Full Disclosure

The Internet Dark Age

- Removing Governments on-line stranglehold
- Disabling NSA/GCHQ major capabilities (BULLRUN / EDGEHILL)
- Restoring on-line privacy - immediately

by

The Adversaries

Update 1

Spread the Word

On September 5th 2013, Bruce Schneier, wrote in The Guardian:

*"The NSA also attacks network devices directly: **routers**, **switches**, **firewalls**, etc. Most of these devices have **surveillance capabilities already built in**; the trick is to surreptitiously turn them on. This is an especially fruitful avenue of attack; routers are updated less frequently, tend not to have security software installed on them, and are generally ignored as a vulnerability".*

"The NSA also devotes considerable resources to attacking endpoint computers. This kind of thing is done by its TAO – Tailored Access Operations – group. TAO has a menu of exploits it can serve up against your computer – whether you're running Windows, Mac OS, Linux, iOS, or something else – and a variety of tricks to get them on to your computer. Your anti-virus software won't detect them, and you'd have trouble finding them even if you knew where to look. These are hacker tools designed by hackers with an essentially unlimited budget. What I took away from reading the Snowden documents was that if the NSA wants in to your computer, it's in. Period".

http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

The evidence provided by this Full-Disclosure is the first independent technical verifiable proof that Bruce Schneier's statements are indeed correct.

Full Disclosure

NSA/GCHQ
Sources and Methods
Uncovered

We explain how NSA/GCHQ:

- Are Internet wiretapping you
- Break into your home network
- Perform '*Tailored Access Operations*' (TAO) in your home
- Steal your encryption keys
- Can secretly plant anything they like on your computer
- Can secretly steal anything they like from your computer
- How to STOP this Computer Network Exploitation

Internet Wire-Tapping

WARNING:
BT Broadband Equipment Contain NSA/GCHQ Back Doors

We expose NSA/GCHQ's most Secret Weapon - Control and how you can defeat it!

Dedicated to the Whistle-Blower

Mr Edward J. Snowden.

Table of Contents

Preface

Preface

When the Government, Telecommunications companies and Internet Service Providers, implant secret spying equipment in your home without your knowledge or consent under the guise of something else, then use that equipment to infect your computers and spy on your private network activity (*not the internet*), we believe you have a **right to know**.

It is not possible to make these claims without actual proof and without naming the actual companies involved.

These events coincide with the global surveillance systems recently disclosed and they further confirm the mass scale of the surveillance and how deeply entrenched the Governments are in our personal lives without our knowledge.

The methods we disclose are a violation of security and trust. Good Information Security (InfoSec) dictates that when we discover such back doors and activity, we analyze, understand, publicize and fix/patch such security holes. **Doing otherwise is morally wrong**.

What is revealed here is the missing piece to the global surveillance puzzle, that answers key InfoSec questions which include:

How do the NSA/GCHQ perform Computer Network Exploitation?

We reveal the *actual methods* used by the NSA/GCHQ and others that allows them to *instantly* peer into your personal effects without regard for your privacy, without your knowledge and without legal due process of law, thus violating your Human Rights, simply because **they can**.

Disclosures

The risks taken when such activity is undertaken is “**Being Discovered**” and the activity being “**Publicly Exposed**”, as well as the “**Loss of Capability**”.

Source of this Information

> **"The simple knowledge that we may be clandestinely observed in our own homes provided the determination to find the truth, which we did."**

This information is **not** the result of any knowledge of classified documents or leaks, but based on information in the public domain and our own fact finding mission due to Forensic and Network Analysis Investigations of private SOHO networks located in the UK.

As we detail the methods used, you will see that information was uncovered **fairly**, **honestly** and **legally** and on private property using privately owned equipment.

Our Laws

There is no law that we are aware of that grants to the UK Government the ability to install dual use surveillance technology in millions of homes and businesses in the UK.

Furthermore, there is no law we are aware of that further grant the UK Government the ability to use such technology to spy on individuals, families in their own homes on the mass scale that this system is deployed.

If there are such hidden laws, the citizens of the UK are certainly unaware of them and should be **warned** that such laws exist and that such activity is being engaged in by their own Government.

All of the evidence presented is fully reproducible.

It is our belief that this activity is NOT limited to the UK.

Companies

BT are directly responsible for covertly embedding secret spy equipment in millions of homes and businesses within the UK as our evidence will demonstrate.

BT have directly enabled **Computer Network Exploitation** (CNE) of all its home and business customers.

Technical Nature of this Information

The information described here is technical, this is because, in order to subvert technology, the attackers need to be able to fool and confuse experts in the field and keep them busy *slowing them down*, but regardless, the impact and effect can be understood by everybody.

Your main take away from this disclosure is to understand conceptually how these attacks work, you can then put security measures in place to prevent such attacks.

Credibility of this Research

We first made our discoveries in June 2013 and kept silent so that we could research the capabilities without being detected. As more Edward Snowden disclosures were published it became crystal clear that what we discovered is a major component of the surveillance system.

Those who wish to discredit our evidence, feel free to do so, but do so on a technical level, simply claiming it "*it's not true*" or performing some social attack simply re-enforces it and identifies the "discreditor" as an agent of the NSA/GCHQ or an agent of the global surveillance system.

Our evidence is based on public available UNMODIFIED firmware images.

To verify our claims using UNMODIFIED images requires connecting a USB to serial port to the modem motherboard board which allows you to login (admin/admin) and verify yourself. As most people will find this difficult, we provided a link to third party MODIFIED images based on **official BT release** GNU source code that allow you to telnet to the device (192.168.1.1), this modified version includes the same backdoor. These can be found here:

http://huaweihg612hacking.wordpress.com/

and

http://hackingecibfocusv2fubirevb.wordpress.com/

The MODIFIED images have been publicly available since August, 2012, *long before the Edward Snowden disclosures*.

The methods we published, allows confirmation *without having to open the device*. However if you are suspicious of the MODIFIED firmware from August 2012, simply connect to the USB serial port of your own existing unmodified modem and login to verify, either way the results will be the same.

Privacy vs Security

Loss of privacy is a breach of personal security and the legal violation of privacy is purely a consequence of that security loss.

We've focused on the technical **breach of security** i.e. the Computer Network Exploitation itself and by fixing that you can restore at least some of your personal privacy.

This illustrates that there is no such thing as a balance between security and privacy, you have them **both** or you have **none**.

Motivation

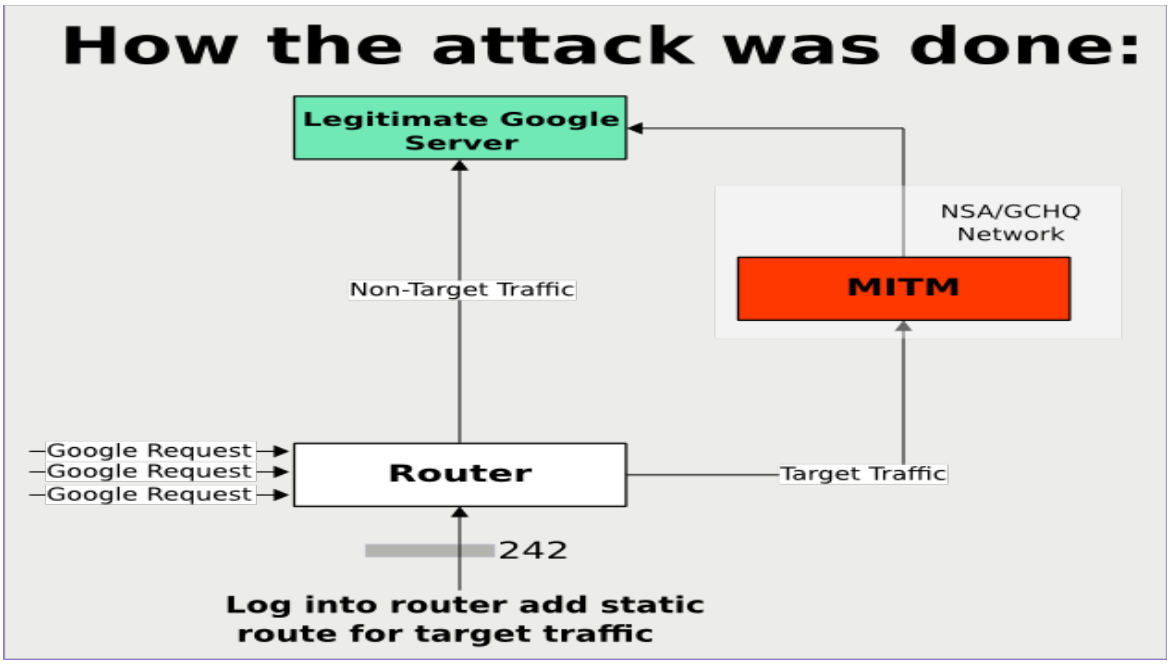
Motivation

After studying in detail the revelations by the Edward Snowden, we realized there was a large *missing part of the puzzle*.

There has been little to nothing published on specifically how the attackers technically achieve their goals. Most information published is based on theoretical situations.

If we don't know how hackers actually achieve these security breaches, we cannot defend against such breaches.

For example, a slide similar to the following was published, of all the slides released, it's uninteresting and easily dismissed, as it simply describes what is commonly known as a theoretical Man-In-The-Middle attack.



The media focus of the slide is of course the **Google's Servers**, and your first thought might be, '*this is Google's problem to solve*', but what if , '**Google Server**' was '**My Banks Servers**', you would probably be more concerned, because that may directly effect you.

But we thought, what if, 'Google Server', was 'Any Server, Anywhere?'

Our investigation led to us uncover, and understand how this attack really works in practice, how it is implemented and the hair-raising reality of its true nature and that is, this not just a back door, but an entire attack platform and distributed architecture.

Terminology

To ease explanation, we are going to use standard security terms from here on.

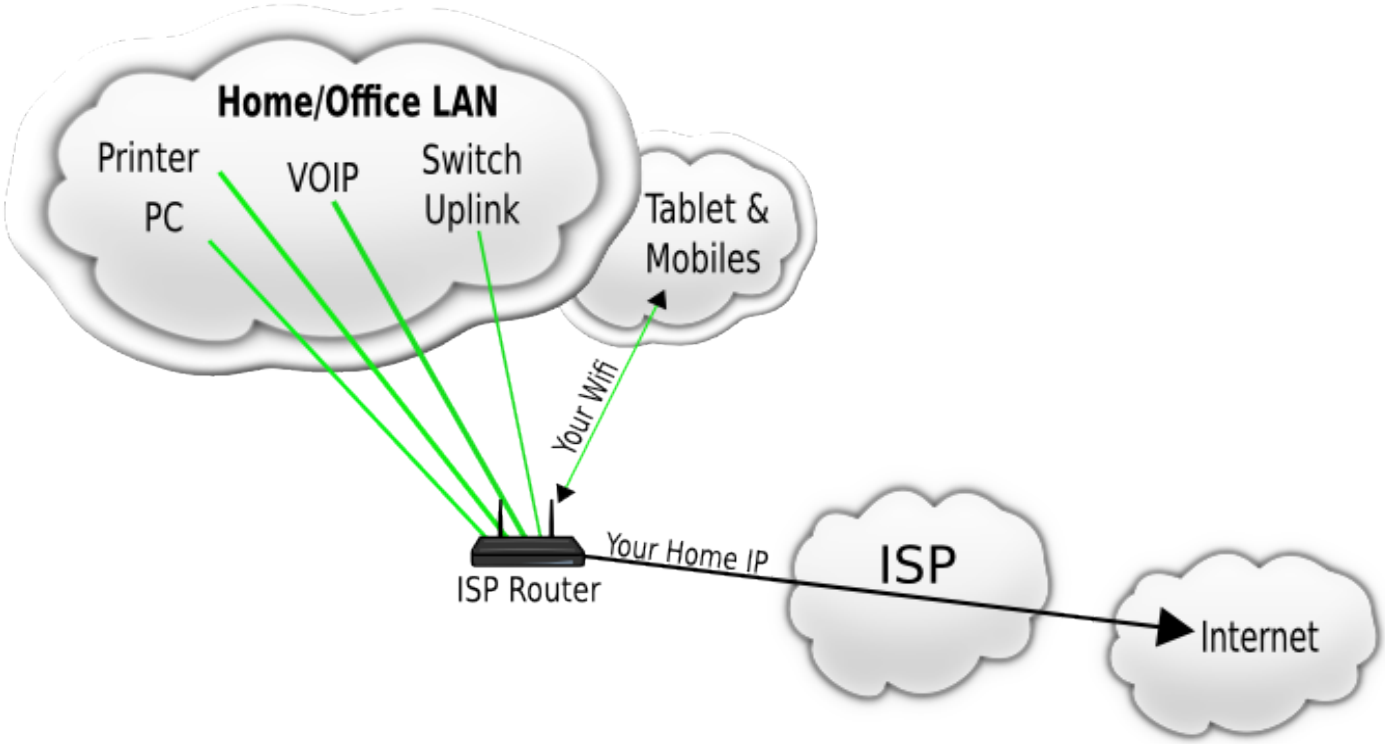
Attacker - GCHQ, NSA, BT Group or any combination.

The Hack – The technical method used by the attackers to illegally break into your home network computers and phones.

Basic Security

Your Home Network

In order to explain how these Computer Network Exploitation attacks work, and how this affects you personally, we must first look at the architecture of a typical home or office network. Look familiar to you?



Most Internet connections consists of an DSL type modem and one or more Ethernet ports attached to the modem that you connect your computers, devices and add-on switches etc.

There are two security factors in operation here:

a) NAT based networking, meaning that your home computers are hidden and all share a single public IP address

b) Your modem has a built-in firewall which is blocks inbound traffic. *The inherent security assumption is that data cannot pass from the inbound DSL line to a LAN switch port without first being accepted or rejected by the built-in firewall*

For the technical minded, these security assumptions are further *re-enforced* if the modems software is open source e.g. using Linux and that its source code is freely and openly available as per the GNU GPL requirements.

Given that the above is the most common architecture on the Internet as it applies to almost every home and office, everywhere, lets now revisit that first slide, but this time, **we ask one simple question**:

> **How do the attackers get between You and Google or some other service?**

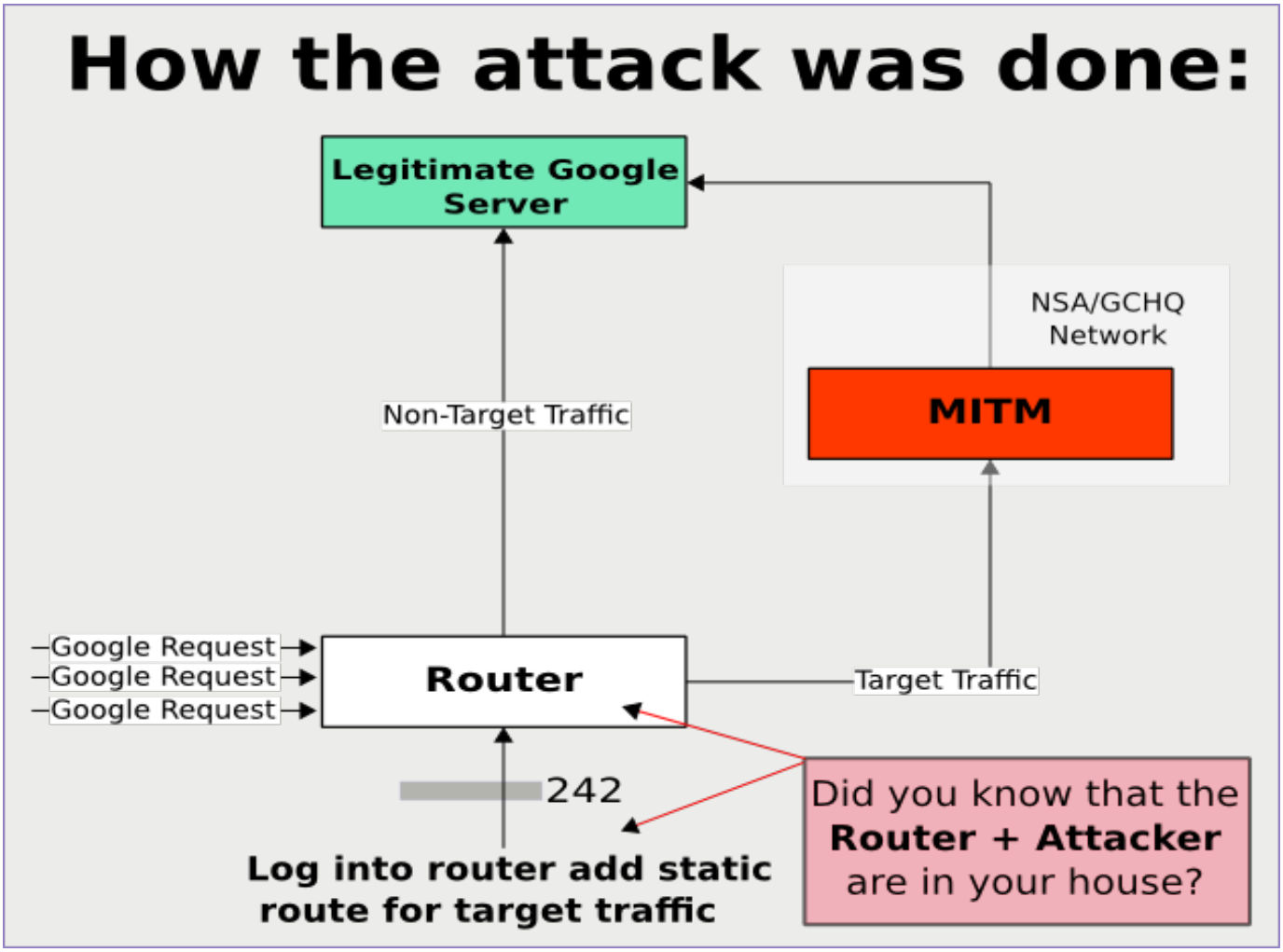
On closer inspection of the diagram you will notice that "**Google Request**" and the **Attacker** (*Log into Router*) share the **same router**, when this slide was released, we all assumed that this router was either Google's own router or some upstream router, that way the **attacker** could intercept packets and perform a **Man-In-The-Middle** (MITM) attack.

However, this would not work for every website or service on the Internet. The **attacker** would need to be upstream *everywhere*!

So where does the attacker hide? Where is this Common Router? again we ask:

> **How do the attackers get between You and Google or some other service?**

Lets examine the diagram one last time.



You guessed it, it's right inside your house. It's the router supplied by your trusted Internet Service Provider (ISP).

If this is true, it means that you are being Internet wiretapped, because the **attacker** has as entered your private property and unlawfully accessed your computer equipment.

Unlike a lawful interception in which a warrant is served on the third party (ISP), the intercept happens at the ISPs property upstream and outside your property.

This is happening in your home or office, without your knowledge, without your permission and you have not been served with a search warrant as is required law.

But worse, is the fact that this **architecture** is designed for Cyber Attacking in addition to passive monitoring as we will detail next.

The Hack

The Hack

This example is based on the UK version of what we are calling **The Hack** using **BT** Internet services. If you are not in the UK and regardless of the service, you **should always** assume that the exact same principles detailed here are **always** being used against you regardless of your country or ISP.

The Hack is based on the **fact** that a second secret/hidden network and second IP address is assigned to your modem. Under normal use, you cannot detect or see this from your LAN, but the **attacker** has direct access to your modem and LAN in your house from the Internet.

How it Works

When the DSL connection is established a ***covert DHCP request*** is sent to a secret **military network** owned by the **U.S. Government D.O.D.** You are then part of that **U.S. D.O.D.** military network, this happens even before you have been assigned your public IP address from your actual ISP.

This spy network is hidden from the LAN/switch using firewall rules and traffic is hidden using VLANs in the case of BT et al, it uses VLAN **301**, but other vendors modems may well use different VLANs. The original slide has a strange number **242** with grey background, we think this represents the VLAN number/Vendor number so BT would be **301**.

This hidden network is not visible from your "*Modem's Web Interface*" and **not subject to your firewall rules**, also **not** subject to any limitations as far as the switch portion of your modem is concerned and the hidden network also has **all** ports open for the ***attacker***.

Other tools and services are permanently enabled inside the modem, which greatly aid the **attacker**, such as *Zebra & Ripd routing daemons, iptables firewall, SSH remote shell server, along with a dhcp client.*

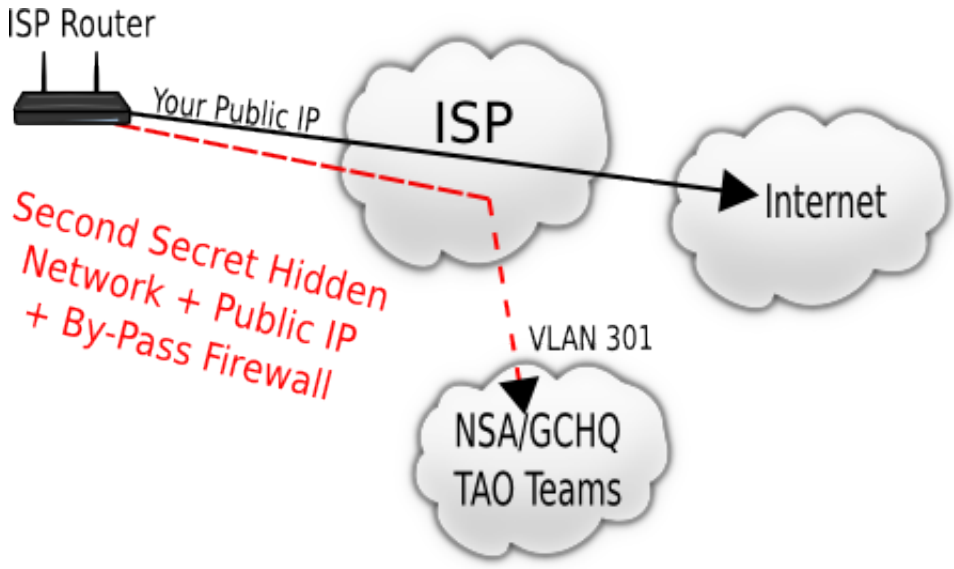
These tools allow the **attacker** *to control 100% of the modem functionality* from the Internet and in an undetectable manner. e.g., the **attacker** can

forward all your DNS requests to their private network, they can selectively route specific protocols, ports or networks or everything to their network and by default they do.

Although the hidden network is owned by **U.S. D.O.D.**, it **is** located within the UK as the ping time to the **attacker's** IP gateway is < 8ms from within the UK.

This clearly demonstrates that the UK Government, U.S. Government, U.S. Military and BT are co-operating together to secretly wiretap all Internet users in their own homes (*with few exceptions*). The modems are provided by BT and ***locked down***. If you cannot confirm otherwise, you must assume that **all** ISPs in the UK by policy have the same techniques deployed.

Your home network actually looks something like the following diagram. To the right is the WHOIS record of the network our modems are automatically connected, yours may vary.




```
NetRange:   30.0.0.0 - 30.255.255.255
CIDR:       30.0.0.0/8
OriginAS:
NetName:    DNIC-NET-030
NetHandle:  NET-30-0-0-0-1
Parent:
NetType:    Direct Allocation
RegDate:    1991-07-01
Updated:    2009-06-19

OrgName:    DoD Network Information Center
OrgId:      DNIC
Address:    3990 E. Broad Street
City:       Columbus
StateProv:  OH
PostalCode: 43218
Country:    US
Updated:    2011-08-17
Ref:    http://whois.arin.net/rest/org/DNIC
```

Whois record says US DOD but attacker located in UK due to low ping times, so assume GCHQ or your local SPOOKS

The above hidden network is created automatically in all our test cases across a wide range of modems.

It should be noted that even before your Point-to-Point over Ethernet (PPPOE) request is issued, this hidden network is **already fully operational**. So much so, that your LAN can be directly accessed even when you think your modem is off-line.

This is an extremely complex and covert attack infrastructure and it's built right into your modems firmware which can also be updated remotely as required by the **attacker** using the built-in **BTAgent**.

The Hack attack is turned **on** by default, but is selectively turned off for special purposes or **specific dangerous customers**, for example, for certain software, firmware and hardware developers/engineers (*which may include you*), so that these people don't discover **The Hack**.

The **attacker** identifies these specific "**threats**" and marks their Internet connections as "NO DHCP", such that the same **dhcpc** requests from their telephone lines are ignored and while these requests are ignored, the hidden network will not appear inside their modem and is much harder to discover.

Firmware engineers usually want to know if the modems are using Open Source software such as Linux and Busybox, in which case they are subject to the terms of the GNU Public License.

These engineers as well as tech savvy users may wish to put their own software (e.g. OpenWRT) on these modems, maybe because they don't trust their ISP, but are prevented by their ISP for obscure reasons.

Most modem providers usually violate copyright law by **not** releasing the source code and BT was no exception to this rule. Only by the threat of legal action did they release the source code. However, BT still prevents the modems from being updated by their customers or third parties.

BT goes to extreme lengths to prevent **anyone** from changing the firmware, and those that come close are first subjected to **Physical and Psychological Barriers** explained later and the few that overcome that, are subjected to a separate NSA/GCHQ targeted **Social Attack** designed specifically to derail any engineering progress made, this is also explained later. These attacks are almost always successful.

During these attacks, BT uses all the information discovered by the engineers to produce firmware updates that prevent anyone else using those same techniques under the guise of security and protecting the customer and this is performed without notice to any customers.

As we move to new generations of hardware, the modems are very sophisticated and very covert, the engineers capable of even attempting to replace the firmware become practically non-existent.

As we detail, the sole purpose of locking the modem is to prevent people discovering that they are actually being wiretapped by BT on behalf of NSA/GCHQ.

As a side note NSA describe Linux/Open Source as Indigenous and a SIGINT target.

(U//FOUO) Indigenous: Non-commercial cryptographic information security system or device developed by a SIGINT target.

NSA documents, describe this means of SIGINT collection as:

MINERALIZE: Collection from LAN Implant

Others include:

General Term Descriptions

HIGHLANDS:	Collection from Implants
VAGRANT:	Collection of Computer Screens
MAGNETIC:	Sensor Collection of Magnetic Emanations
MINERALIZE:	Collection from LAN Implant
OCEAN:	Optical Collection System for Raster-Based Computer Screens
LIFESAVER :	Imaging of the Hard Drive
GENIE:	Multi-stage operation; jumping the airgap etc.
BLACKHEART	Collection from an FBI Implant
PBX	Public Branch Exchange Switch

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123

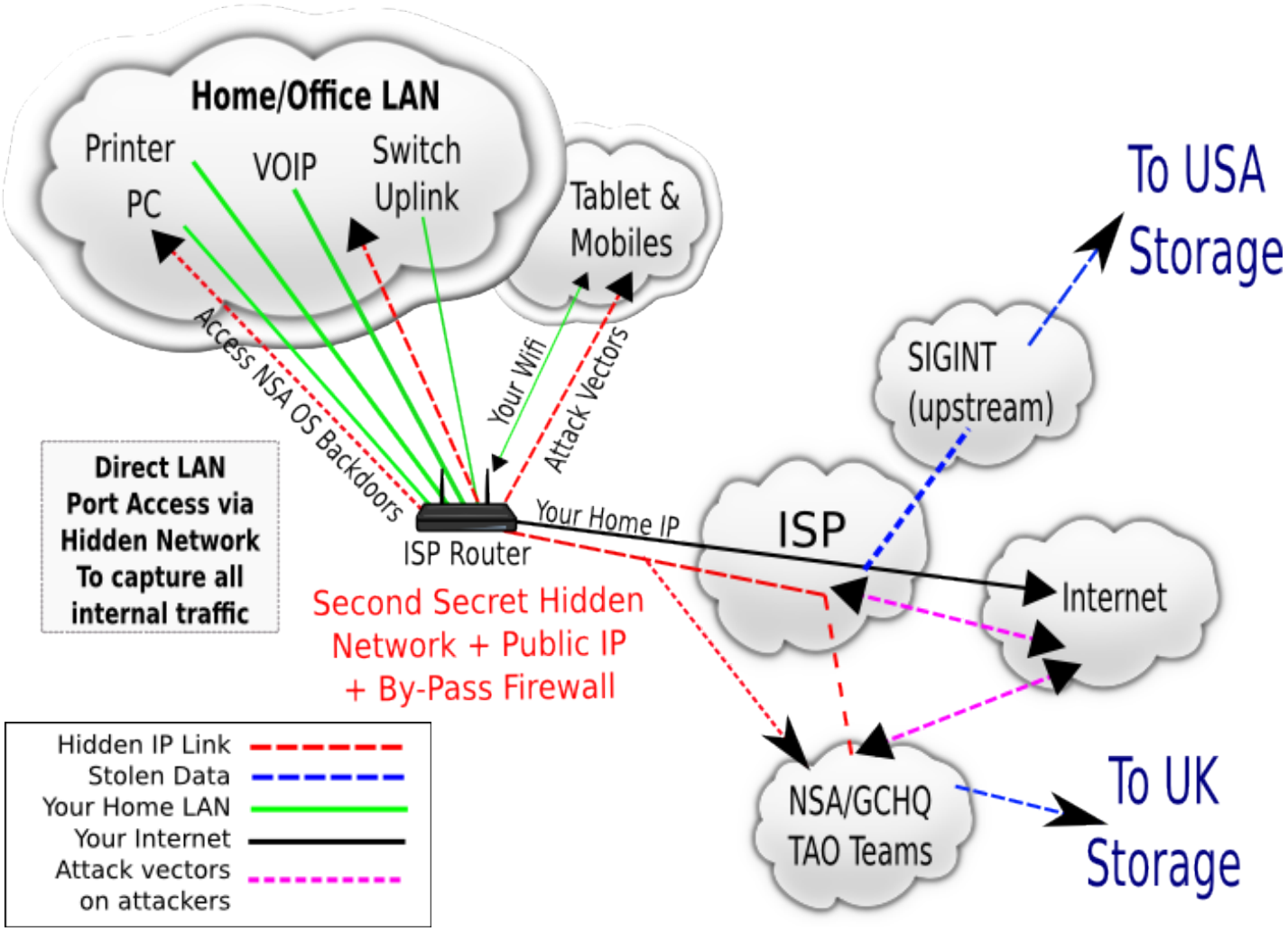
and

RADON	Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of Denied networks using standard on-net tools.

Your Real Network

Your Real Network

The following is a more realistic view of your home network and what is now possible, given the **attacker** now has secret access to your home LAN.



It is now a simple matter to use other tools and methods available to the **attacker** to penetrate your internal computers, this includes:

- Steal private VPN/SSH/SSL/PGP keys
- Infect machines with viruses
- Install key loggers
- Install screen loggers
- Clone/destroy hard drives
- Upload/destroy content as required
- Steal content as required
- Access Corporate VPNs
- Clean up after operations
- Route traffic on demand (e.g. MITM)
- Censorship and Kill Switch
- Passive observation

The Attacks

The Attacks

This section lists the attacks on you that are now possible by the NSA/GCHQ.

Later, we show how you can defend against these attacks and it would be wise to implement our defenses with immediate effect.

Unlike the revaluations so far by Snowden where the attacks occur out there somewhere on the Internet, **these attacks happen in your home/office**.

The attacks listed are the most obvious attacks, some are mentioned in Edward Snowden revelations and referred to as ***Computer Network Exploitation*** (CNE).

Internal Network Access

The attacker has direct access to your LAN and is inside your firewall.

Your modem acts as a server, it listens on lots of ports such as SSH (22) and TELNET (23), so the attacker can just hop on to it (but you cannot).

This is possible because another hidden bridged interface exists with its own VLAN. Firewall rules do not apply to this interface, so the **attacker** can see your entire LAN and is not subject to **your** firewall rules because those rules apply to the BT link (**black line**) not the **attackers** link (**red lines**).

When you scan your BT Public IP address from outside, you may well only see port 161 open (**BTAgent**, more on this later), but when scanned from the **attackers** network, **all necessary ports are open** and with an SSH daemon running (*even the username and password are the basic admin:admin*).

Basically the attacker is inside your home network, and ironically, in most cases, *right behind your actual curtain* (*where the modems are usually located*).

This is the digital version of **Martial Law** with a Cyber Attack Soldier in every home in the country.

The first task of the **attacker** is to perform a site survey and learn as much as

possible about all the devices attached to your network.

All your hardware can be identified by the specific MAC addresses and then fingerprinted for specific protocols and software versions. All this cannot be detected unless you are logged into your ***locked*** modem.

The above is just the base platform of the NSA/GCHQ from which hundreds of types of attacks are now possible, which now include all of the following:

Man-In-The-Middle Attack

The **attacker** controls all outbound **routes**, he can easily perform an HTTPS Man-In-The-Middle attack by forwarding specific traffic for port 443 or destination network to a dedicated MITM network which he controls (*as per previous slides*).

The only thing required is a valid SSL certificates + keys for a specific domain (**which he already has, see below**), The **attacker** is between you and any site you visit or any service you use (*not just websites*). e.g. Skype, VOIP, SSH etc.

The **attacker** simply creates a static route or more easily publishes a Routing Information Protocol Request (RIP) request to the Zebra daemon running in the router for the target network address and your traffic for that network will then be routed to the **attackers** network undetectable by you.

The **attacker** can then use asymmetric routing and upon examination of the requests he can filter specific requests he is interested in and respond to those, but let the target website server or service respond to everything else.

The key here, is, traffic from the target website back to the user *does not then have to go via the **attackers** hidden network*, it can go directly back to users public IP (which would be logged by the ISP).

MITM can be on any port or protocol not just HTTPS (443), for example your SSH connections, all UDP or GRE, PPTP, IPSec etc. or any combination of anything.

All SSL Certificates Compromised in Real-Time

The security of Public Key Infrastructure (PKI) is based primarily on the security of the owners private keys. These private keys are not necessarily required in order to perform a MITM attack.

All that is required is an actual duplicate signed certificate using NSA/GCHQ own private keys. The MITM attack can be as simple as running a transparent proxy and you will always see a valid certificate but unable to detect the attack.

At the point of the proxy all your traffic is decrypted in real-time, at which point targeted packet injection can occur or simply monitored.

It makes perfect sense that the trusted Certificate Authority (CA) actually make a second duplicate SSL certificate with a separate set NSA provided private keys, as the CA never sees the real certificate owners private keys.

When you send your Certificate Signing Request (CSR) and order your SSL Certificate, a duplicate signed certificate is then automatically sent to the NSA and stored in their “CES Paring database” as per Snowden releases.

We must therefore assume that NSA/GCHQ already have a duplicate of every PKI certificate+key (key different from yours).

This means as soon as you revoke or renew your certificate, the NSA is ready and waiting again, allowing them to do real-time decryption on almost any site anywhere across any protocol that uses PKI.

Theft of Private Keys

Home networks are usually very insecure, mainly because only you or family use them, your guard is down and your SSH, VPN, PGP, SSL keys are all vulnerable to theft by the **attacker** and his available methods.

The Hack is the key mechanism that enables these thefts.

As an example of the above, if you use the modems built-in VPN feature, you usually add your certificate and private key to the modem or generate them both via its web interface, at some later time, the **attacker** can just copy these keys to the "CES Pairing database" via his private network, the data collected from SIGINT can later be decrypted off-line or in real-time.

In the case of keys extracted from the modems built-in VPN, the "CES Paring database" now contains the real key/cert pair, meaning the attacker can now attack the VPN server environment directly when that server would have not being exploitable otherwise.

The **attacker** can also mask as the genuine user by performing the server attack from within the users modem (*using the correct source IP address*), this way nothing unusual will appear in the VPNs logs. Once inside the parameter of the VPN server the cycles repeats.

You should **assume** that all "Big Brand" VPNs and routers use the exact same attack strategy and architecture with variances in the specific implementation e.g. Big Brand supports IPSec, Little Brand supports PPTP.

The NSA Bullrun Guide states:

> "The fact that Cryptanalysis and Exploitation Services (CES) works with NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with specific industry partners".
>
> Specific implementations may be identified by specifying Equipment Manufacturer (*Big Brand/Make/Model*), Service Provider (*ISP*) or Target Implementation (*specific modem/router implementation*).

In this disclosure, we are interested in "Target Implementation", because in our example case, BT has covertly implanted these devices in homes where there *is an absolute expectation of privacy*, whereas the other implementations exist within the ISP or large corporations in which you cannot expect privacy.

It's important to remember that "Big Brands" also make small SOHO DSL and

cable modems.

Further evidence of the mass global distribution of this technology to at least the 14 Eyes: USA, GBR, CAN, AUS, NZL, FRA, DEU, DNK, NLD, NOR, ESP, ITA, BEL, SWE and almost certainly many more countries:

Quote from GCHQ regarding their ability to steal your private keys:

> *It is imperative to protect the fact that GCHQ, NSA and their Sigint partners have capabilities against specific network security technologies as well as the number and scope of successes. These capabilities are among the Sigint community's most fragile, and the inadvertent disclosure of the simple "fact of" could alert the adversary and result in immediate loss of the capability.*
>
> *Consequently, any admission of "fact of" a capability to defeat encryption used in specific network communication technologies or disclosure of details relating to that capability must be protected by the BULLRUN COI and restricted to those specifically indoctrinated for BULLRUN.*
>
> *The various types of security covered by BULLRUN include, but are not limited to, TLS/SSL, https (e.g. webmail), SSH, encrypted chat, VPNs and encrypted VOIP.*

And

> *Reports derived from BULLRUN material shall not reveal (or imply) that the source data was decrypted. The network communication technology that carried the communication should* ***not*** *be revealed.*

From the NSA:

5.	(TS//SI) The fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable.	TOP SECRET// COMINT *at a minimum*	1.4 (c)	20291123	(U) Specifying the specific system is protected by an ECI..

The Kill Switch

Actual capabilities uncovered here include the actual ability to apply physical censorship on the Internet by governments directed at individuals, groups, companies, entire countries or the majority of the users of the Internet at once (given *a coordinated government agreement*). This is something that can be turned on globally within minutes.

This “kill switch” is only a small portion of the total capabilities available that are in place right now. Essentially, any operation that can be applied using a single firewall or RIP router, can be applied to every customer at once.

Uploading/Download Content

The attacker can upload or download content via either your public ISPs network or via his private hidden network. The differences is that your ISP could confirm or deny from their logs the user did or did not upload/download content from/to a particular source.

In other words, the possibilities and ability to frame someone cannot ever be overlooked.

When the **attackers** steal content, that information always travels via the private network.

Hacking in to a VOIP/Video Conferences in Real-Time

As an example, it's a trivial matter for the ***attacker*** to route specific traffic for specific media protocol such as VOIP (SIP/H.323/RTSP) etc. to his network in real-time these protocols are usually not encrypted so no key theft is required.

In the case of Skype, it's no stretch of the imagination to assume that Microsoft handed over the keys on day one.

Those they do not redirect in real-time as we know, will be collected via upstream SIGINT.

Tor User/Content Discovery

Users of the Tor network can easily be discovered by LAN packet fingerprinting, but also by those who download the Tor client. The attacker can stain packets leaving your network and before entering the Tor network, making traffic analysis much easier than was previously known.

All Tor traffic can be redirected to a **dedicated private Tor network** controlled by the **attacker**, in this way the attacker controls ALL Tor nodes and so can see everything you do from end-to-end.

This is not something the Tor project can fix, it can only be fixed by the user following our methods.

Tor hidden services should drop all traffic from un-trusted Tor nodes, this way clients running in the simulated Tor network will fail to connect to their destination.

Encrypted Content

The **attacker** is in your network and has all the tools necessary (such as operating system back doors) or zero day vulnerabilities to hack into your computers and steal your VPN, PGP, SSH keys as well as any other keys they desire. Also, content that is encrypted can be captured before encryption via any number of methods when the attacker is already inside your network.

Covert International Traffic Routing

The **attacker** can secretly route your traffic to the U.S. without your permission, consent or knowledge thus by passing any European data protection or privacy laws.

Activists

We have seen many activist groups, protest organizers identified and silenced over the few years, we believe this is the primary method used to capture activists. Knowing the victims ISP would indicate which ISPs are involved.

Destroy Systems

Released documents state that the U.S. Cyber Command have the ability to disable or completely destroy an adversaries network and systems, the first step to this would be to penetrate the adversaries network firewall making secondary steps much easier.

Censorship

The **attacker** has control of the hidden firewall, it is easy for the **attacker** to simply block traffic based on specific ports or based on destination address or network route, for example, the government can block port 8333 at source and therefore block all Bitcoin transactions.

A coordinated attack on the Bitcoin network is possible by blocking ports of Minors around the world. Reducing the hash rate and blocking transactions.

Mobile WIFI Attacks

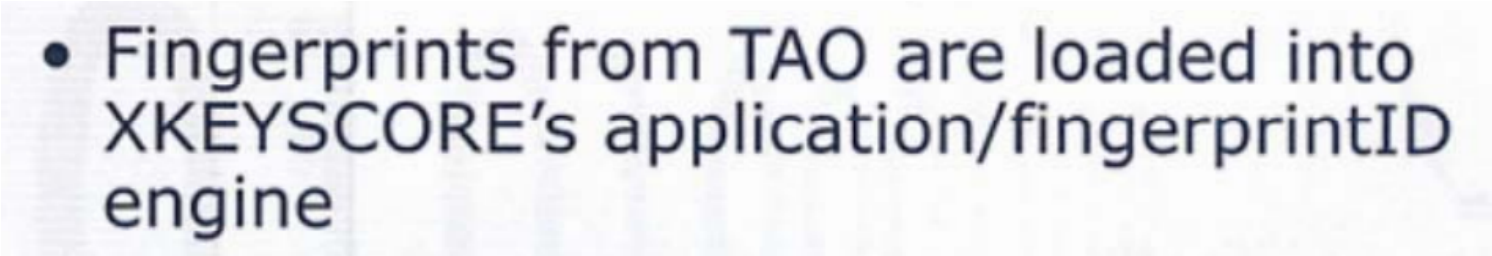
Mobile devices phones/tablets etc, are as easily accessible once they connect to your WIFI network which is, from the attackers perspective, just another node on the your LAN that the **attacker** can abuse.

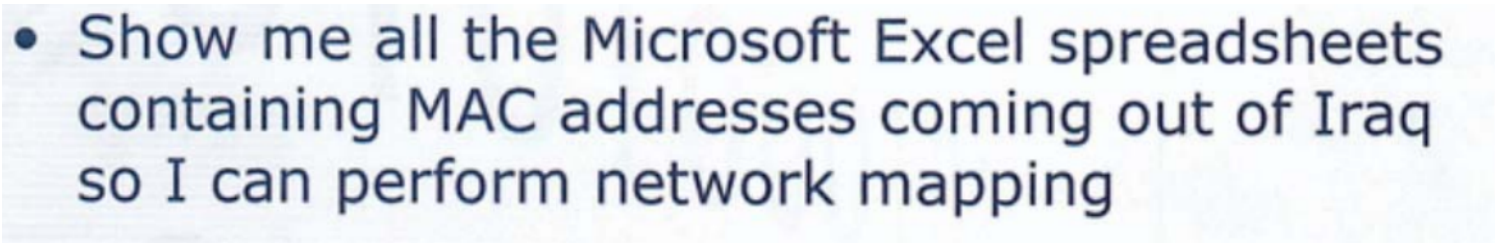
The level of sophistication or advanced encryption in use by your WIFI is no defense because the attacker has gained a trusted position in your network.

All MAC addresses gathered from your LAN are stored in the XKEYSCORE database so they can be used to identity specific devices and specific locations, allowing the attacker to track you without the aid of GPS or where no GPS signal exists.

Document Tracking

Microsoft embeds the physical MAC addresses of the computer inside documents it creates. This allows the source of a document to be identified easily. The following is from the XKEYSCORE PowerPoint.





The Mobile Hack

2G/3G/4G Mobile Attacks

Given the NSA/GCHQ plan to spy on **“any phone, anywhere, any time”**. **The Hack** detailed in this document is a carrier independent method to achieve that goal that works very well. The **attacker** will almost certainly re-use the same strategy for all Mobile phones or wireless broadband devices.

Your mobile phone (2G/3G/4G) is almost certainly subject to this same attack architecture because from the **attackers** perspective, his side of the infrastructure would remain the same regardless of device being attacked.

A mobile phone these days is simply a wireless **broadband modem** + **phone**, so any encrypted messaging system for example can be captured before encryption. Therefore mobile phones are subject to all the same *and many more* attacks as per **The Hack**.

This would mean that mobile phone makers may well be in collusion with the NSA/GCHQ because they would need to implement the equivalent routing and firewall ability in each mobile phone as part of the OS if it was to remain hidden.

The mobile phone version of **The Hack** is also much more difficult to detect than the broadband version. Mobile phones make more use of IPv6 and the overall complexity of IPv6 means that even experts may not know what they are looking at in the routing tables even if they could see them. Carriers often have multiple IPs for different services they provide.

Even top-up mobile phones without any credit can be accessed, for example, the mobiles phones top-up services are always available and their DNS servers are always accessible regardless of your top-credit state.

Modern kernels use multiple routing tables (e.g. ip rule show) for policy based routing, so again unless you confirm who owns a specific IP6 range, it will be difficult to spot, especially as firmware hackers are not even looking for such back doors. Maybe now they will.

We do not provide defense methods for Mobile Phones at this time.

Basic Defense

Basic Defense

Knowing how you are being attacked is half the battle, but in this case, due to the **attackers** abuse of a privileged position and the fact that the **attacker** is your own government and its foreign partners, defense is much more difficult, compared to a common virus, worms or hackers.

One of the best defenses is to take Legal action against BT or your ISP.

If you are serious about your privacy, don't expect any help from your **attackers** (as attackers never help their victims). You must ensure your own privacy. Before we explain practical defenses, here are some good tips.

Secure your end-points

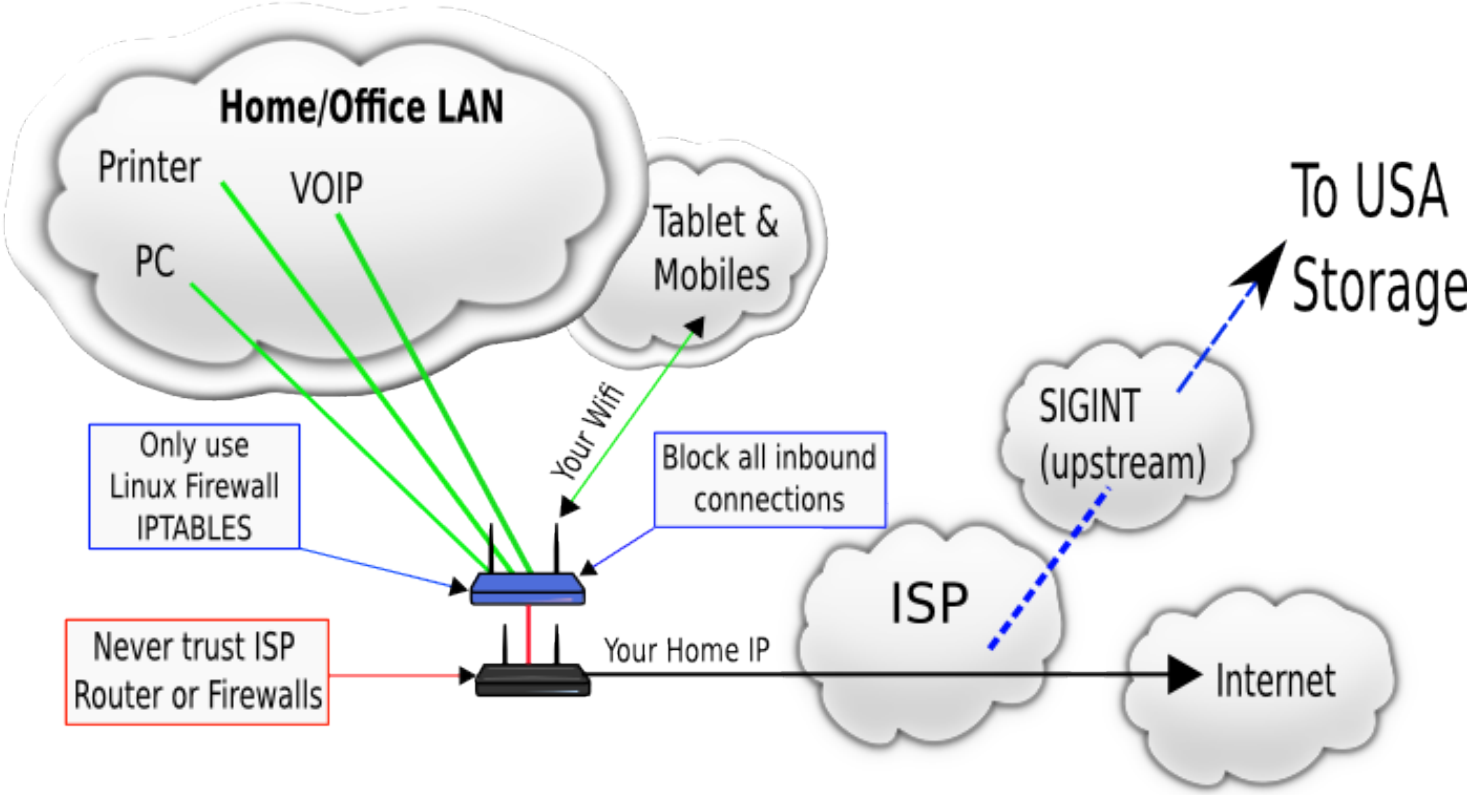
- Never ever trust ISP supplied equipment (e.g. router, firewall, STBs), always consider such devices as hostile and position them in your network architecture accordingly i.e. in the Militarized Zone (MZ)
- Do not use any built-in features of ISP equipment (e.g. Firewalls, VPNs)
- Never ever trust a device that has any closed source firmware or other elements, regardless of the excuses the your **attacker** gives you
- Never trust a device that you cannot change the firmware yourself, regardless of "big brand" names
- Disable all protocols that you don't use or don't understand, especially TR-069 and any other Remote Management features, these are all part of the surveillance **control** system (*e.g. BTAgent firmware update*)
- Always use a second Linux firewall which you control, that you have built
- Control all your NAT on your second Linux firewall not the ISPs supplied router
- Make sure you control all end-points whenever possible
- Ensure that 100% of packets UDP/TCP (*e.g. including DNS*) are encrypted leaving your second firewall (***this is the key to end-point security***), this requires using **Outbound Defense** method described later
- Always use a VPN and remote proxy that you control or trust, disable logging altogether to protect privacy. This requires using **Outbound Defense** method described later

Inbound Defense

Inbound Defense

This defense method against most NSA/GCHQ **Inbound** attacks is fairly easy to implement and not too technical, everybody at a minimum should include this method in their defense strategy.

The strategy will **only** prevent NSA/GCHQ from *hacking* into your home/office LAN. It **cannot** prevent other direct attacks because the **attacker** can still intercept and route all packets leaving your property.



A second Linux firewall device (**blue**) that **you control and manage** is placed in front of the ISP router effectively placing the ISPs router in the Militarized Zone (MZ) i.e. the Internet. A single cable (**red**) is used to link the LAN of the ISP router to the Internet LAN port of the Linux firewall.

Block all inbound access including multicast packets from the ISP router, run DHCP and NAT on your Linux firewall.

Your second firewall can then issue PPPOE requests via its Internet port and create a local ppp0 device which will be its new Internet connection. All packets leaving the firewall will now be PPPOE encapsulated.

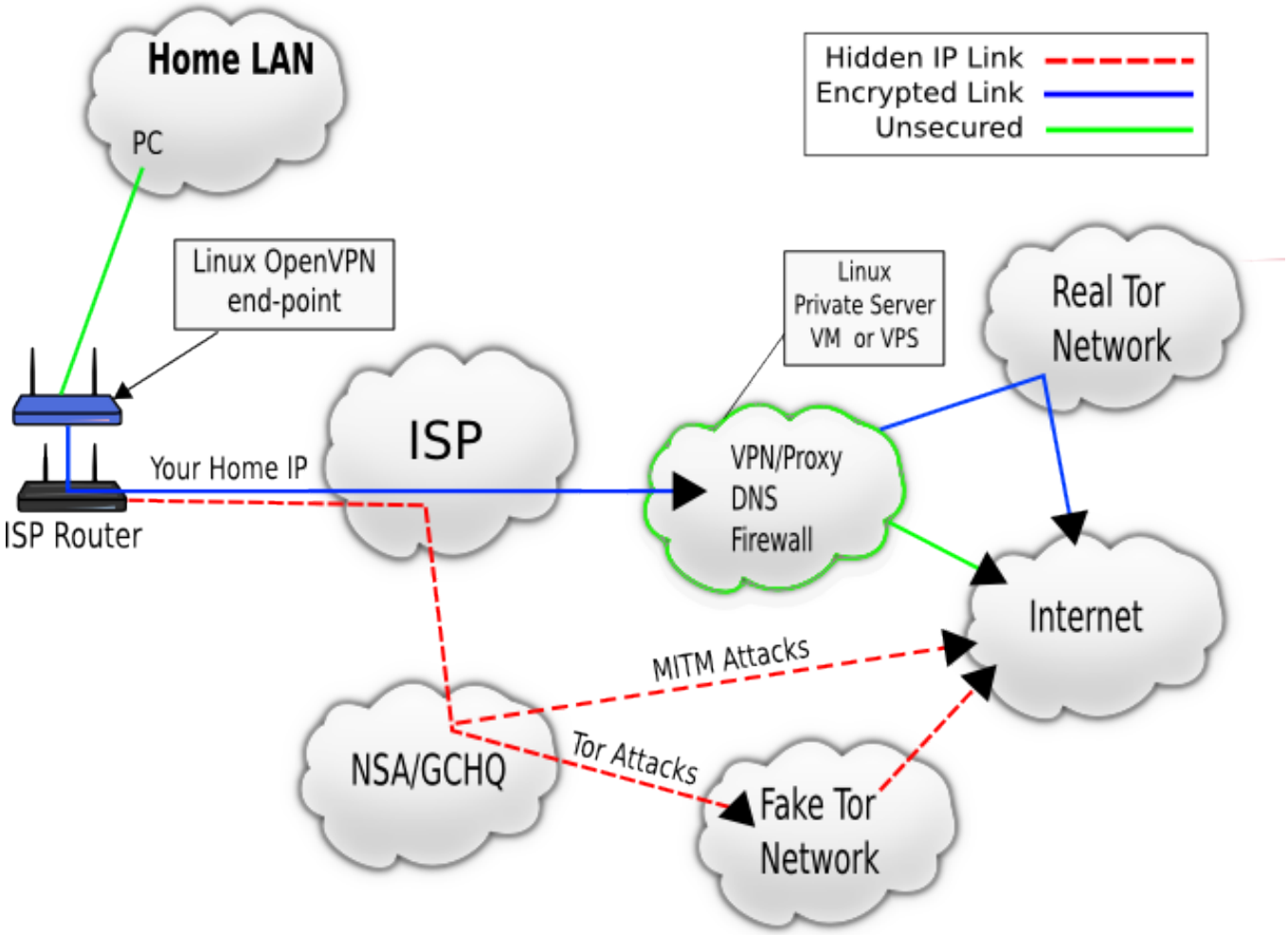
Outbound Defense

Outbound Defense

This defense method should be used against all NSA/GCHQ **Inbound** and **Outbound** attacks. This is the only sure fire method to protect Tor clients.

This defense requires that you (control/*own/rent*) a Server or VM elsewhere on the Internet (far away from your **ISP**) and preferably in a different country.

Run a VPN such as OpenVPN between your Linux Firewall (**blue**) and the your VPS server (**green cloud**), there, you run Squid Proxy and DNS and block all inbound access except from your VPN. Always run your own DNS service on your VM/Server.



An alternative short-term defense is to use **OpenWRT** router software that you install into the modem yourself so that you can confirm no hidden networks or IP addresses exists and that the firewall actually functions.

However, this is technically impossible for must users.

For open source router software visit https://openwrt.org/

More Defense Tips

- Isolate your WIFI from your LAN and limit by MAC address + strong passwords *alternatively*, Isolate your WIFI from your LAN and leave it **open** as a free hot-spot.
- If you are capable, install your own router firmware (openwrt)
- Tell your ISP you do NOT want a router with back doors or malware in it, ask them to confirm in writing that back doors do not exist, this will help you in court when suing them
- Stop using any operating systems that is known to contain back doors
- Only use Tor if you are using **Outbound Defense** method, otherwise you could be using a NSA/GCHQ wonderland version of the Tor network
- It cannot be emphasized enough, never trust closed source routers
- Never use your ISP DNS servers

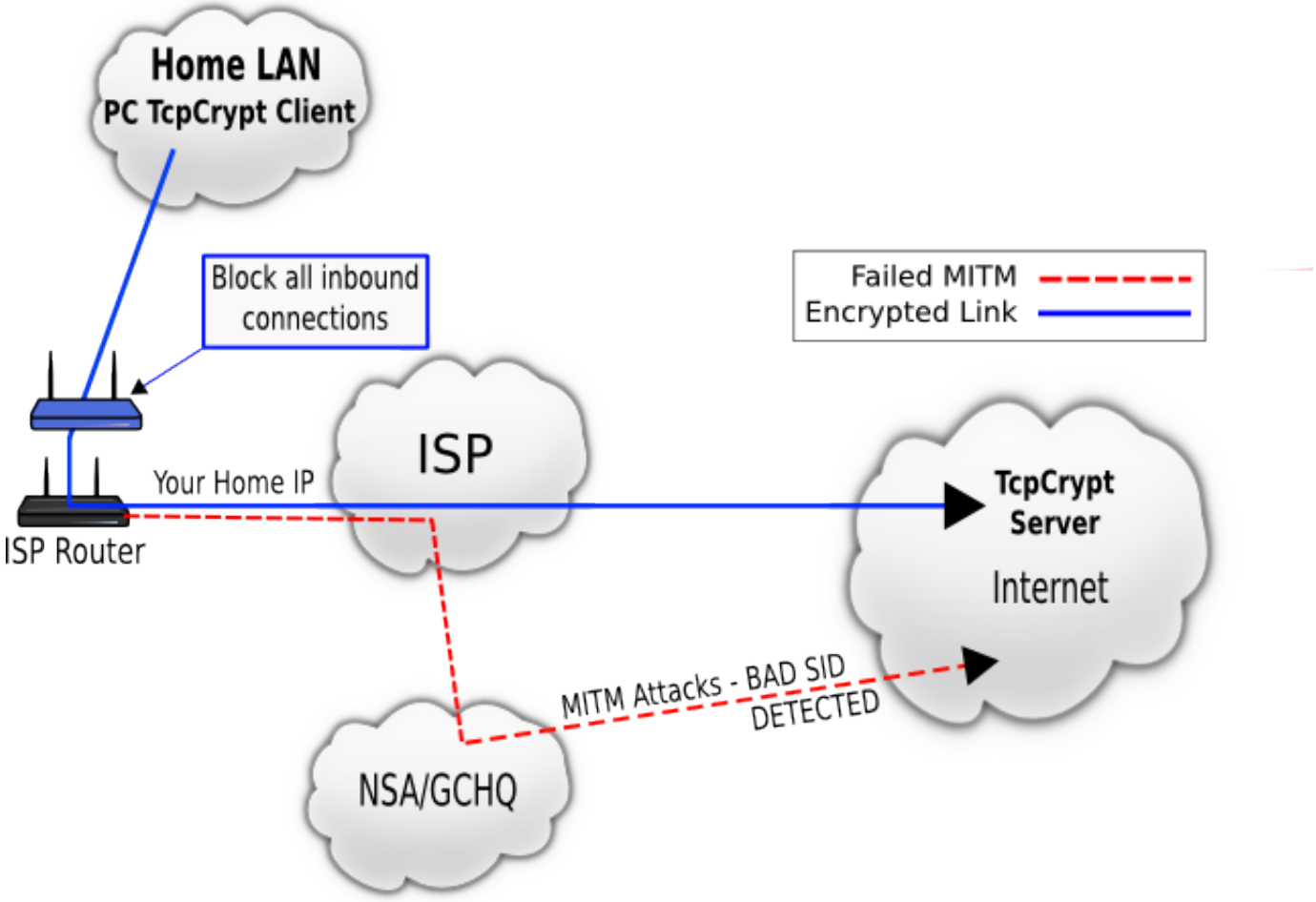
MITM Defense

MITM Defense

Until now, it was not fully understood how a MITM actually worked with regard to how the **attacker** could get in the middle of **any** connection.

Now we know with 100% confidence that the man is **not** in the middle, but in the **modem** and that's how **any** individual can be subjected to MITM attack. We hereby rename this attack **Man-In-The-Modem** attack.

As an alternative defense for the future in place of the previous (*admittedly complex outbound defense*), you could use TcpCrypt. You can prevent this attack by ensuring that your client and servers are running TcpCrypt, which is a TCP protocol extension. It works without any configuration and automatically encrypts TCP connections if both server and client support it or it will fall back to no encryption. It's also 100% **NAT friendly**.



Once installed, this works for any port not just port 80, it will also protects HTTPS, SMTP, SSH and every other service.

TCPCRYPT

TCPCRYPT

TcpCrypt is a very secure approach to many of the problems posed by the NSA/GCHQ because its true native end-to-end encryption and does not require a certificate authority and is free open source software.

The NSA have tried to kill this project a number of times and will continue to do so or limit its use, you must not let that happen.

Let's get all TCP connections Encrypted by default!

Available now free open source for Linux, Windows and OSX visit:

http://www.tcpcrypt.org/

Kernel Developers - please support

TcpCrypt Kernel Module

If you would like to see how NSA and GCHQ agents try to kill projects like this in public, view the video http://www.tcpcrypt.org/talk.php and go to 26:22 and hear the voice of the NSA and then GCHQ.

Frequently Ask Questions

Why Full Disclosure?

We are under no obligation to withhold this information from citizens of Europe, specifically we are not subject to any provisions of the Official Secrets Act of 1998 **as we have never been**:

- a member of the security and intelligence services
- a Crown servant or a government contractor

But more importantly because:

- This information was discovered on private property
- As security conscious users of the internet, we identified serious intentional security flaws which need to be fixed, and fast
- The needs of the many outweigh the needs of the few
- Under the rule of law, the truth is an absolute defense and that is what we present here
- lastly, **Because we can**

Who should read this information

The intended audience is citizens of Europe, but anyone who is or could be a victim of global surveillance systems, this includes everybody in the world now and in the future.

Why does this document exist

When a person(s) or government takes away your **inalienable rights** such as your Right to Privacy (especially in your own home), **you take it back**. This is **not** something that can be negotiated or traded.

What about the debate, the balance?

There is no such thing as a balance between privacy and security, you either have them **both** or you have ***none***.

I'm an American, does this apply to me

The NSA would only use this technique in the U.S. if they really thought they could go undetected. In the UK they have gone undetected until now (*since 2011, as evidenced by the date of the firmware*), you should assume that the U.S. is doing the same to **all Americans** and you should use the defenses as detailed herein as a precaution. We can **turn off the lights** ourselves.

Will stopping BTAgent software stop these Attacks

No. **BTAgent** is just misdirection. It is not required or directly used in the attacks. It can be used to update the firmware of a target modem should the **attacker** need specific functionality on the modem, but this would be unusual. So, killing **BTAgent** is does not help (*you should kill it anyway*).

Is it possible that BT is unaware of this

No, this is their firmware, controlled by BT, publish by BT, updated by BT, they also lock the modems.

My equipment is completely different?

The Hack is an **NSA/GCHQ Global Strategy** and its architecture is independent of a specific make or model of modem or mobile phone, it is also independent of the method transport e.g. dial-up vs. ADSL, DOCSIS, VDSL, Cable modem etc.. It sits at the top of the stack (TCP/UDP etc), so however you connect, it connects. Each implementation will vary and improve with each generation.

You should only use, fully open source, firmware that is publicly verified.

I've never done anything wrong

Yes you have, you have allowed hackers to enter your home network and plant malware that infects your computers, which may now have become part of a zombie army with tentacles controlled by the NSA/GCHQ. This is worst than any virus or worm you can imagine.

How can I verify this myself

Following the instructions in the following sections, you can also create simulations off-line, but that is more technical.

I would like to donate and support your work

Thank you, please see the last page of this document for details.

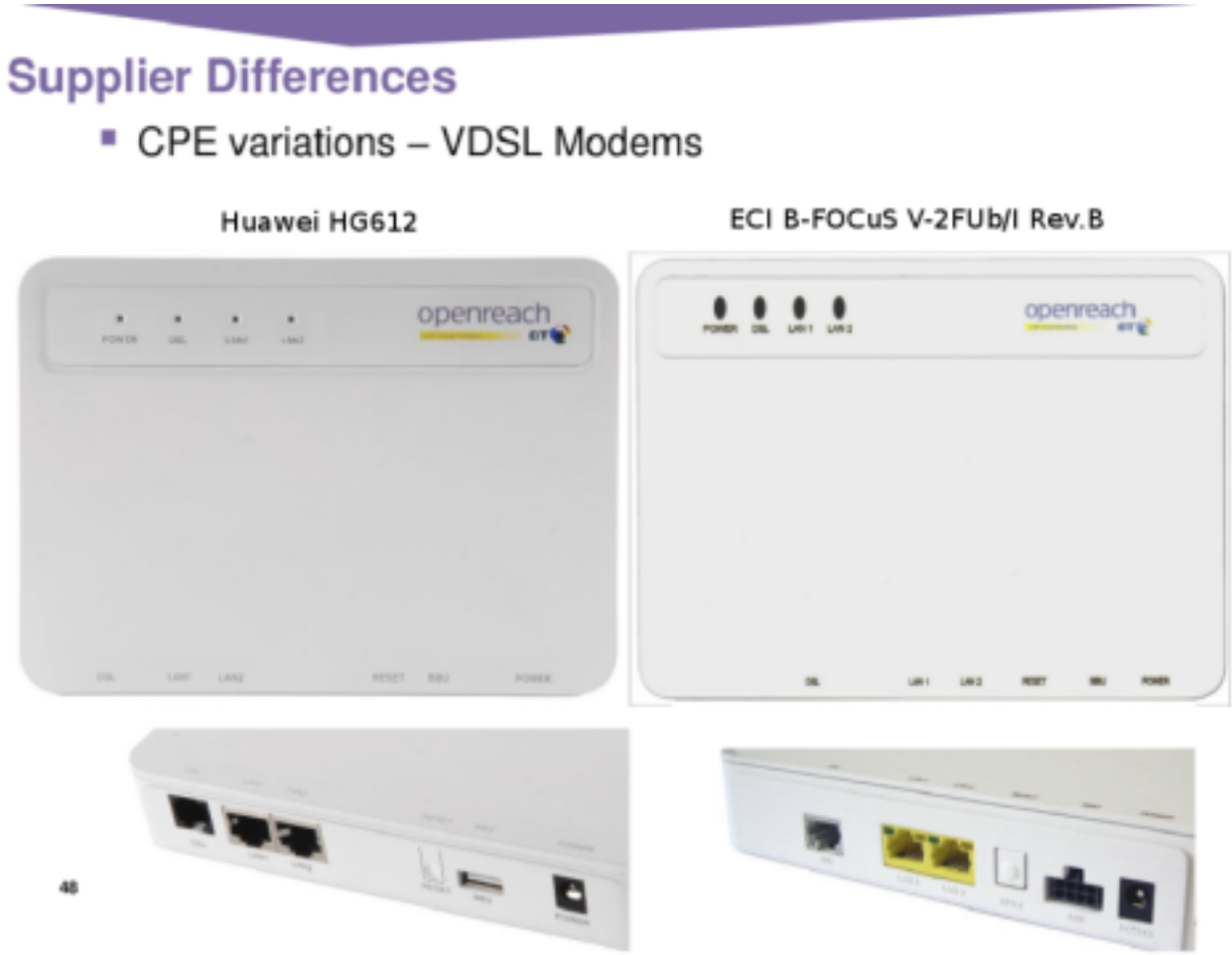
How you can verify

The following section explains how you can confirm that your modem has the GCHQ/NSA back door.

In these examples, we use two **BT OpenReach** white modems, (*but more accurately described as **BT OverReach***) models:

Huawei EchoLife HG612 and **ECI B-FOCuS VDSL2 modem.**

These two look almost identical. The HG612 is an earlier model.



The process of confirmation is slightly different for each modem.

We will show two of ways to verify the back door, the first is something anyone can do and requires just the ping command. The second requires re-flashing the firmware so you can login to the modem itself.

Claims of Huawei modems (Left) having back-doors are false, the vendor (e.g. BT) build and install the OS for these modems. Huawei simply provided hardware. ECI Telecom Ltd, is the provider of the second modem (Right) – the more dangerous of the two.

Easy Confirmation

Step 1. Remove Power from the modem and disconnect the telephone line.

Step 2. On your PC (assumed Linux) add an IP address 192.168.1.100 i.e:
 # ifconfig eth0:1 192.168.1.100 up

Step 3. Start to ping 192.168.1.1 from your PC i.e:
 # ping 192.168.1.1

Step 4. Connect a network cable to LAN1

Step 5. Plug-in the power cable to the modem and wait for about 30 seconds for the device to boot, you will then notice:

64 bytes from 192.168.1.1: icmp_seq=115 ttl=64 time=0.923 ms
64 bytes from 192.168.1.1: icmp_seq=116 ttl=64 time=0.492 ms
64 bytes from 192.168.1.1: icmp_seq=117 ttl=64 time=0.514 ms

You may notice up to ten responses, then it will stop.

What is happening is the internal Linux kernel boots, the start up scripts then configure the internal and virtual interfaces and then turn on the hidden firewall at which point the pings stop responding.

In other words, there is a short window (3-10 seconds) between when the kernel boots and the hidden firewall kicks in.

You will not be able to detect any other signs of the hidden network without actually logging into the modem, which is explained in the next section.

Hard Confirmation

Method 1: (no firmware modification required)
For this method, you need to connect a USB to serial port to the serial port pins on the modem motherboard as detailed here:

http://hackingecibfocusv2fubirevb.wordpress.com/

If you are unable to use this method because it requires opening the modem, please use method 2.

Method 2: (public firmware modification required)
For this method, you will need to re-flash the modem by following the instructions in the document called **hg612_unlock_instructions_v1-3.pdf** which is available from:

http://huaweihg612hacking.files.wordpress.com/2011/11/hg612_unlock_instructions_v1-3.pdf

Or you can navigate to: http://huaweihg612hacking.wordpress.com/
and click "**Unlocked Firmware Images for Huawei HG612**" on the right panel.

Once you have re-flashed your modem, you will be able to login to the modem via telnet as follows.

Note: If your network is not 192.168.1.0, you will need to add the IP address to your PC as explained previously, i.e.

 # ifconfig eth0:1 192.168.1.100 up
 # telnet 192.168.1.1, then login
Username: **admin**, Password: **admin**
then type: **shell** to get the BusyBox shell prompt.

Your telephone line (RJ11) cable should remain disconnected.

To prevent your devices firmware from being updated, disable the following components, as they are not required for confirmation.

Kill the pid of the /bin/sh /BTAgent/ro/start (*See **UN-Hack** later*)

kill pid
killall tftpd sshd MidServer btagent

```
[root@localhost /]# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Welcome Visiting Huawei  Home Gateway
Copyright by Huawei Technologies Co., Ltd.
Login:admin
Password:
ATP>shell


BusyBox v1.9.1 (2010-10-15 17:59:06 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

You will be surprised to learn there exists 16 network interfaces inside the device, most are legitimate, but others are part of **The Hack**.

All IP + MAC addresses have been redacted to protect victims identities.

```
# ifconfig -a
br0       Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2 <--redacted MAC address
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

br1       Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

dsl0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          [NO FLAGS]  MTU:0  Metric:1

eth0      Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0.2    Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          BROADCAST MULTICAST  MTU:1500  Metric:1

eth0.3    Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          BROADCAST MULTICAST  MTU:1500  Metric:1

eth0.4    Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0.5    Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

imq0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:16000  Metric:1
```

```
imq1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:16000  Metric:1

imq2      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:16000  Metric:1

pktcmf_sa Link encap:UNSPEC  HWaddr FE-FF-FF-FF-FF-FF-FF-FF-00-00-00-00-00-00-00-00
          UP NOTRAILERS RUNNING NOARP  MTU:0  Metric:1

pktcmf_sw Link encap:UNSPEC  HWaddr FE-FF-FF-FF-FF-FF-FF-FF-00-00-00-00-00-00-00-00
          UP NOTRAILERS RUNNING NOARP  MTU:0  Metric:1

ptm1      Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

ptm1.101  Link encap:Ethernet  HWaddr 10:C6:1F:C1:27:A2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

ptm1.301  Link encap:Ethernet  HWaddr 10:C6:1F:C1:25:A3
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Lets examine the routing table:

```
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 br0

# ip route show
192.168.1.0/24 dev br0  proto kernel  scope link  src 192.168.1.1

# netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.1:23          192.168.1.100:57483     ESTABLISHED # telnet
tcp        0      0 127.0.0.1:2600          127.0.0.1:33287         ESTABLISHED # Z->rip
tcp        0      0 127.0.0.1:33287         127.0.0.1:2600          ESTABLISHED # rip->Z
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  3      [ ]         STREAM     CONNECTED        766 /var/BtAgentSocket # SPIES Socket
```

Lets see what processes are running: *(duplicate and uninteresting lines remove for brevity)*

```
# ps
  PID  Uid        VSZ Stat Command
    1 0          336 S    init
  101 0              SW   [dsl0]
  116 0              SW   [eth0]
  127 0          504 S    mc
  131 0          380 S    /bin/msg msg
  136 0         1124 S    /bin/dbase
  146 0         1680 S    /bin/cms
  147 0         1148 S    /bin/cwmp
  191 0          328 S    zebra -f /var/zebra/zebra.conf
  193 0          332 S    ripd -f /var/zebra/ripd.conf
  548 0          396 S    dhcpc -i ptm1.301 -I ptm1.301 <--HELLO?
  552 0          504 S    monitor
  570 0          348 S    dnsmasq --conf-file=/var/dnsmasq.conf
  733 0          248 S    tftpd -p 69
  741 0          292 S    sshd -E <-- HELLO?
  762 0         1136 S    MidServer
  766 0          380 S    /bin/sh /BTAgent/ro/start
  780 0          832 S    ./btagent
```

All looks innocent at first. Now, lets **plug-in** the telephone line cable and wait few seconds:

NOTE: We have redacted some IP addresses assigned to us by the **attacker** xx = redacted address.

```
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 br0
30.150.xx.0     0.0.0.0         255.255.xxx.0   U     0      0        0 ptm1.301
0.0.0.0         30.150.xx.1     0.0.0.0         UG    0      0        0 ptm1.301 <-Default?

# ip route show
192.168.1.0/24 dev br0  proto kernel  scope link  src 192.168.1.1
30.150.xx.0/21 dev ptm1.301  proto kernel  scope link  src 30.150.xx.xx
default via 30.150.xx.1 dev ptm1.301
```

We have a new IP address on VLAN 301, this is before any computers are connected and before the PPPOE discover command has been issued from the LAN connected Hub or PC. **The default route sends all traffic to the attacker by default @ 30.150.xx.1**

How close is the attacker? very close, < 8ms

```
# ping 30.150.xx.1
PING 30.150.xx.1 (30.150.xx.1): 56 data bytes
64 bytes from 30.150.xx.1: seq=0 ttl=64 time=7.174 ms
64 bytes from 30.150.xx.1: seq=1 ttl=64 time=7.648 ms
64 bytes from 30.150.xx.1: seq=2 ttl=64 time=7.685 ms
```

NOTE: You are now pinging the NSA/GCHQ

Now lets see what is happening at a socket level (comments on right after #):

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:161             0.0.0.0:*               LISTEN # This is BTAgent
tcp        0      0 127.0.0.1:2600          0.0.0.0:*               LISTEN # This is Zebra Router
tcp        0      0 127.0.0.1:8011          0.0.0.0:*               LISTEN # Transparent tproxy
tcp        0      0 30.150.xx.xx:8081       0.0.0.0:*               LISTEN # This NSA/GCHQ Services
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN # This is DNS
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN # This is SSH Server
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN # This is TELNET
tcp        0     55 192.168.1.1:23          192.168.1.100:57484     ESTABLISHED # This telnet session
tcp        0      0 127.0.0.1:2600          127.0.0.1:36825         ESTABLISHED # This is zebra-rip
tcp        0      0 127.0.0.1:36825         127.0.0.1:2600          ESTABLISHED # This is rip->zebra
udp        0      0 0.0.0.0:69              0.0.0.0:*               # TFTP Server for upgrades
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  3      [ ]         STREAM     CONNECTED       766 /var/BtAgentSocket # Special Agent BT
```

The device is now awaiting the hub/PC to issue a PPPOE discover request, at which point you will receive your “Real Public IP”.

At this point the **attacker** has complete control of the modem and your LAN, extra firewall rules are added the moment the ptm1.301 VLAN device is enabled by the **dhcpc** command.

The UN-HACK

The UN-Hack

If you are able to login to your router (via serial port or LAN), there is a defense which will prevent **ALL** the attacks using **The Hack**. This will **un-hack** the modem and needs to be done after each reboot.

Step 1. Unplug the telephone cable and boot the Modem then login and issue the following commands (in bold), the hash is the prompt (don't type that):

Kill the following processes:
 # killall zebra ripd dnsmasq tftpd sshd MidServer

Kill the pids of the **/bin/sh /BTAgent/ro/start**:
 # kill 766

Now, Kill all of the BTAgent processes:
 # killall btagent

Unmount the BTAgent partition:
 # umount /usr/BTAgent

Remove the attackers VLAN 301:
 # vconfig rem ptm1.301

Kill the rogue dhcpc process with force (-9) or it will re-spawn
 # killall -9 dhcpc

Remove all hidden firewall rules
 # iptables -F -t mangle
 # iptables -F -t nat
 # iptables -F

Step 2. Plugin the telephone cable and the DSL will connect to BT (without the NSA/GCHQ listening).

Step 3. Now start your PPPOE session from your second Linux firewall machine as per the instructions for **Inbound Defense** and **Outbound Defense** as applicable and **Enjoy your privacy**.

Special AgentBT

Special AgentBT

This “special“ software installed on all modems provided by BT called **BTAgent**.

This software listens on port 161, which is the IANA assigned port for Simple Network Management Protocol (SNMP), anyone looking at this process would automatically assume this to be the case. SNMP type programs are often referred to as SNMP Agents.

The primary purpose of **BTAgent** is unpublished, but a version has been partially reverse engineered and the software does download firmware and update the modems flash.

BT responses to queries about their **BTAgent** is to claim that they need to *“remotely manage modems for security purposes”.*

User concerns with BTAgent:

1. *It's closed source*
2. *Users cannot turn it off*
3. *The secretive nature and responses from BT*
4. Users cannot upgrade the firmware using BTAgent
5. Port 161 is open to the public internet

The second (special) purpose of the **BTAgent** is purely reverse reverse psychology and designed to keep you wondering about it, to cause you to waste your time reverse engineering it, when it may well be what it says on the tin and while your thinking about **BTAgent** you're not thinking about the other network interfaces such as **ptm1.301** and the **dhcpc** requests which all look innocent but actually perform the dirty deeds right in the open.

When you reverse engineer **BTAgent** and publish your results, this allows the NSA/GCHQ to target you for other type of **attacks**.

We should remember, that with a single Firmware update from **BTAgent**, it could morph itself and into what we originally feared!

Psychological and Physical Barriers

Barriers

The NSA/GCHQ will do anything and everything to stop the **The Hack** being discovered. The first step is to deal with the majority of users and prevent them from even thinking about opening it up or even touching the modem.

Some of the suggestions listed here may seem extreme, but the less interest created in this box, the less attention it receives from consumers.

1. It's a white box, psychologically it's not a “black box” so it should be safe
2. It comes in a plain brown cardboard box, which contain no words or graphics whatsoever, with a single white bar-code label with make/model of the modem
3. The BT engineer personally carries and installs it in your home, while other components such as BT Home Hub, the more expensive component are sent through the postal system. BT cannot leave this shiny white modem hanging around for a week while they allocate your connection, you may try to open it or do research about it online, and they want to know who is researching it
4. The telephone socket (RJ11) is designed such that when you plug in the telephone cable, it becomes very difficult to remove it, much more so than a standard telephone RJ11. Its not just a case of pinching the lever, you have to pinch and push further in, then remove. This is subtle, but it will prevent a lot of people from even attempting to disconnect the telephone cable, just in case they break it
5. The older model was easy to open, just a few screws, the newer models is almost impossible to open because it is clip locked closed, meaning that you will damage it if you attempt to open it
6. Red Warning Sticker on the back – “Don't cover Air Holes”, wise but scary
7. The only documentation is a single piece of white paper detailing how it should be mounted, there is no instructions about which cables go where, this is designed never to be touched
8. All internal serial port headers are removed so, you can easily hack it
9. The modem is plain white and square, extremely uninteresting, boring, “***Nothing to see here, move along***”,

All of this subtle “Anti-Marketing” for the most advanced BT product?

Social Attacks on Engineers

Social Attacks on Engineers

Having discovered the attack architecture and disabled it, we decided to visit some forums online, we were interested to see if anyone, anywhere is close to uncovering **The Hack** and how the NSA/GCHQ react to such issues.

Generally, there are engineers chatting and sharing pictures of their modems and how they solder wires on to the (usually hidden) serial ports, the discussions usually leads to login and gaining root access of the modem or replacing the firmware altogether.

When engineers start to get really close, something usually extra-ordinary happens, almost like "***superman to the rescue"***, someone who is highly qualified, someone who has built up a reputation of being a ethical hacker/security expert, introduces themselves and produces what appears to be major break-through in gaining access to the modems.

However, because of the "ethical" element, **superman** instead of sharing the method contacts BT, or BT contacts **superman**, directly and they agree to allows BT to fix the flaw (*e.g. giving BT a 30 days head start*) after which, **superman** will publish the method he used.

All things being equal, this is fair enough, but things are not all equal because this was a complete smoke screen, played out to discourage the engineers from further development knowing that in a few weeks "**superman**" will give them access.

Many of the engineers/enthusiast waiting end-up getting caught by upgrades of their modems firmware which then locks them out of the game.

This is a cat and mouse game, and engineers should be very wary of those bearing gifts, their agenda is to slow you down and prevent you from making any progress hoping you will just give up.

You can clearly see this on the BT forums as well others such as http://www.psidoc.com, http://www.kits.co.uk/, http://http://community.bt.com, and others. Reverse engineering is legal, legitimate and it is a great source of innovation.

Counter-Intelligence

Counter-Intelligence

The NSA/GCHQ et al. have being watching and attacking us, it's about time we turned the tables, started defending ourselves and also watching them.

This section is not going to detail specific techniques, but rather suggest overall approaches, some of which we have done over a period of months.

NSA Honeypots

Now we understand the attack architecture, we can simulate the modem in a MIPS Virtual Machine (*BTAgent is not required).*

We can route the NSA/GCHQ traffic to your lab and just let them hack away in a private cloud while we log traffic including how they attempt to use their back doors and other dirty tricks.

You will need to forward and tap VLAN **301** (*in the case of BT et al*) to the virtual modem where you can analyze its traffic in real-time or offline, you should **always** store whatever information you gather forever, (*just like they do*).

After gathering enough evidence, you can then publicize it and take legal action, your logs can be used in court when you sue the conspirators and co-conspirators under the "***Computer Misuse Act 1990***" as well as other laws.

About the Authors

The authors of this document wish to remain anonymous. However we are fully prepared to stand in a court of law and present our evidence.

We are a group of technical engineers, we are not associated with any activists groups whatsoever. We don't have a name, but if we did it would probably be "**The Adversaries**" according to NSA/GCHQ.

Our Mission

Freedom is only appreciated when lost. We are on the brink of a irreversible totalitarian multi-government regime and even though the European Parliament has stated that citizens should not have to defend themselves against state sponsored Cybercrime, the fact remains that our own Governments continue to attack us in our own homes while we sleep.

Our mission is defensive and legal. Our objectives are to expose the sources and methods used by those that harms our personal freedoms and rights and to provide practical information to individuals around the world allowing them to defend themselves against such cyber attacks.

We believe this as well as future disclosures to be in the public interest.

Donations

Our ongoing work is technical, slow, tedious and expensive any donations are very welcome. We only accept bitcoins at this time.

bitcoin:1D6Hj37DS2mPTPm9u7TqS5ocddPHXjmau8

You can also support us by **sending this document to a friend** or host it on your website.