so on, so pay a little more and get something decent that works, you don't need to get the stuff that the pros use, but even the cheap stuff at Jaycar or Bunnings will do a good job for the occasional handyman.

You can get the connectors, jacks, and cable from Jaycar, DSE if your in a hurry, and most decent electronics stores, shop around though, some are criminally over priced, same with decent cat5e or cat6 cable. If you're not in an urgent (like you need it right now) hurry, I recommend checking out 4cabling or TTServices, my orders are normally next day delivery. Regardless of where you look, don't fall for the sales pitches in retail stores, the cheaper cat5e is perfectly fine for gigabit speeds, in fact you'll get 10gb out of it up to about 30-50 metres, and Cat5 is a lot cheaper and less finicky than Cat6 too.

Cables and Connectors

The connectors used for ethernet plugs are called 8p8c's (8 pin, 8 connector), or more commonly called RJ45's, they are an 8 position modular connector that looks kind of like a large phone plug (although some telcos now use them on phones as well), and please keep in mind phone jacks are different in telecomms, if you use a smaller RJ 11/12 connector in an RJ45 socket, yes, it will in most cases work fine, but you can damage the internal pins, so if you come to need to use the larger 8P8C/RJ45, you'll likely have problems.

There are two different types of cable, solid and stranded, if your making a lead that's to be run through the roof or walls, and is not going to be moved, then use solid, and if you're just making patch leads, then only get stranded. As for brand of cable to use? Well, I've used a lot of Belden cable in times gone by at a previous ISP when we bought boxes (come to think of it we got our connectors off them too), and in recent times since I've never needed bulk cable buys, I've just used patch leads, cable rolls, connectors and sockets from 4cabling or TTServices since then.

Update/Warning: I've seen some really shit error prone links because people have bought cheap flimsy non compliant cable off Ebay thats sheath is as soft as cotton friggin wool, its too soft and very prone to damage, no doubt would be a dangerous chemical fume situation if there was a fire, the junk would melt like butter too, it clearly didn't have the required twists so is passed off as cat5 when it would probably fail as cat3 even, and this mob couldn't understand it when I told them I'd have to rip it all out and replace it. In other horror stories, I've seen some trying to pass off CCA (copper clad aluminium) as certified Cat5, which is bullshit, the Cat5/6 standard for solid core is 100% copper, and almost as scary as earlier situation, CCA "melts" easy, yes, aluminium has a very low melt point, where copper does not, so do you really want to a hundred meters of that junk powering bunch of PoE devices? So please, only buy it cables from reputable suppliers.

Same goes for Connectors, pay attention as to if the connector is intended for stranded or solid wires. For braided/stranded wires, the connector has sharp pointed contacts that pierce the wires. The solid has finger like prongs that cut through the insulation and make contact by grasping it from both sides.

Don't really worry too much with the plugs, most stores only sell the one type and that's for stranded, since solid is typically in-wall and not carried by a lot of places. The only issue with mismatching plugs is tension strength, but heck, it's not likely you're going to be bungy jumping off the darn things is it, well... I certainly hope not

Here is a diagram and pin out of both a plug, and a jack, note the position of pin 1...

OK, now for the exercise itself....

First, memorise the colour codes order, remember, we are using the T568A standard so green pair is first.

Patch Leads

Strip off about 2 inches of the outer cable sheath.

There are four pairs, you now need to untwist each pair, only back to the sheath, don't try overdoing it with untwisting back inside the sheath, they are wound the way they are for a reason, to avoid what's known as crosstalk.

Align the coloured wires according to the wiring diagram for T568A (above), sometimes bending up and down a few times can help, but don't over do it!

Trim all the wires to the same length, about 1/2" to 3/4" left exposed from the sheath.

Now comes the fiddly bit, and if you have never done this before, go do some tai chi or yoga for an hour first No really, I mean it, I'm serious, trust me, you'll thank me in the long run, hehe - patience and a lot of it is needed when learning this process.

Insert the wires into the connector. Make sure each wire is fully inserted to the front of the connector and is still in the correct order. The sheath of the cable should extend into the plug by about 1/2", kind of under the little inset part of the top side of the plug. If when you have the wires all the way in the plug, your sheath is outside of the plug, and you see exposed colour coded wires, they are too long, and you need to trim some more length off the wires, note how many mm/cm of coloured wires you see, carefully slide the wires out, position your fingers right you'll keep them in order still, and nip off that extra bit of length.

Place the connector into the crimper, use gentle force to keep the little buggers in place and firm, then crimp all the way down with even force using the crimper tool, give it a couple of crimps to make sure, then, gently from the other side of insertion, push the connector back out, give a slight, gentle upwards pull on the little lever, that gives it the click you hear when locking when you push the plug into a device.

Verify the wires remained in the right order and that all the wires extend to the front and make good contact with the metal contacts.

Now repeat the above steps on the other end of your cable.

When completed, if you have an ethernet cable tester handy, verify the continuity of each wire (don't panic if the ground doesn't match anything though, that is normal with most cables in the wire map test unless you have shielded cable).

Fixed Cabling

Wiring cables from jacks to jacks is much like patch leads, in fact, It is much easier, since most jack inserts have both of colour codes on them, making it easier to know what goes where, but remember to use the right standard, T568A as shown at left, and, there's no fussy struggling to get the wires in and keep them in, the right order stuffing them into something you can't really see.

The equipment you need here is a good pair of scissors, and a punch down tool, don't fret, you can get them cheap at Jaycar, for home handyman stuff, get the 110 type, you can pick these up for around ten dollars, DSE even sell small disposable ones for a few dollars less, but I recommend searching for better ones, and don't pay ninety dollars for one either, they are for the pros who need to do this hundreds of times every day of every week of every year, you do not need to go to that extreme.

Before we go any further, some important things to remember...

Be generous with cable, finding you only have 28.5m when you need 29m is not fun!
Leave at least 50cm extra cable each end, and an extra 1 or 2 mtrs half way.
Don't run data cables parallel to electricity cables unless separated by wall stud.
Don't install your wall plate within 15cm of the centre of a nearby power point.
If you need to loop the cable, keep the loops no tighter than 10cm.

When securing cable bundles, use velcro strips not cable ties.
When securing cables to rafters or walls, use cable clips, not staples.
Most cables (like me) don't like powerful ultraviolet light, if you must run cables externally, use conduit (4mtr or so of 20mm is about $4 at Bunnings).

Loop (widely) the excess you left in the centre, and tuck away the excess 50cm or so at each end in the wall cavities, why all this extra cable you ask? Well, you need room to work on the connectors don't you, and you may at some stage need to move one end, having the extra in the middle allows for this, and lets not forget that the most expensive cable in the world, is the cable that's not long enough!

Again, like patch leads strip about 2 inches of the cables sheath, untwist and separate the four pairs then align each of the coloured wires according to the T568A layout of the jack as the above image shows.

When inserting the wires into the jack, place the sheath part of the cable hard up on, or slightly into, the jack as shown at left, this keeps the twisted wires as close to the jacks contacts as possible, if when you are done and you house the jack you can see coloured wires outside the jack, start again.

When done, use the punch down tool to insert each wire into the jack, it doesn't mater if your wires are long over the edge of the jack, the punch down tool will make the wires connect and cut off the excess.

Crossovers
As I mentioned earlier, T568B, is used with T568A when you need to make a crossover cable, so you can directly connect two PC's without a switch/hub, if you need to make one of these, below is the wiring colour code layout for the "B" end...

So hopefully now you understand what's involved, and you have a lot of fun doing it!

Posted by NoelB at 21:37

Tuesday, May 1. 2012

IRC - The online hangout before, during, and after, facebook

Internet Relay Chat, or IRC as it is commonly known as, was the first and original open access public multi-user chat (excluding unix "talk"), yes kiddies, the Internet's old hands were publicly multi chatting long before ICQ, MSN, and well before privacy invading predatory sites like facebook were even dreamt of, in fact, back as early as 1988, and it's still a very active social outlet today, yet, rather unjustly, doesn't get the attention it deserves, perhaps this is a good thing, it's not like IRC is just for elitists these days, it hasn't been that way since the nineties, but it has its loyal fanbase, and contrary to popular belief, not everyone thinks facebook is the "in thing", nor will it ever be to many, if you want to make public comments, set up a blog, or share pictures for anyone to see that's archived for life, there's always your blog, or twitter.

Sure, there is a difference, facebook and the like record what you say, even if you do not save it, and shows it and your shared pictures to almost everyone at any time and kept indefinitely, refusing to actually delete anything, only hiding it, override your rights by claiming copyright ownership on everything you post, let people know when your away so criminals can break in and clean you out, let the world know all about you, so you can become a high risk target of identity theft - well there ya go, facebook does have its purposes afterall . IRC on the other hand, is a real time multi user chat service, you need to be there, there and then to see what's being said, your private messages go nowhere but to the recipient, your public messages for all in the channel, but not logged by the servers, and one other thing I really love about it, is there is no in your face constant server sponsored or paid spamming of advertisements occupying three quarters of your bandwith.

IRC was originally created by Jarkko Oikarinen to replace a chat program called MultiUser Talk used on a BBS (Bulletin Board System) back in 1988, it also quickly replaced the old unix talk program, which became horribly messy with only a mere few users at the same time. Although IRC was assigned port 194 TCP by IANA, IRC servers have always run on TCP port 6667, it was common for some larger networks to also use 6668, 6669, and others as well. The reason they have always used 6667 instead of their officially allocated port, was to avoid having to start the IRCd software with root privileges, which was, and always will be, a very dangerous thing to do. Oh, and in case you are wondering, yes, many of the popular IRC servers like ircu are designed to be IPv6 capable.

IRC is an UN-MODERATED medium, meaning its more or less a free for all and anything goes, but most IRC Servers will have policies, you can view these by typing /motd, normally they are just common sense rules. IRC is also really easy to use, there are clients for any Operating System, Linux, Mac, Windows, and so on. There are also some networks or providors like mibbit that offer Web access to some networks, I do offer a word of caution on using Web based chats, including mibbit, well, they are Web based, therefore, they are not a server, they are a remote client as far as the IRC servers are concerned, and like with most local clients, they do offer a way to log all chats that you are involved in, so should probably be avoided at all times if you value your privacy, most real IRC clients do not take up much disk space at all anyway, so I highly encourage you to use one (see below).

Most IRC servers do not require users to register an account, but you'll need to choose a nickname to be known as when connecting. I'm not going to re-invent any wheels here, this is not a blog about every aspect on learning and using IRC, so for beginners, a suggested read is the Undernets Beginner class. When you're ready to try out IRC, you should pick a small Network at first for you to play around on until you get familiar with how it all works, then try chatting on smaller channels if you do not know anyone or can't get your friends to join you for some fun. Everyone needs to learn to crawl before they can walk, something most experienced IRC users (like almost anything in life) seem to forget, if a newbie enters a busy channel, they may be eaten alive

There are a myriad of servers and networks in operation in many countries around the world, most IRC clients have a server list that contains some of the more popular servers to connect to, in our example we'll use auschat.org, a small, quiet, and private IRC server originally set up for a few friends to chat on without mass interruptions but is open for anyone to use, so if you're a newbie (or old hand looking for a quiet place to chat), you can use that server to play around and get familiar.

So lets say you want to connect to auschat IRC server, your nickname (alias) used will be Nobby, and you want to join channel wasteland, type:

/server irc.auschat.org

Posted by NoelB at 19:46

Friday, April 20. 2012

Copyright Enforcement (Updated)

UPDATE April 20 2012

The High Court of Australia has today dismissed AFACTS appeal with costs.

Today, the HCA declared that ISP iiNet did not authorise infringing users on its network. It re-enforces the decision by the Full bench of the Federal Court, and the decision of original Federal Court hearing with Justice Cowdroy.

Other important notes to come out is the recognition that terminating users wont stop them moving to another ISP and carrying on with their file sharing infringing actions.

As I've said before, MPAA et al need to change their ways by making the content available at same time as overseas, and digitally online and at reasonable prices.

TV Networks need to stop making us wait 4 to 8 months (or longer) for a series return, or a new hit series - after it has already aired in the U.S. and U.K. If they fixed this, TV pirating would be pointless, we know they can do it. FFS we have how many digital channels now? How about thrashing all these constant repeats and non popular shows and the like on one of the secondary digital channels. We should be able to watch the current airings of hit series at same time as U.S. and U.K. and by same time, I appreciate contracts declare it must air first in say, the U.S., but given the time differences, 24 hours would be acceptable, even 48 hours, but 4 to 8 plus months? Completely unacceptable, so the networks only have themselves to blame for this, no one else.

If these organisations changed their ways, there would be little to no need for piracy , ya know... EVERYONE, then wins!

If these changes are made, and with a little bit of hope, this High Court decision will make them wake up and come into the 21st century, and piracy remains rife (doubtful), then AFACT and the like need go after actual offenders, via the courts just like the legal avenues that have been there in place for decades now already, rather than try blame the meat in sandwich, sue enough of them, and then people will rethink their actions.

Original Story - 2011-07-12 15:55

For years people have allegedly infringed on artists rights, be it music or movies.

The alleged music copyright violations were mostly by people not able to get or use music the way they want, times changed, this thing called the Internet appeared along with a myriad of choices to play and store music, and after a while the music industry changed with it, the complaints of file sharing music became almost non existent because people were able to buy it legally from the likes of iTunes and other services offering same, it took a couple years more but then the DRM was removed so people who bought a track could use it on portable music players as well as their PC without dramas, but it seems here were are ten years later and the movie industry still hasn't caught on to a viable market, I guess it means they wouldn't be capable of justifying their high rip-off costs.

So, rather than grab another marketing avenue (like the music industry did a decade ago), they rather keep to their old ways, bullying Internet Service Providers into playing coppers to police and do their dirty work, this is evident in Australia in iiNet V AFACT where AFACT lost its case because Justice Cowdroy made it pretty clear ISP's are not net-cops....

The movie industry appealed several points on the findings, and Justice Emmett found that if the notices could be proved valid, the ISP's might have a case of failing to act, AFACT want to continue to try force ISP's to be liable for their users service. So, in this way of thinking, why is not the likes of Telstra Corp liable? After all they are the first port of call really, since they provide the direct means, by connecting the last-mile of copper, should Acer, HP, Dell, and so on be

held liable because they provide the device for the end user? Will power companies be liable since without power there can be no Internet, yeah, hear what I'm saying, where does it end...

Why the three strikes wont work

One of my responsibilities at an ISP I worked for in early to late 00's was to also be the enforcer of AUP and T&C, we used to act on such requests, which, in recent times the Federal Court deemed we had no obligation to, although we had no right to kick off alleged file sharers, this was common amongst a number of ISP's then and at that time it seemed the lesser of headaches for us, because at that time, there was no legal clarification, something AFACT had a free ride on for way too long, since they never had to justify anything, now they've been told by Justice Emmett they do.

The robot notices are a joke

These automated bot things should have been ignored, why? Well, apart from the fact we assumed their guilt with no real evidence, and an ISP is not a police force, a court, nor a jury, because we once got a notice for a user sharing Open Source Software, so there is clearly no quality control on these things, when I attempted to converse with the complainant at the time (BayTSP) all of my requests were ignored, not one responded too, at that time, our policy, or at least my policy was to be slightly relaxed on this and issue warnings but only act upon very apparent repeat file sharers, a quick look at some of the accused infringers daily/weekly/monthly usage stats would be the basis for taking action or just another warning, but, in saying this, it is pretty hard to justify doing 300GB a month on a residential service, you likely are doing things you shouldn't be.

Terminating Users will never work

So, why the push for three strikes then terminations? What purpose is it going to serve?
I know first hand it makes no real difference at all to those who do this en mass. The New Zealand political party responsible for their three strikes rule is going to remove it from The Act, so there's no likelihood of anyone being kicked in the first place.

Termination for alleged Copyright breaches has not taught anyone a lesson in over 10 years, so it makes no difference, none what so ever at all to those who intend to download and share movies or TV shows etc, at best, it will temporarily inconvenience them for a few hours as their service is churned away to another provider, at best, it has them offline for a few days, where, they will reconnect with another ISP and continue their alleged acts of piracy.

I have seen it first hand, people I have terminated the services of have re-appeared on IRC gloating their back and downloading and sharing movies again, one person I even caught out admitting after he had his service disconnected, he reapplied using a different name and number, it was a share house of students, 4 of them living there with three phone lines, he was down for a total of 3 days, it made no difference to them, and this is not an isolated incident.

Take it from someone who knows, kicking them off is not, and I now admit, never has been, nor ever will be, the solution. They will be back, just with another provider, who might not be so quick to kick em off for them to churn to yet another ISP or method, and with the prevalence of pre paid accounts for access methods such as HSPA and dial up, mean they can be back before we even kick them. All it's doing is sending the problem to another service providor, it's not attacking the root cause.

Stop blaming the ISP's

It is a lazy cop out to suggest the solution is to go after ISP's, who legally can not just spy on their users for the hell of it and its been proved and shown in my personal experience and elsewhere as brought out in the initial court case, that these so called notices can not be taken at face value, even an alleged offender under the criminal code has his/her day in court where the evidence must be proved, but the movie industry think they are above the law and don't have to prove anything, imagine the chaos that would reign if every criminal court case was judged on word of mouth and not proved factual evidence.

The main reason that alleged file sharing is so rife is because the end users know the industry wont go after them, AFACT has as good as said that, so they are trying to have the ISP's made out to be the big bad bullies in all of this instead by insisting they do AFACTs dirty work for them, because going after the actual alleged offenders must be just too hard, and too much work, even though, it is the correct and only way to do it, and only way to make a change, that

and making their product more obtainable, and at a fair price.

The buck must stop with the alleged offender, no one else, you don't see car manufacturers being done over because their vehicle type was used to transport offenders to a crime do you? Why should this be any different, it is high time policy makers came into reality and stopped bowing to the dollar$ of the movie industry. Life is all about balance, the law exists now to deal with the alleged infringers, why do they not want to use it? Why do they insist its the problem of someone else who is not the offender? If it wasn't such a serious matter it would be a complete joke.

But AFACT and their like, want the easy, lazy way out, it's easier to sue an ISP for millions, sit back and celebrate with their carton of $2K a bottle champers... they wont get that out of a student, will they...

The Solutions

People have a right to protect their work, it can be there lifeline, but there is a right way to deal with alleged infringement, it is the responsibility of AFACT and other movie industry representatives to go after the actual alleged offenders, by way of court orders for users details to allow for suite, prove to a court that the alleged infringer is guilty, if the courts agree, they will find in the industries favor, it might take a few cases, but word would soon get around and that would be by far the only real chance they have of reducing the level of the alleged offences, it might mean the poor diddums will actually have to get off their lazy a$$e$ and do some work for once, and actually even prove the offence was really committed.

Recently, even the European Commission has joined into this by saying:

The EU?s E-Commerce Directive says that ISPs are generally not responsible for the activity of
customers and that member states must not put ISPs under any obligation to police illegal activity on its service.

In my opinion, Justice Cowdroys findings in the iiNet V AFACT case were correct and reflect the real world.

The sane thing to do is to stop ripping off consumers, and the TV networks stop treating its viewers with utter contempt by showing re-runs of crap, when they could be airing current series of popular shows, why are we waiting 3 months to, in some cases over a year, to see a new series that airs in the U.S and U.K., and yes even the ABC is as guilty as the commercial networks (to which I also include Pay TV providors).

AFACT at it, yet again

In recent days AFACT has tried the bully tactics again, more or less threatening ISP's in a letter they sent out to them - "If I do not hear from you within that time, AFACT will proceed accordingly," Mr Gane writes.

Read more on the latest stand over tactics by the AFACT goons at
http://www.theaustralian.com.au/australian-it/afact-prepares-new-campaign-against-isps

In March AFACT announced that it had sought leave to appeal the Full Court's verdict to the High Court of Australia. iiNet are also contesting some points of the appeal.
The application will go to a special hearing which is expected to be heard around November 2011.

Note: I currently have no directly related interest in this one way or another, as at time of writing, I do not work for an ISP providing end user services, but I have done for a number of years, I know and understand the reality when it comes to online activities of end users.

Posted by NoelB at 11:49

Thursday, March 1. 2012

Security and The Net

In an era where people are dependant on Computers, Mobiles and Tablets, one needs to stop being complacent about access to it, and I'm not talking about physical access. Far too many people assume things are safe by default, or are of the mindset that It'll never happen to them, well, wake up and smell the coffee, because things are not always as well as you would want to believe, and often because of the simplest reasons, opening an email from a friend who has had their PC infected and sending out malware, getting a strange MMS or SMS ringtone, downloading torrents, using a trojaned program, phone or tablet app, forgetting to change a devices default password, or not applying security on that brand new, or just reset WiFi device, as you see, most of these are user faults, and yes, it gets worse for the user faults.

Then there are times I think there should be a licence to use The Internet, especially when you repeatedly here of the same horror stories of people constantly being scammed, really, you've won millions from a lotto in another country you never entered? Overnight millionare from some long lost relative being told by plain email yet they want you to supply your details? really? The groups committing these crimes have been doing this for over ten years, they are masters of the art, most are highly intelligent, discreet, well organised, and highly resourced, their capabilities may be the envy of many a spook.

It's not however, only scams where you send them money, all some of these scam artists want is as much information as possible about you, that all leads to an ever increasing identity theft database for the fraudsters, who don't have to be international crime gangs, they can be someone in your local area, mostly where free public access WiFi is available.

The Internet is not however as bad as some make out, and it certainly is nowhere near as bad as scaremongering clueless idiots, like techo-weenie politicians and some religious groups like the Australian Christian Lunatics Lobby (incidentally, I'm yet to meet a Christian who says the ACL speaks for them), who all in having absolutely no idea themselves, make out the Internet is the anti-christ, thankfully most people have a higher IQ than those peoples shoe sizes, and can see them for the fear and scaremongering clueless uninformed morons that they really are. There are far more deviant people in the real world with far greater access to most things than online, but, just as in the real (offline) world, you need to take precautions.

It is actually easy to protect yourself online, and no you don't need to hire an army of armed guards, so much of it starts with plain 'ol common sense, after all, you don't go out whilst leaving your doors and windows at home wide open or unlocked do you? You don't give out your personal details to someone who just walks up to you in the street do you? Certainly in the later not without proof of who they are and represent (yeah I too hate those hawkers, good thing we have a Rottweiler)

The simple things to remember...

Never give out any of your personal or financial details to anyone you do not know!

In the case of phone calls, where you did not initiate the call to a recognised organisation on a publicly listed and recognised telephone number - this means no last names (if they address you as Mr and ask for your first name, politely decline as well), no addresses, no other phone numbers, and certainly no dates of birth or drivers licences, no, any company you do business with will not call or email you asking you to confirm your details!

By the way, computer techies are not mind readers, nor do they have ESP, if your "windows" has a virus or is broken, I think you would know before them, wouldn't you say? You would be calling a known local tech firm, not someone from India calling you Not even someone claiming to be from Microsoft, and if they claim to be from your ISP, thank them then just hang up, now you call your ISP yourself, don't ask them for any number, use the ISP's publicly advertised number.

Nor should you ever send that information to anyone, even a recognised organisation, by Email, if a business you wish to do business with wants that information, and, of course you called them, that's a different story, but again, do not Email them any of it, I've never come across a business that wont take your details on the phone, but if they need it in hard form, ask for them to send you an application, they can email it to you, but again, don't reply with it, print it out, and mail it to them, sometimes you can sign up and buy online, this is usually safe if the web address they give is a valid secure socket, commonly referred to as SSL or https, once you load the online application form, ensure there are no

warnings, ensure you are on a https:// web site with a green bar, or padlock (depending on your browser), and ensure the certificate is valid, if the website presents an unknown or invalid certificate, quit the site immediately and go elsewhere, SSL certificates cost very little, some are free, if they can't be bothered setting your peace of mind at ease, then why should you bother sending them your custom.

If you receive unusual email from a friend or colleauge seeking money, or an otherwise out of character message content, be aware that the persons email may have been hijacked and is being operated by some criminal group. Contact the person by phone or talk to them in person to confirm the communication prior to responding. It is important you do not respond to strange or unknown senders. This is also important with regards to an email from any organisation you deal with, be it a bank, your phone provider, Ebay, paypal or facebook, there are many emails out there impersonating such organisations that look very real, but the link they embed is to a site designed to collect your identity or login information, these are called phishing sites.

Email and social networking profiles are regularly targeted and compromised by criminal groups for the purpose of committing fraud and other illicit purposes including intelligence gathering for identity theft. Facebook is a prime example of this, people often make comments on unprotected pages that they are out for the night or going away on holidays, might seem innocent enough, but you really are easy prey in doing this, crime gangs are not the usual druggies on the street doing anything for a quick fix, these gangs are highly sophisticated and patient, if they get your details from somewhere, or decide to target you, they will stalk you on facebook, twitter, myspace, and so on looking for every little slip up you make in their intelligence gathering, given enough time they could know as much about you as your real friends, maybe even more.

So, be mindful of what you post on social networking sites in relation to personal information.

With regards to facebook, the site itself has little regard for your privacy, ensure you have the highest privacy settings, be careful on what you put in the about you, and your hobbies, activities etc as these can not be hidden, nor can your profile picture, the place has more privacy invading holes than a block of swiss cheese! If you are concerned, open up a separate browser, make sure you are not signed in and have stored/flushed web cookies, try viewing your profile, so you'll then see, what people you don't know see. And most importantly, don't blindly add people you don't know, because you never know what their reasons are or who they are.

If you want to know how much Facebook keeps on you, take a look at this U.S. government order for users details.

If you want to chat to other people and make new friends, do it how we used to before facebook - use IRC (Internet Relay Chat), it's much safer as well, if you're new to IRC try getting used to it by using a small quiet server, once familiar you can move on to a larger network such as Undernet.

With passwords, common sense rule number one - NEVER give your password out to anyone!

Always use different passwords for each different website. Never, re-use the same password.

Don't use guessable passwords - never use names, dates of birth, phone numbers, favourite places, family or pet names or variants of - as your password. Never use common words or phrases, it is recommended that passwords be at least 8 characters in length and comprise of an assortment of upper and lower case letters, numbers and other characters. If you're terrible at remembering passwords, a good way is to use character substitution, for example a password of lazyboys used on a site could be accessed by brute force in minutes, but lazyboys can easily become l4Z%8oYs a password that may take hours or days to find in a brute force, by which time many alarm bells should be ringing at the service provider where they can take action to block them.

The use of open WIFI facilities will make your online activity vulnerable to interception and you could therefore become a victim of identity theft. Any user names and passwords used, files sent and received are vulnerable, any files kept in shared folders on your PC or Mobile device may be compromised. Ensure any use of public WiFi is encrypted, in other words, SSL and especially on your Email as these programs by default, send information in plain and clear text.

Regardless of the access method or device, configure your Email (and FTP) clients to use SSL, in particular, TLS for both POP3 and SMTP, this means they wont see your Emails you receive or send, nor will they see your login name or password! Some client examples can be found at kb.ausics.net

If you operate a wireless network at home or work, make sure that at the very least you are using WPA2 encryption.

Never use

Posted by NoelB at 20:48

Wednesday, February 1. 2012

The Internet and Legal Jurisdictions

I'm sure you know where this is coming from, yes, the U.S. Governments targeting of Megaupload. But it's not just about Megaupload really is it, not when you think about it, it's about all data services within the U.S. and its Governments believed extended reach, be it Megaupload, Amazon, any Web Hosting company, Google Services including Apps and Gmail, or even Twitter and facebook.

Before I go any further, let me make it very clear from the outset that I have no, never had any, nor ever could see myself having any, data, dealings, association or interest in, or with, Megaupload or any of its associated companies. My interest is in the future of a free, neutral, uncensored, and UN-Govt-molested Internet.

We all know the Megaupload folks knew their services were used for allegedly illegal purposes, although registered in Hong Kong, and staff based in non U.S. countries, the U.S. Govt is claiming jurisdiction because the equipment used in providing that service was in full or in part, located on U.S. soil, this is in my opinion a fair call. However, some legal talk over this seems to suggest the U.S. Government thinks it can claim jurisdiction on anyone who uses, for example, Paypal (being located in the U.S.), or simply because they may have a .com or .net domain name, the latter being highly questionable and is really clutching at straws and reeks of pure desperation, one I'm sure any civilised and rational nation would refuse to extradite over, extradition treaties are very specific in nature as to what offences are allowed in order to meet the criteria. I have faith that the courts in my country for example, would quash based on the latter.

The danger signs have been around for well over a year with the well publicised illegal blocking of funds for Wikileaks from Visa, Mastercard, Paypal and others.

It is also

Posted by NoelB at 18:47

Thursday, January 19. 2012

I'm on Strike! Stop SOPA/PIPA/ACTA/TPP

Today, the 18th January UTC, my various web sites, including the surprisingly popular ITS site, joined thousands around the globe and went on strike, now, some of you may be wondering why, since I'm not in the U.S., and we only have two hosts, hosted there, the answer is rather simple.

True SOPA/PIPA will not directly affect anyone outside of the United States of America, however, when you take into account the likes of Youtube, Twitter, Wikipedia, Yahoo, Hotmail, Google and even that hopeless site that has total disregard and utter contempt for everyone's privacy - yes, facebook, are all registered entities in the U.S. and are mostly located in the U.S., therefor, SOPA/PIPA will indirectly affect all non Americans, at least in the interim, because if this does become law in the U.S. it likely wont take too long before the U.S. is bypassed for most things Internet based, remember how quickly Youtube and Google took off? It wont take long before they are replaced, so the only harm will be to themselves in the long run.

The EU has made its opinion on Internet censorship and filtering very clear in that it should never happen.

The European Court of Justice gave a preliminary opinion that will have far-reaching implications in the fight against overaggressive copyright monopoly abusers. It is not a final verdict, but the Advocate Generalâ€™s position; the Court generally follows this. The Advocate General says that no ISP can be required to filter the Internet, and particularly not to enforce the copyright monopoly.

Further to this, the Internet Strike page provides a link to the U.S. State Department where non U.S. citizens and residents may place an objection, letting them know this is unacceptable and, as the site so rightly states, it is very hypocritical of the U.S. given the State Dept is so outspoken about other countries trying to censor the Internet, in fact it was barely 18 months ago that Hillary Clinton herself made public statements condemning the Australian Federal Labor Government for trying to censor the Internet to its citizens, so, what happened Hilly? Is it the typical U.S. Govt way of things, you know, do as we say, not as we do? I think the answers blowin' in the wind - only this time right around the world.

Some commentators have also asked why this is still going ahead, since some congressmen have said they are delaying, and from most reports its only delaying by a month or so, well, hello, wake up and grab some fresh coffee you bloody morons, delaying is not abandoning.

Furthermore, if the U.S. passes this garbage, it will give minority groups everywhere the power and incentive to push for more censorship, and may help set a precedent that other countries may use to introduce similar.

People power can work, despite the tiny minority Religious groups and political party family something or other, trying its best to get their beliefs and morals forced upon the vast majority of the Australian population, people power stopped the Australian Labor Govt from introducing it, with not only most members of their own party against it, all major opposition parties have refused to support it.

So, our American friends, don't give up hope, but also, don't just sit on your ass expecting the guy next door to voice his opinion for you, pick up your phone, send a fax, or pay a personal visit to your local members office and be heard!

Update: Feb 13, 2012
Seems the U.S. Government are trying it on again, this time with the current secretive talks the U.S. (surprise surprise... not...) Trade Office is trying to push to the world in the well publicised and despised TPP, which is as usual one sided, U.S takes, we all give. this sort of corporate sponsored nonsense needs to be stamped out once and for all, no mater what name you give it, its meddling, meddling by power hungry tyrants in a country where politicians can it appears be bought by hollywood execs.

Posted by NoelB at 10:02

Sunday, December 11. 2011

Why One Should Avoid The Cloud Hype

This entry has been updated (Feb 20, 2014)

Cloud computing is nothing more than a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. (Source - Wikipedia)

Cloud computing is nothing new, it has been around for decades. Email or Web Hosting anyone? The term Cloud is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents, but in recent times, some marketing hero decided to come up with a new hype, and like all techno weenies, the media picks up on it, these stormy cloud times are rather funny, but sad.

Richard Stallman of the Open Source Software Foundation summed it up nicely in an interview with The Guardian â€œItâ€™s a trapâ€¦ Itâ€™s worse than stupidity, itâ€™s a marketing-hype campaign.â€•

Here at home in Australia, organisations investing in off-shore cloud services could find themselves on the pointy end of legal action should the privacy of Australians be breached as a result, Victoria's acting Privacy Commissioner has warned

For companies, its a privacy nightmare, you may not even know which country your data is in, and chances are their privacy laws wont be as tough as local laws, then there's the inherited dangers of dealing with American firms, The U.S. Patriot Act requires all U.S. incorporated businesses to comply with demands for information, even if your data is on that firms non U.S. located servers. The Canadian Government has made it unlawful to host Government material in the U.S. explicitly because of The Patriot Act and many other Governments and companies around the world are thinking twice about using the U.S. Cloud hosting. Australians are fairly lucky in respect to having tough privacy laws, but all that goes out the window too when hosted in the U.S. and likely other overseas content providers, as well as any U.S. incorporated firms based within Australia, yes, this could mean Microsoft, Google, Amazon et cetera.

Then there is data integrity, what sort of network is your data on, what is the competency of their programmers, their server administrators, what sort of contingencies do they have to keep your staff working, or your clients happy in event of failures, we've all seen the failures of Google and Amazon clouds multiple times in past year or so, even Microsoft cloud services had a pretty big failure earlier this year as well.

This post was started in draft stages on Dec 5, since it always takes me a few days to be happy enough to finalise it ready for publishing, I must have known something (wish my lotto entries had as much success as my other sub conscious predictions heh) by not getting back to it for a few days longer this past week, because on Friday, Telstra Big Pond (Largest Australian Service Provider) had a massive Privacy Breach in its systems for customer self service that saw it, and all Email disabled for close to 24 hours, It affected a large number of people "The exposed site offered customer service-level access to customers of Telstra bundled products. Information accessible included a veritable feast for identity theft: bundle information, telephone numbers, users names and addresses, logins and passwords" - surprisingly what most did not know is that Telstra outsource this service, yes, you guessed it, to the stormy Cloud, how stingy can they get, not using their own infrastructure, to quote The Register The site is not actually hosted on a Telstra domain: itâ€™s a cloud-based service on the custhelp.com domain operated by RightNow Technologies. The equally scary thing is, apart from being reported on two online media outlets, the SMH and the Australian, lets face it who the hell reads either of those? Maybe half a chance for the SMH if you live in NSW, but what about the rest of the country? There were no reports in the mass media, ie: Radio and Television news, certainly not on the more popular commercial stations, and still hasn't been, very nice job of hushing things up appears to have been done. It just goes further to show why this marketing thing called Cloud, is a load of rubbish and has very severe security implications for all who use, or contemplate using it.

World renown security expert Kevin Mitnick has had much to say on Twitter about this, but one of Kevins recent tweets sums it all up nicely:

With the Cloud, security has been, and continues to be, a real concern. It might be a convenience, but is it really in the long run? Businesses (in fact all) data protection should be of the highest concern, and the only way you will know it is secure, is by housing the equipment in-house where you can separate the intranet from the big bad internet, and have direct and immediate control of what code developers do. It's like that file server with all those highly confidential contracts on it being plugged into the Internet, with no access control lists, all there for the taking.

What about if you have a dispute with the host provider and they suspend your service? How long will your business last if they deny you access to your own data?

Cloud is nothing new, with what these marketing folk interpret as The Cloud today, is mostly used in cost cutting, with a very high degree of risk. This risk is acceptable in Web Hosting, Online shopping carts and so on, everyone knows what to expect because it's been around for well over 20 years, and everyone's doing it, but, it's a completely different thing when it comes to putting businesses operational material on an Internet based service, this is very very dangerous, and all businesses should conduct a fine detailed risk assessment, including your insurance and banking, and so on, you might find your premiums increase, your bank manager might consider it too risky to approve your next loan, and you might be in breach of the law if your move to the Cloud makes you non PCI DSS compliant.

Simply put, leave the real Cloud (Internet) for what it was designed for, transmission of information (ie: Email, Web, et cetera) and keep your business data on an air-gap (no way possible to reach Internet) Intranet, that way the security is assured. Your customers don't care about buck passing, like for example, RightNow, they have no contract, no service agreement, no nothing with them, they have those things with you, or in our example, Telstra. It is your name that will be damaged, now that might be acceptable to an organisation of Telstras size, and lets face it, they don't care too much for what anyone thinks about them anyway, but ask yourself this, are you big enough for any backlash? Most would have to say no, especially if you're concerned about your company image, remember, word of mouth can do damage as well as good, most people will research you online before considering doing business with you.

Privacy waived by carriers

Australias Telstra agreed more than a decade ago to store huge volumes of electronic communications it carried between Asia and America for the U.S. Government

â€¢ Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal;

â€¢ The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail;

â€¢ The company worked with the FBI this year to allow the NSA easier access via Prism to its cloud storage service SkyDrive, which now has more than 250 million users worldwide;

â€¢ Microsoft also worked with the FBI's Data Intercept Unit to "understand" potential issues with a feature in Outlook.com that allows users to create email aliases;

â€¢ Skype, which was bought by Microsoft in October 2011, worked with intelligence agencies last year to allow Prism to collect video of conversations as well as audio;

â€¢ Another Dangerous U.S. Govt Act is the Stored Communications Act, and little known fact that classifies all data older than 180 days as abandoned, this means it can be accessed at any time, without warrant or just-cause, or any reason at all, so if you thought those messages on gmail or hotmail/live, or your data in Googles Drive or Microsofts Skydrive, which is over 180 days old, are covered by any privacy laws, then think again, the U.S. Govt interprets this data as abandoned and can read to their hearts content.

Updates!

In what can only be described as a shocking decision, Bigpond customers emails are now to be stored in the cloud. The horrifying thing about this is, Bigpond users although warned of this outsourcing, were not told the data will not be stored in Australia, but likely in either Singapore, or the U.S.A., both of which have far relaxed privacy laws compared to Australia, and as indicated in my comments in my The-Internet-and-Legal-Jurisdictions article, you can see how far the

U.S. agencies will go, but it will not be much better in Singapore!

Time for Bigpond'rs to consider if they want to remain in the muddy puddle or move to brighter and greener pastures.
Reference: ITNews

I trust Telstra will no longer use the add that involves the lyrics I am, we are, Australian, since they have shown what they think of Australia.

And a new warning to rethink where you host anything might be even more important now to consider given the U.S. FBI wants legal back doors mandated into websites that will of course see non U.S. citizens also targeted with this stealth secret police state mentality the U.S. Govt agencies have as well as their own citizens.

Even a very famous hacker from years gone by turned security consultant, Kevin Mitnick, does not trust the cloud.

Update:
Recently, Amazon has shown why not even they are all that reliable for your business..
Amazon Web Services sometimes replaces the hardware virtual servers run on and switches those servers off without elegant or accurate notifications of whatâ€™s about to happen.

A trawl through AWSâ€™ support forums suggests that the company isnâ€™t switching off servers without notifications every day, but threads pop up quite regularly in which users complain about servers disappearing.

Full report courtesy of The Register

Update2:
Yet more Amazon outages, this time 20 hours for major clients during Christmas 2012, yet another one in the ever growing number of outages, where the smaller players, as in most local Web Hosting providers, or in-house data storages, don't experience so much drama.

Update3 - 2013
A routing fault on the SingTel network has caused four days of mail issues for subscribers to Microsoft Office 365, once again (losing count now) highlighting yet another failure by using offshore cloud services.

The problem was first reported in the Microsoft Office 365 Community forum on January 5, 2013, with users noting that they could not reach the servers hosting their Outlook mail and that they had received retransmission errors.

Read more about yet another offshore cloud screwup

Update Aug 9, 2013

In what can be described as a sad day for Email providers, Lavabit has now, at least for the time being closed, due to secret efforts of the US government trying to spy on its users, with a stern warning from its owner

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.
Ladar Levison
Owner and Operator, Lavabit LLC

Update Aug 15, 2013
Google's lawyers freely admit your Gmails are theirs, and not yours.

Consumer Watchdog has unearthed a brief filed by attorneys for Google saying Gmail users have no reasonable expectation that their communications will be kept secret.

â€œGoogle has finally admitted they donâ€™t respect privacy,â€• said John M Simpson, Consumer Watchdogâ€™s Privacy Project director. â€œPeople should take them at their word; if you care about your email correspondentsâ€™

privacy donâ€™t use Gmail.â€•
read more at Siliconrepublic

Update Oct 15, 2013
Telstra Dumps Offshore Cloud Email Hosting.
Telstra has quietly shelved a major deal with Microsoft that would have seen it migrate 4.2 million email addresses to offshore hosting facilities.

Update Feb 20, 2014
In another Google cloud screwup involving serious breach of privacy, accessing third parties Google Drive files

Attackers can access a user's Google Drive files and record them through their webcam by tricking the user into clicking hidden links, a researcher found.

.. Google fails to verify whether a user is authorised to view the sensitive thumbnail
Hell, they even allow unauthenticated access to the thumbnail!

Read more of the yet another cloud blunder at ITnews.

Posted by NoelB at 16:02

Friday, July 29. 2011

550 Access Denied

The biggest problems with getting your Email to someone is getting through the receiving ends mail servers defences.

Sadly, long gone are the days of the early 90's where spam was really only something that was heard of in a supermarket, although it had been around for years, even on ARPANET, it was not of plague proportions like it reached in the mid-late 90's through to the problem it is today. Long gone also are the days where you can trust strangers to use your mail server, where it was common two decades ago for most mail servers to be open relays, but, as with anything that's available, it soon became abused, so to combat the problem of spammers abusing this privilege, MTA's like Sendmail soon released versions that no more by default permitted open relaying capabilities, like the 'ol saying... if you abuse it, you loose it!

Defence comes in many forms, most common is the well known method of DNSBL's (DNS based Real-time Block Lists), often also referred to as RBL's, PBL's, Blacklists, or even Blackhole Lists, these are DNS based lists of domain names and IP numbers of trouble makers, people who have given others grief in some form or another (spam, phishing, compromised, abuse, etc...), they become submitted to these lists by trusted persons, also through automated processes, including hidden addresses to trap spambots when they harvest websites looking for addresses to add to their spam-out lists.

Today there are more than 30 such public lists, each with their own listing criteria, however, there are only a handful of what are considered reputable lists that the vast majority of administrators use, not to mention many private lists (like the one we run), and in-house DNSBL's used amongst a group of ISP's, occasionally even sharing data between them. You can test a blacklist entry here

But DNSBL's are just one obstacle, before you get that far, you often go through several other checks like local access lists, hostname and DNS compliance testing, and so on, this is where greater than 90% of the rubbish is filtered out.

One of the best ways to help get your mail received is to ensure your DNS is properly configured. In your domains DNS zone file you should have an A record entry, and in your in-addr.arpa or ip6.arpa zone files for your IP allocations, a matching (rDNS) PTR record entry - for every machine, and in particular, for every server. RFC 1912, Section 2.1, para 1 and 2 clearly states "Every Internet-reachable host should have a name" and "Make sure your PTR and A records match" and "For every IP address, there should be a matching PTR record".

With IPv6 starting to get off the ground, it is going to be far more of an issue given that most people will end up with so many addresses. So it will be more important than ever to set correct DNS for your IPv6 and IPv4 addresses for any server that should be sending mail, be it a mail server, or a web server that might for example, run a forum or blog, and needs to send mail for confirmations, updates, password resets etc.

Another well used trick involves rejecting dynamic users, these are connections that have good forward and reverse DNS, but include things like a dotted or dashed version of their IP number, ppp, dial, xdsl, pool, cpe-, ip- , dyn, cable, and res, to name only some, in their hostname, this normally indicates a residential host, with likely no dedicated mail server or a genuine need to be directly sending mail. So in selecting a service, ensure your rDNS can be changed to a suitable name, if not, find a provider that does offer it, even if only by request to support. The recipients ISP's wont tolerate constant whitelist me please requests because you or your network provider can't get their act together, remember it's you/your host that are non compliant. So, in your naming conventions, don't use the IP number or parts of it in your DNS/rDNS entry for servers, but it is of course fine to do so for general PC's, laptops and mobiles that should have no reason to directly send Email to anyone, and make sure that your server hostname settings match, if they present a HELO/EHLO with rubbish, you can be sure you'll get blocked for that as well. Make life easy, give your servers a server-like name, eg: falcon.your.domain, and configure it and DNS for that name only, if you run a dedicated mail server, call it mail.your.domain, or some othername that resembles a servername, and ensure your DNS zone has that name listed in the MX record field.

If running a mail server, and you block a host because of policy, ie: access lists, milters, RBL's, etc, you must do this at the initial smtp connection, where your server can reject the message with a 55x error code so the sender knows they have been blocked, and why, the only time you are not required to do this, is if using an anti-spam set like spamassassin

and you silently drop high scored spam messages, low/medium scored should still be delivered, most anti spam mail server software has the ability to send a warning message and attach the original spammy message to it, I personally use a cutoff of around 15, that's high scored and silently discarded anything less and amavisd will warn the recipient and include the spam as an attachment, please do not ever use software that bounces spam or notifies the sender of the spam message, if you have accepted the message, you must either deliver it, or discard it, never bounce it (chances are the addresses will be forged anyway).

Speaking of forgeries, I also suggest you use SPF, you should not only publish your SPF record for your domain (and any domains you host), but enforce SPF checks on your mail servers too. There would be so much less phishing attacks, especially for financially related incidents, if only those organisations would use SPF.

When implementing SPF, I recommend testing thoroughly first by publishing a softfail condition, and once you're sure it works right, change your DNS SPF resource record (RR) to a hardfail, that's from ~all to -all. The modern way of using SPF in DNS is with the Type SPF, but, because there are a lot of lazy admins out there who have not updated their daemons or scripts, you should also publish your SPF data in the deprecated TXT method as well for the time being. In its simplest form, all you need is the IP address numbers of the servers you want to allow to send mail on your domains behalf, for instance this domain, ausics.net has the following SPF and TXT records:

v=spf1 ip4:27.33.160.23 ip4:62.113.243.167 ip6:2a00:f48:1029::1:a05d:e257 ip6:2001:470:67:524::0/64 -all"

This means only those addresses can send mail for any email address at ausics.net (based on envelope sender) (I do not recommend using name types or mx's, use IP address or ranges only, SPF is of course very powerful and can be extended to include other zones, and even use regex's, if you're new to this, stick to the basics only, don't over complicate things.) You must always remember, like everything DNS, you need to keep things up to date at all times, so if you change mail server IP's change your SPF too!

Another advantage of publishing SPF records is if sending to Live.com (Hotmail), or Gmail, under their scoring systems, you get a higher rating, meaning greater probability of inbox delivery.

Some people are anti-SPF claiming it messes up your mailing list posts, I've published SPF records for a great many years now, and have never seen any collateral damage like this, most modern list servers re-write the envelope sender address, so although a mailing list post might reflect From deletethis@ausics.net, the envelope sender which SPF uses, will be different, it will be from the domain of the sending list server, eg: cisco-nsp-bounces@puck.nether.net, so SPF receivers, would be testing if puck.nether.net is allowed to send for cisco-nsp-bounces@puck.nether.net, and not testing for deletethis@ausics.net. You can learn more about SPF at openspf.net.

The most popular used anti spam program, SpamAssassin, is used on a very large number of servers and proprietary hardware devices, it looks for keywords and styles and is based on a score system, so don't send Emails that are obviously spammy and it wont positive score you, SpamAssassin, like everything else, is not foolproof, nothing is, and anyone trying to convince you their solution is, is full of crap, but SpamAssassin works, and works really well. Some sites rely on outsourced services (or rules), meaning they pay a ridiculous amount of money for some re-badged server from one of the mobs selling these hardware devices and relying on their rules, their decisions, and don't custom configure the devices at all. I've seen and heard countless admins cursing those things, but, you got to expect that if you're prepared to let someone else decide what your network gets. Personally, I don't believe in those things, if I'm providing a mail service, that's for me and my colleagues to decide.

Note: SpamAssassin has an internal whitelist when it comes to URIBL's (which check links inside emails), some domains on that list should never be there, like mail.ru, and a few more, so I highly recommend adding into your local.cf the keyword option: clear_uridnsbl_skip_domain

If you run a mailing list, ensure it is configured to double opt in, and don't blindly add any addresses to it under any circumstances. Configure the list to suspend delivery of mail after a very small number of bounces - Mailman and Ecartis are able to do this, and, although its been many years since I looked at it, I think ezmlm also. Make sure only subscribed members can post to your lists, moderate new members for the first few messages if at all possible, spammers love to abuse mailing lists too. Having someone on a list that doesn't want to be, is the worst thing you can do, so make sure your list server works properly for those wishing to unsubscribe, and make sure it works by email as well as any web interface, nothing worse than having to use a web login to remove ones self from a mailing list. Failing to adhere to most of these things is another great way to be placed on a blocklist.

IP numbers are finite, yes, they get re-used, and it is possible the ranges allocated to you were previously used by low

life scum who spammed and the range was listed in one or more blacklists, you will have problems convincing blacklist maintainers removing that listing, ensure all PC's with access to your LAN are virus scanned and kept patched, this is especially so for Windows users. Research your service provider well, and if you're on ISDN/xDSL/Cable etc, perhaps explain to your ISP your dilemma and ask them to change your IP range, hopefully you do this when you first get your connection up and running before you migrate and go live on your new connection.

There are some whitelists around for SpamAssassin and hardware devices using nice-lists and reputation, there are some money grabbing bastards who operate some block/reputation lists, that when you are blocked via their lists, the reject message is telling you to go to some web site and pay to be whitelisted/get a good reputation - WTF? Seriously people, save your money - Trust can only be earned, not bought! I also work under the assumption of my network, my rules.

With relation to grey-listings, don't bother, many spam bots are cluey enough to retry these days, all it serves today is to delay legitimate Email, something that could cost you or your employer in many ways. I'm also not a real fan of DKIM, since it can, and does break with mailing lists (often you'll see it with gmail users), and when you have many domains on one server it gets trickier.

One thing I need to make clear to you if you're new to setting up your own mail servers, do not ever allow it to accept messages for non existent users or blindly relay for others, backscatter is the fastest way for your mail server to get blacklisted. Ensure you only relay for your local IP ranges, better still, use the message submission port (SMTP Auth) (port 587) and only accept inbound mail on smtp (port 25) that's destined to your own network from external addresses, and block outgoing port 25 on your router (with the exception of your mail servers IP of course) if at all possible.

In conclusion, if you follow the above rules, the chances of your mail getting through to the recipient, will be pretty good, you'll have less rubbish yourself to deal with, and overall, also be a better netizen

Posted by NoelB at 19:47

Thursday, July 14. 2011

Phone Hacking - OH NO!!! No, your mobiles not actually hacked

So, in light of Murdoch's staffs criminal actions, the worlds media have been filling our airwaves with the term Phone Hacking, why, I'll never know, as it is really incorrect, no phones were actually hacked at all, no conversations were monitored in real time, no phones contacts list or stored emails or photos were ever compromised in this latest scandal.

What is actually occurring is illegal access to peoples voicemail boxes. Most of us, and yes, I bet *you*, are still using the default PIN number for voicemail. Now, most of the time we don't need to know it, since the phone networks know who we are and just give us access, but, you do know that you can access your mobiles voicemail from any phone, anywhere, at any time.

Usually when your voicemail is first activated you will or at least should be, asked for a PIN, if you did not get asked for whatever reason, your voicemail box will be using the default PIN, in 99% of the time, that is simply the last four digits of your mobile number

So, by knowing someones mobile phone number and the network they use, which wont take long to suss out either way since all networks publish voicemail access numbers for members to be able to remote retrieve their voicemail, someone can very easily illegally gain access to ones new and stored mobile messages. It is in some cases as easy as dialing your own mobile number, instead on leaving a message, hitting the star button gives you access, where you will be asked for your PIN.

The way that has been used in recent times with prominent people is, a partner of the offender will place a genuine call to the unsuspecting victim, whilst the other partner goes about accessing their voicemails.

It is imperative that everyone who is not sure, goes to their phone providers website and find the voicemail FAQ, and sets up a personal PIN, in most cases this is done via dialing your voicemail number (321) and going into setup and finding the option to setup or change your PIN.

So, although the media have got it named all wrong, the hype about its risk and dangers is very very real, and should be taken seriously by every mobile user in the world.

Now you've finished reading this and should have a better understanding of the dangers, you are now about to hop off changing your PIN, right?

Posted by NoelB at 10:22

Friday, July 1. 2011

Data Centre Cooling

For decades most Data Centre's utilised raised floors to inject cool air from underneath up to the racks in a back to back arrangement, this is called the Hot aisle Cold aisle method, but for some years now this method is considered outdated and rather inefficient for Data Centre cooling.

inefficient hot aisle - cold aisle approach

This method, as seen at left, involves hot air from hardware released from the rear door of a rack into the general Data Centre airspace, to assist with some form of hot air containment, most rows of racks will be so two rows are back to back, but, this still allows for hot air mixing with cold air as they are not truly contained for exhaust.

Many modern Data Centre builders have got it right in what makes far more sense using the all Cold aisle method, which involves an overhead plenum for the hot air to be expelled into, this means only cold air in your DC, and no mixing of cold and hot air, since the idea is to keep everything cool so your valuable hardware stays at a safe operating temperate.

The cold only method works by, as mentioned above, using an overhead return plenum to capture the hot air, and in most buildings this is already in place by means of false ceilings which can easily be sealed and used for this purpose. The racks will often have a low current fan that pulls the hot air out into the plenum by way of a type of boot, think of it as like a house chimney expelling smoke into the outside air, rather than filling up your lounge room. The cold air can be pumped in from overhead or the side so your racks can sit on that nice firm slab of concrete, and in this day and age with the world experiencing a horrific number of earthquakes, it also just might save your bacon if you are in a quake zone.

efficient all cold aisles approach

The method works best by using a grated front cage door on the racks to allow the cold air in, with the two sides and rear door fully sealed so the rear hot air rises to be expelled into the plenum. It's also more efficient if all blank RU's have blank panels attached to trap that hot air in the rear, back in 2007, I even saw pictures of some rack RU's covered and taped over with plastic, some racks even with cardboard... well... so long as it does the job I suppose

This approach has the benefit of keeping your entire Data Centre cooler, and given the CRAC units have an intake inside the plenum, they have less work to do, anything that needs to cool 27/28c into 22c must be better than something that needs to cool mid-high 30's and in Brisbane, that's more summer days than not, even days around 40, which, although not having the same humidity level, even Sydney can see a good number of days up that high. This makes your DC cooler, Greener since you'll have less of a carbon footprint, and more cost efficient.

It is also important I think to have a fresh air intake to your CRAC's for OH&S, some DC's in the U.S I've heard inject outside air for five minutes every 30 minutes, sure, that kind of contradicts the above advantage injecting some hot air, but overall it's cooler temps to be cooled and the idea of this is after all to keep the DC cool, the other is just beneficial side affects.

Sidenote
The entire idea of this is hot air containment, so if you only have a small room, with a few racks in it and use in-row CRAC units, you can take a similar approach, using sealed rack sides, sealed spare RU's and front grated doors, but with rear grated doors to expel the hot air into the small area behind, sealing above and the sides of your row of racks (even cheap perspex will do the job) forcing all hot air into that small isolated area at the rear of the racks where your in-row CRAC unit has its inlet, or, by still using duct cut outs into the plenum to allow the hot air to escape for a building CRAC, so long as that rear area is isolating the hot air from the server rooms cool air, the net effect is pretty much the same, and its much cheaper idea if you only have a few racks using in-row air cooling.

Posted by NoelB at 07:42

Saturday, June 25. 2011

Digital Signatures and Encryption with GPG/PGP

In this day and age, I think it is wise that people use digital signatures with methods such as GPG/PGP to prove authenticity and using its encryption capabilities for privacy when storing mail on untrusted networks, such as those hosting mail in other countries, especially those countries who have questionable laws regardng privacy.

It is useful in many ways, from saying "Yes, I really sent that message", to using it to encrypt a message or files for privacy, to something as important as signing a checksum file, after all, what's the point of creating a checksum for a file, since if your machine is compromised, all they need to do is to recreate a new checksum and you're none the wiser, but this is harder to get around when it is also expected to be digitally signed by someone.

GPG is available for Linux, Mac, and Windows.

Windows users should install GPG4Win

Apple users should install GPGMail

GPG with Linux/Unix
This is not designed to be an indepth guide, it's a quickstarter. Most distros by default include GNU Privacy Guard (gpg) in the base install so you should not need install anything, we will be using command line, so if you're in X, open a terminal window...

Some things to remember, when creating keys, it is important to remember to create a revocation key, and to backup not only your public key, but your private and revocation keys as well. It is also important to upload your public key to a key server and make it publicly available via your website so your signature can be confirmed for authenticity and recipients can decode encrypted files you send them.

Create your key

gpg --gen-key and follow the instructions, basically, you want to use the default type (1) RSA and RSA (default)
What keysize do you want? (2048) hit enter, 2048 is very strong.
The key lifetime is up to you, on work keys I would use no more than 2y , if its personal, I use 0 for indefinite, we are going to create a revoke authority key later.

Next enter your First and Last name, the email address this key is associated with, any comment (you don't need one, but if you worked for say TPG, you could enter TPG.
Now you'd end up with something like....
Real name: Noel Butler
E-mail address: deletethis@ausics.net
Comment:
You selected this USER-ID:
"Noel Butler (TPG) "
Then hit o for OK
Then you will have to enter a pass phrase, think of a good one, do NOT use names or people/pets, or dates, phone numbers etc and make sure you use numbers and mixed upper and lower case characters.

You will need to move your mouse or hit gibberish on the KB so it can generate enough random goodness.

When its done, you will end up with your Key details

gpg: key xxxx94E marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 2 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 2u

gpg: next trustdb check due at 2012-07-02
pub 2048R/xxxx94E 2011-07-03 [expires: 2012-07-02]
Key fingerprint = xxxx xxxx xxx x
uid Noel Butler
sub 2048R/ xxxxhy2011-07-03 [expires: 2012-07-02]

Congratulations, most the hard work is done, well, kinda.... copy the characters on the pub line, after the 2048R/ in our example it's xxxx94E

Submit your Key

Now you have your keys, you should send your public key to a keyserver so others can find it.
There are several key servers, they do sync up with each other so you don't have to upload your public key to all of them, just one is sufficent.

Warning: Do not ever send to a key server, or give out to anyone, your private keys! Only your public key.

From our earlier example your key is xxxx94E, so to submit this key you would issue the command
gpg --send-keys --keyserver hkp://subkeys.pgp.net xxxx94E

Next, we are going to export our public key to a text file so we can put it on our website for those who can't access it via key servers for whatever reason...
gpg --export -a -o .gnupg/pubkey.asc xxxx94E

You should now enter your keyID (xxxx94E) in your email client's security section if you want to sign or en/decrypt mail.

Backup your Keys

Now the all important backup stages, first backup your private key...
gpg -ao .gnupg/backup-secretkey.asc --export-secret-keys

then backup your public key...
gpg -ao .gnupg/backup-pubkey.asc --export KEYID

To restore your keys to your keyring in case it gets corrupted or deleted...
gpg --import backup-secretkey.asc
gpg --import backup-pubkey.asc

Revocation Keys

Next step is to create a revocation key in case our key has been compromised...
gpg --output revoke.asc --gen-revoke xxxx94E

If you need to revoke your key, use (and this is how you add someone elses public key to your keyring)
gpg --import revoke.asc, and to complete the revocation
gpg --keyserver subkeys.pgp.net --send xxxx94E but lets hope you never need to do this.

Warning: It is very important that your revocation key, and the backups of your private keys are kept very secure. I usually have a spare directory where all of my gpg backup files are kept, but they are all also encrypted by use of ccrypt, so anyone who gets a hold of them has to know my rather long pass phrase before they can decode them.

Note: You cannot, at least at this point in time, delete your keys from the keyserver network, once there, they are there forever. This is why it is important to create a revocation key, this amends your key status to revoked with, in most cases, a reason, but again, it does not delete them, I hope that one day this will be possible, but as things stand today,

it's not.

Expiration of Key

There are merits in setting an expiration in your keys lifetime, it is not essential, but if you are using your ISP's or Work Emails, then it's likely an OK idea.

So, you've done all that, and here it is a year or so down the track and the keys about to expire, the Email account is still valid, so you want to extend the life for another two years, you can do this via the gpg shell using --edit-keys, so, if your email is deletethis@ausics.net you would run

gpg --list-keys deletethis@ausics.net

The resulting information would be

pub 2048R/xxxx94E 2011-07-03 [expires: 2012-07-02]
Key fingerprint = xxxx xxxx xxx x
uid Noel Butler
sub 2048R/ xxxxhy 2011-07-03 [expires: 2012-07-02]

We will need both the primary and sub key ID's in our example,
key 0 xxxx94E
key 1 xxxxhy

Now, run gpg--edit-key xxxx94E
You're now in the gpg shell, by default the primary key is key 0, so just type
expire
You'll see something like

Changing expiration time for the primary key.
Please specify how long the key should be valid.
0 = key does not expire
= key expires in n days
w = key expires in n weeks
m = key expires in n months
y = key expires in n years

Type is, for example 2 years : 2y
You'll then be presented with the new expiration date, enter in y to confirm, and your password when prompted, next we need to update the sub key by typing

key 1
expire
2y
y

and your password when prompted, now, we are almost done, before quitting you need to type
save

Congratulations your keys are now updated, don't forget to save your new key to a text file if you make your public key available via a website etc, and, importantly, you need to submit your updated key to a key server, eg:

gpg --send-keys xxxx94E

Signing Messages and Files

As mentioned earlier I often create checksum files for configs and some files, but, to ensure they are not also tampered with, I also sign them, being text files I can add the signature to it by way of

gpg --clearsign filename
I'll be asked for my pass phrase, once entered, a new signed file will appear, for example, I've just made a checksum file called files.md5, now I gpg --clearsign files.md5 afterward I'll also have files.md5.asc (the signed version) so I can delete files.md5 (the unsigned version).

For obvious reasons you can not really sign a binary file, like a zip file, so you would sign as...
gpg --sign file this results in a sig file being created of same name plus .asc, eg:

gpg --sign CAM results in the file CAM untouched, but the verification file is now created as CAM.gpg which must stay with the file CAM.

Verifying Messages and Files

To verify a file (or message) is from someone, you would typically use gpg --verify filename
The file may be a clear signed file with gpg information embedded or a .gpg file.

In some cases, the file will be unmodified, but will be accompanied by a .sig file, generated by gpg -b filename, in this case you verify it using gpg --verify filename.sig filename

Most email clients do this automatically so you don't need to bother too much there, but if it is an attached message or one sent via other means you may need to issue this, especially so for files.

If you need to import their key (necessary for encryption) use gpg --recv-keys THEIRKEYID

In some cases, if a key is not found, you can try searching key servers by:
gpg --search-keys 'senders email'
eg: gpg --keyserver hkp://subkeys.pgp.net --search-keys 'deletethis@ausics.net'

You'll then be presented with a list of their keys, select the most current key matching the address you are sending to, it should then automatically import that key for you to your keyring

If you have problems, in particular with mail, you may see in some messages GPG/PGP Fingerprint, you can determine their key by using the last eight digits in their fingerprint then try gpg --fingerprint THEIR_KEYID

Verifying Keys

You will from time to time see messages like Good signature but untrusted or unverified or something similar, all this means is the message is likely valid, but untrusted as you are not 100% sure it is truly that person and their right key. The following key signings is not mandatory to effectively use GPG, it is only added as an extra security level, for instance most senior Government officials or corporate directors sending confidential information to each other or their lawyers, accountants etc, should take this extra step.

For organisations and clubs, they sometimes have key signing ceremonies, this is for the web of trust that needs to be created. If you're in an urgent situation and you need to verify immediately and you know the person concerned, you can ring them (or ask them in person) to verify their key, you type in gpg --fingerprint email-address/or Key ID, example: gpg --fingerprint deletethis@ausics.net and look for the Key fingerprint = line, read that line and ask them to verify if it is really them and they will confirm or deny. If you are going to set up trust for someone you do not know, then you should follow the basics, meet the person, in person, they should provide you a printed copy of their key, and produce photo ID, such as a drivers licence so you can know it's really them and you should so same.

The way you do this is issue a gpg --fingerprint your.email > fingerprint.txt and give a copy to each person you want to set up a trust with.

You can print out a page full of these using gpg-key2ps for mass handouts, eg, to print out 2 columns of a full sheet of A4 size paper, if your keyID is xxxx94E you would use:
gpg-key2ps -p a4 xxxx94E > gpg_fingerprints.ps

Where xxxx94E is your key, if you have multiple keys, just add the extra keyID after the first, when done, simply print gpg_fingerprints.ps

Once you get home, take the key ID and import their key, like gpg --recv-keys THEIRKEYID (from their fingerprint slip) then type gpg --sign-key THEIRKEYID you'll be asked if you're sure, hit Y, then enter your gpg pass phrase, then it'll be signed by you.

Optionally, you can then export the signed key by gpg -a -o THEIRKEYID.sasc --export THEIRKEYID
Send this file by email to the person using the email address in their key, then submit this key to a keyserver, gpg --send-keys THEIRKEYID

When they get it (this applies to when you get one from others also) import that file as mentioned earlier (gpg --import THEIRKEYID.sasc) then send your keyID to keyserver gpg --send-keys MYKEYID

Encryption
To encrypt a file, you must have access to the recipients public key, this allows me to sign it and them to decrypt it...
If you do not have the recipients public key, import it as suggested earlier.

Then to encrypt a file, for example called builds.txt and send it to someone at deletethis@ausics.net, you would use gpg -e -r deletethis@ausics.net builds.txt

Now you have your encrypted builds.txt.gpg which you can put on a USB key or email to your friend who then decrypts it using your key.

To decrypt a file, all you need to do is use...
gpg --decrypt file

Encrypting with only Password or Pass Phrase
If you want to encrypt a file for general distribution, you of course may not know all of the recipients, to get around this, you can use the symmetric option which takes a password instead of using keys, eg:
gpg -c builds.txt
-or-
gpg --symmetric builds.txt

This will result in builds.txt.gpg the encrypted version of builds.txt (which will remain untouched)

Tips

You might also want to add into ~/.gnupg/gpg.conf
keyserver hkp://keys.gnupg.net
keyserver-options auto-key-retrieve

To list all keys on your keyring with fingerprints use gpg --fingerprint --list-keys

That's it, I hope your not so confused, Have fun....

Posted by NoelB at 19:49