

# COMPUTER & NETWORK SECURITY

Lecture 24:

## The Politics of Cryptography

# THE POLITICS OF CRYPTO

Connectivity is becoming ubiquitous; we are becoming immersed by the Internet, wireless, personal area, RFID and social networks. It's the future. Where gaining access from "any computer on the network" suddenly means every computer on any network. Where soon "computer" will mean your mobile phone, your watch, your wallet, your refrigerator, your pacemaker, your passport, your printer, your photo frame, your glasses. And guess what? They're already infected with viruses. Viruses with End User License Agreements. And McAfee doesn't make a version strong enough for my pet cat...

It's a brave new world where communications and technology stitch together every facet of our lives, allowing everyone to strap themselves on their own personal silicon curve, driven by the network effect. The only problem is, in the digital world everything is made of bits. However, bits have no uniqueness. And bits are easy to copy. So everything you have, whether it be information, privileges, identity, media or digital money- I can replicate with perfect accuracy. As a result, pretty much all of information security revolves around making bits hard to copy; which is as Bruce Schneier says - is like trying to make water not wet. The result - all systems are [insecure](#) in the digital world.

Any risks here?

# THE POLITICS OF CRYPTO

The remarkable thing about Information Security is that it is unique among technical fields; it touches on on business processes, politics, the law, psychology, management, computer science and engineering.

"Be very glad that your PC is insecure - it means that after you buy it, you can break into it and install what software you want. What *you* want, not what Sony or Warner or AOL wants"

-- John Gilmore (EFF)

"We live in a global village, where a judge in a country you've never heard of stops you from getting any business done"

-- Ross Anderson (Cambridge)

"People confuse 'security' and Trustworthy Computing."

-- Craig Mundie (Microsoft)

# NSA

The National Security Agency ("No Such Agency") is the official security (cryptology) body of the US Government.

The primary concern of the NSA is signals intelligence (SIGINT).

The NSA conducts extensive research into both cryptology (both code-breaking and code-making).

"It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. [The] NSA is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the Government."



# NSA

The NSA is the largest employer of mathematicians in the world *and* the largest purchaser of computer hardware in the world.

The NSA's work in cryptology is said to be up to 20 years ahead of the civilian world (though this gap may be closing in particular areas with the recent shift of crypto to the mainstream).

The NSA's budget is classified but is said to be over US\$13B per annum (US\$21M on just electricity).

The US government is cutting costs everywhere... Except the NSA.





# ASD

**The Australian counterpart of the NSA is the Australian Signals Directorate (formerly Defence Signals Directorate), Australia's national authority for signals intelligence and information security.**

**Similar to the NSA, the ASD has two roles:**

- To collect and disseminate foreign SIGINT

- To provide Information Security (INFOSEC) products and services to the Australian Government and its Defence Force.

**Some of the ASD INFOSEC work is unclassified**

- Guidelines for security systems (ACSI 33)

- Evaluated products



# US EXPORT RULES

Cryptography is classed as munitions and appears on the US munitions list (USML) among others. The USML is published as part of the International Traffic in Arms Regulations (ITAR).

Note the main purpose of these restrictions are to regulate encryption products, not authentication products.

In effect, the NSA controls issuance of Commodity Jurisdiction (CJ) permits. To obtain a CJ, the product must be submitted to the NSA for approval.

Anecdotally, it has been said that the NSA never approves anything as "secure" that it can't already break.

# US EXPORT RULES

Since cryptography is classified as munitions in the United States, if you sell cryptographic tools overseas without a license, effectively you're an international arms smuggler.

After WWII, all NATO countries together with Australia, Japan and Spain form part of the Coordinating Committee for Multilateral Export Controls (**CoCom**).

**CoCom** is an unofficial non-treaty organisation chartered to coordinate national restrictions on the export of sensitive military technologies to foreign nations.

The ground is shifting somewhat with the acceleration of technology push of crypto into the civilian world, and CoCom has been replaced with the Wassenaar Arrangement, to which 34 countries are signatories.



# US EXPORT RULES

In 1996, the US government formally offered exporters the ability to incorporate DES (but nothing stronger) into their products.

(good news: everyone uses a standard we made and understand)

The catch is that they would have to incorporate backdoors ("key recovery") into their products within 2 years.

Key recovery is another way of saying key escrow; i.e. a way in which keys can be obtained by the government at will, in a manner which users cannot circumvent:

- Lodgement of keys a priori.

- "Backdoors" in the software.

As a result, most software exported from the US is crippled in some way (e.g. 40-bit keys, key shrinkage)

# ■ AUSTRALIAN LAW :: EXPORT CONTROL

Australia is a signatory to the **Wassenaar Arrangement** (1995), which is an international agreement which aims to control trade in conventional arms and dual-use goods and technology.

The Wassenaar Arrangement treats strong encryption software like high-grade munitions products. Export of all encryption products is banned unless a license is granted by the Minister for Defence.

Export licenses are determined on a case by case basis by the DSD. There is no published policy information to assist potential licensees. Licenses often require some form of key recovery to be granted.

There is no law currently regulating domestic use of cryptography.

# WASSENAAR ARRANGEMENT

---

**Export licenses are determined on a case by case basis by the DSD. There is no published policy information to assist potential licensees. In general, it is believed:**

Australia generally follows the US guidelines.

Applications for export to specific end users in "friendly" countries have a good chance of approval.

Applications for products with "weak" crypto, e.g. 40-bit keys, present no problem, although there is no firm policy.

Products employing non-standard algorithms can be subject to a long and expensive evaluation process.

Products with key recovery receive favourable treatment.

Export via the Internet is regarded as requiring a license, even though the Act does not cover "intangibles".

# WASSENAAR ARRANGEMENT

5. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature and having any of the following:
  5. A. 2. a. 1. a.  
A "symmetric algorithm" employing a key length in excess of 56 bits;  
or
  - b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
    1. Factorisation of integers in excess of 512 bits (e.g., RSA);
    2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over  $\mathbb{Z}/p\mathbb{Z}$ ); or
    3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2. in excess

# WASSENAAR ARRANGEMENT

---

## **Australia recently has made moves to amend it's position on the Wassenaar Arrangement:**

The scope of the General Software Note is to be changed so that shrink wrapped and public domain software which used to be excluded from export control is now to be included.

Previously export over the Internet was not covered by the agreement, being classed as "intangible exports". This is to be brought under the Wassenaar umbrella. Currently only the US controls the export of intangibles.

**<http://www.wassenaar.org>**

**Incidentally, its interesting to read the changes to this agreement, particularly on the sensitive lists..**



# PASSWORDS AND KEY ESCROW

---

In an OECD meeting in 1995, Australia has expressed little interest in judicial use of trusted third parties (e.g. key escrow schemes).

Instead, in the event of issue of a warrant, suspects must render their secret keys.

Obviously this has implications for self-incrimination.

In the United Kingdom, you can be jailed for up to five years for not revealing a password if “national security” is at stake...

In Japan, a hacker posted death threats. The police arrested four people based upon IP addresses and “extracted” confessions.

Except the hacker then proved he hacked into and used their computers and the police were forced to apologise...

# FIXES FOR REVEALING PASSWORDS

TrueCrypt is open source on-the-fly encryption and creates a virtual encrypted hard disk within a file, partition, or entire storage device.

It also offers “plausible deniability”... A hidden volume can be created within another volume.

This means you can end up with two or more passwords:

- Password A: reveals the person’s banking details
- Password B: reveals a porn stash
- Password C: reveals their plans for a dirty bomb

This data is just hidden on disk. If someone starts using your computer, they can just overwrite it on accident. It doesn’t protect itself as that would prove it exists.

# PATENTS

---

In many countries algorithms (including cryptographic algorithms) can be patented.

In the US the lifespan of such a patent is 17 years.

Many of the algorithms we have covered in class are (or have been) protected by patents.

Particularly public key crypto (RSA expired in 2000)

In the US, the NSA works above the patent system:

They may block patents under the Invention of Secrecy Act (1940) and the National Security Act (1947).

They may apply for a patent and block its issue. At some later date when the secrecy order is removed, the patent is valid for 17 years.

# ZIMMERMAN AND PGP

---

In 1991, Philip Zimmerman released **PGP** ("Pretty Good Privacy"), a freeware email security program, on the Internet.

PGP originally used IDEA (symmetric cypher - speed) for encryption, RSA for key management and MD5 for a hash function.

In PGP there are no Certification Authorities; instead it introduces the concept of a "web of trust", or distributed model for key management.

This led to its wildfire growth; PGP is now the defacto standard for securing e-mail communications.

Open PGP (RFC 2440)

# ZIMMERMAN AND PGP

The deployment of PGP upset the US government which placed a lawsuit on Zimmerman that was only dropped in 1996 when the technology was firmly entrenched.

The lawsuit was for violating the Arms Export Control Act.

PGP and the Zimmerman case was really the first time issues dealing with cryptography and privacy hit the mainstream press and marked the first massive deployment of cryptography designed for civilian use.





# COPYRIGHT

---

The digital world has created a massive paradigm shift for the film, book and music industries.

Never before has the ability to breach copyright become so easy and these industries felt so threatened.

As a result there is a proliferation of digital rights management (DRM) schemes.

Unfortunately:

“Making bits hard to copy is like making water not wet [...] All digital copy protection schemes can be broken, and once they are, the breaks will be distributed...law or no law” -- Bruce Schneier

# DMCA

Following lobbying, a treaty was made in 1996 under the auspices of the World Intellectual Property Organisation (WIPO).

The aim was to harmonise treatment of digital copyright.

The US implementation of this was the Digital Millennium Copyright Act of 1998.

The DMCA makes it a crime to "circumvent" copyright protection systems. Here is the language:

Sec. 1201. Circumvention of copyright protection systems

(a) (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work ...

# DMCA

Copyright law has provisions carved out of it in the interests of the public:

- (1) **Fair use** is the right to make unauthorized copies of works for certain protected purposes - mainly for academics, reporting, or criticism. When a student quotes a book in a high school paper, she is making a fair use, and can't be stopped by the copyright owner.
- (2) **First sale** is the right to sell a copy over and over again, once it is made, as long as you don't make any new copies. When you read a book, then sell it to a used book store to be bought and read by someone else, you're exercising your rights under first sale.
- (3) **Limited time** means that copyrights are granted for a limited time. After that time expires, the work goes into the public domain - it can be copied and used by anyone, for any reason.

# SKLYAROV

In July 2001 Dmitry Sklyarov, a Russian PhD student and cryptographer, reverse engineered the encryption algorithms used to protect Adobe eBooks (which wasn't that hard; one of them was ROT13).

As part of this, he created an application which provided a partial decryption of eBooks as a proof of concept.

Elcom, a company he works for then sold it over the Internet.

Sklyarov then came to the US, to discuss his work at a security convention in Las Vegas (Defcon).

# SKLYAROV

Adobe, aware he would be coming to the US, ordered the FBI to arrest him under breach of the DMCA.

Dmitry Sklyarov and his employer, Elcom, were indicted on 5 counts of providing, marketing, and conspiring to provide and market technology to circumvent the encryption of Adobe eBooks.

The case was the first criminal indictment under the Digital Millennium Copyright Act's anti-circumvention provision. Adobe later backed out due to bad publicity (read: stock price)

Sklyarov was released on \$50k bail and later dropped in exchange for testimony. In December 2001, he was allowed to return to Russia.

On December 18, 2002 following a two-week trial in San Jose, California, a jury found that Elcomsoft had not wilfully violated the U.S. law.



# DMCA

Unfortunately the DMCA is worded in such a way that that Engineers and Computer Scientists seemingly are not covered by these rules, and can no longer research software to ensure it provides adequate protection.

However it can be argued that source code is a form of speech, and protection of this is guaranteed in the US under the first amendment of the constitution.

Daniel Bernstein challenged the US government over this. As a student at the University of California, he wanted to publish his work on a cryptosystem called Snuffle.

He was restricted from publishing his paper and code under restrictions on the exportation of cryptography. He was also not allowed to teach foreign students.

He eventually won the right to do both of these, partially using the first amendment by saying his free speech was impinged.



## DECSS

---

The DeCSS case was the first major test of the DMCA.

"The DeCSS case is almost certainly a harbinger of what I would consider to be the defining battle of censorship in cyberspace. In my opinion, this will not be fought over pornography, neo-Nazism, bomb design, blasphemy or political dissent. Instead the Armageddon of digital control, the real death match between the party of the past and the party of the future will be fought over copyright"

-- John Barlow



# CSS

When DVDs were introduced in 1996, Hollywood took fright like many times before when a new medium was released, and said that unless DVD had a copy protection mechanism, first class movies wouldn't be released on it.

A content scrambling system (CSS) was invented.

In combination with this, the world was divided into seven regions, and disks were only supposed to run on players which were enabled for that region.

This was to minimise the loss of a film if it flops, and control distribution timing to increase profits.

Unfortunately for Hollywood, globalisation killed off this idea as the market wants players that will play all movies.

# CSS

CSS was known to be vulnerable at the time DVDs were launched.

In brief CSS works as follows:

CSS uses a stream cypher to encrypt content. The cypher itself was designed to be weak (40-bit keys), and even worse poorly implemented (breakable with about  $2^{25}$  effort) [it has been argued this was to get around US export restrictions on strong crypto].

Each manufacturer of DVD players has a secret manufacturer key  $k_{mi}$

Each DVD disk has a secret key,  $k_d$ .

Each DVD stores the secret  $k_d$  encrypted with all current manufacturer's keys (several hundred of these).

Decryption of content is done by using sector keys which are derived from the secret key  $k_d$ .

# CSS

**Thus leak of any manufacturer key breaks the system.**

System is forward-secure, though (why?)

**Part of the problem also was that the PC is an open platform.**

Thus DVD player software needed to be obfuscated so people couldn't reverse engineer it.

**In addition, the Linux (or non Windows/Mac) market wasn't high on the priority list for DVD software.**

Thus Linux users either had to shift to Windows or break CSS.

Unfortunately most of the world's engineering and computer science students use some form of UNIX.

**In the end, a 16 year old Norwegian hacker from MoRE (Masters of Reverse Engineering) wrote a program called DeCSS which allowed people to play DVDs under Unix-like systems.**



# CSS

The attack was quite simplistic; the DVD player code was decompiled and the manufacturer key for Xing was revealed (which incidentally was not encrypted in the software as it should have been).

After the discovery of Xing's key they were able to derive over a hundred additional keys due to the weaknesses of the encryption algorithm.

Jon Johansen, a 16 year old Norwegian from MoRE, and his father, were arrested for... burglary.

While the MPAA and others were trying to quash distribution of DeCSS, it turns out that the lawyers for the plaintiffs actually had the source code in the appendices of their reply declaration statements.

## CSS :: THE RESULT

Many websites in the US received litigation from the MPAA for hosting the source code (and even simple linking to it).

Ironically, one could go to Disney's (one of the litigants) search engine and search for "decss" and find hundreds of links to the source code.

In particular, the hacker organisation "2600" was taken to court for linking to sites that hosted the source.

The argument was that DeCSS was developed to allow hackers to steal movies

Ironically pirates don't care about DeCSS: they simply copy the whole disk verbatim, including the copy protection.

This battle was fought in the courts with help from the Electronic Frontier Foundation (EFF).

2600 lost.

# AACS

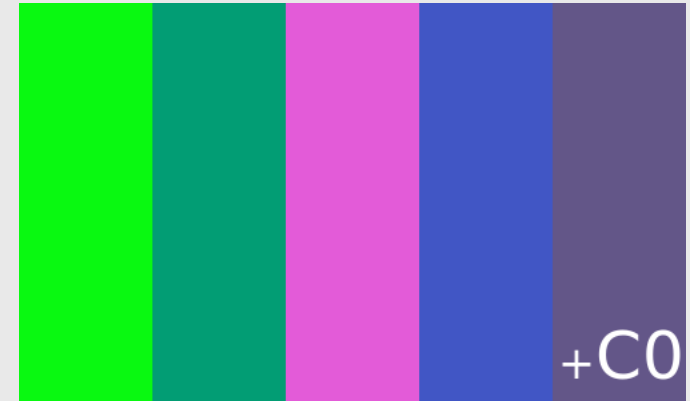
AACS, the next version of CSS, was implemented on HD DVD and Blu Ray.

Improved security: CSS was 40 bit, AACS was 128 bit AES.

One of the keys was eventually leaked. The MPAA and AACS LA began issuing DMCA notices to websites to remove the 128 bit key.

Digg received a DMCA notice and then all hell broke loose. A "cyber riot".

Google results: Tuesday (9.4k), Wednesday (300k), Friday (700k), ...



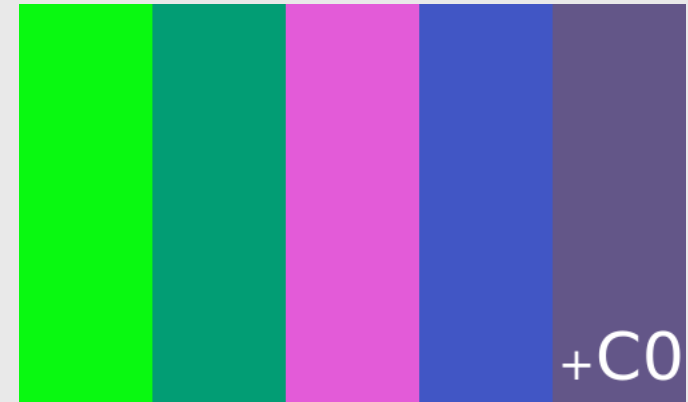
# ILLEGAL NUMBERS

What if you're not allowed to write a specific number... Is that an illegal number?

What happens if take the AACSS key and make it an image, like the top right?

There are also illegal primes – primes that people have found that can be decompressed using gzip to be the original DeCSS program...

This was extended to an *executable* illegal prime.



```
85650 78965 73978 29309 84189 46942 86137 70744 20873 51357 92401 96520 73668 69851 34010 47237 44696 87974 39926 11751 09737 77701 02744 75280 49058 83138 40375 49709 98790
96539 55227 01171 21570 25974 66699 32402 26834 59661 96060 34851 74249 77358 46851 88556 74570 25712 54749 99648 21941 84655 71008 41190 86259 71694 79707 99152 00486 67099
75923 59606 13207 25973 79799 36188 60631 69144 73588 30024 53369 72781 81391 47979 55513 39994 93948 82899 84691 78361 00182 59789 01031 60196 18350 34344 89568 70538 45208
53804 58424 15654 82488 93338 04747 58711 28339 59896 85223 25446 08408 97111 97712 76941 20795 86244 05471 61321 00500 64598 20176 96177 18094 78113 62200 27234 48272 24932
32595 47234 68800 29277 76497 90614 81298 40428 34572 01463 48968 54716 90823 54737 83566 19721 86224 96943 16227 16663 93905 54302 41564 73292 48552 48991 22573 94665 48627
14048 21171 38124 38821 77176 02984 12552 44647 44505 58346 28144 88335 63190 27253 19590 43928 38737 64073 91689 12579 24055 01562 08897 87163 37599 91078 87084 90815 90975
48019 28576 84519 88596 30532 38234 90558 09203 29996 03234 47114 07760 19847 16353 11617 13078 57608 48622 36370 28357 01049 61259 56818 46785 96533 31007 70179 91614 67447
25492 72833 48691 60006 47585 91746 27812 12690 07351 83092 41530 10630 28932 95665 84366 20008 00476 77896 79843 82090 79761 98594 93646 30938 05863 36721 46969 59750 27968
77120 57249 96666 98056 14533 82074 12031 59337 70309 94915 27469 18356 59376 21022 20068 12679 82734 45760 93802 03044 79122 77498 09179 55938 38712 10005 88766 68925 84487
00470 77255 24970 60444 65212 71304 04321 18261 01035 91186 47666 29638 58495 08744 84973 73476 86142 08805 29443
```

## PLAYSTATION 3

Sony protects the Playstation 3 using Elliptic Curve DSA (ECDSA) signing.

Sony failed in their method of random number generation however...

A group, *fail0verflow*, found the ECDSA private key that Sony used. They didn't publish it however for fear of repercussion.

Eventually, a 21 year old who called himself *geohot* published the private key, as well as "Hello World", for the PS3.

A week later, Sony sued both *fail0verflow* and *geohot* over DMCA and Computer Fraud and Abuse Act violations. As part of the settlement, geohot has promised never to hack a Sony product ever again.



# SIGINT

Why would governments wish to cripple civilian cryptography?



# ECHELON

SIGINT has been living in the golden years; for the last few decades communications has been booming- telephone, fax, telex, radio, e-mail, the internet- and virtually all traffic sent across this plethora of media has been in the clear.

En mass harvesting of this information yields a wealth of information; perhaps one of the most valuable sources of intelligence.

In 1947, UKUSA was formed between the NSA (USA), GCHQ (UK), DSD (Australia), CSE (Canada) and the GCSB (New Zealand) to share this intelligence as part of a global integrated electronic surveillance system called ECHELON.



# ECHELON

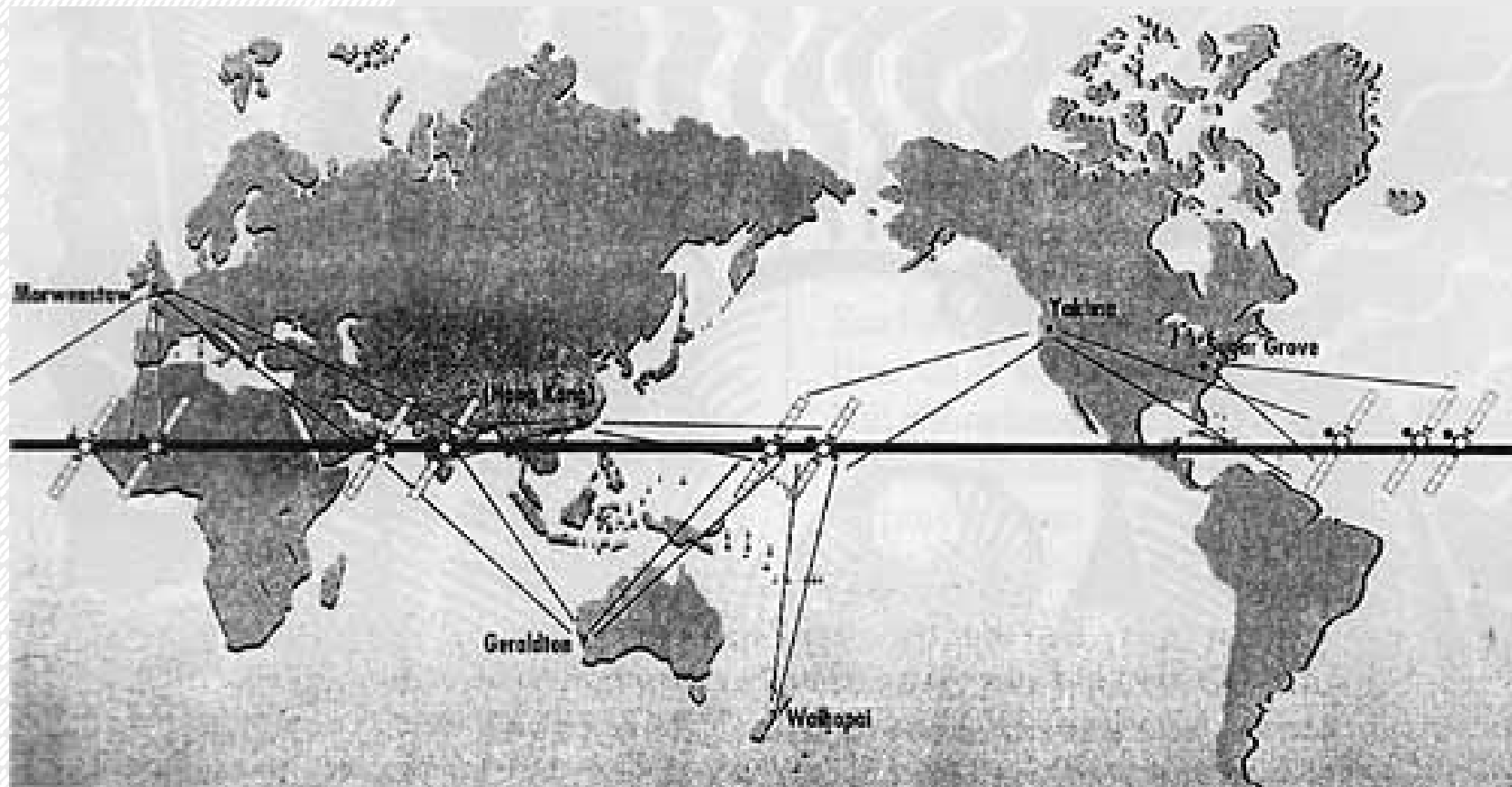
This system has the capability to process in real time a significant portion of the world's communications traffic

Electronic mail, telephone, fax, telex, telegrams, cable etc.

ECHELON runs upon a global TCP/IP network called EMBROIDERY which was larger than the Internet until the 1990s.

ECHELON processes communications in real-time using complex filters which prioritise traffic based upon themes (far more complicated than simple "word" matching). These systems are codenamed DICTIONARY.

# ECHELON



# ECHELON

Message themes were originally identified using n-gram analysis, which is a way of identifying a theme based upon pattern matching (not contextual analysis).

e.g. here are 10 messages intercepted between two groups of paramilitaries, find me more like these.

The beauty of n-gram analysis is that it works in noisy environments (e.g. when the sender can't spell properly or the intercepted communications have interference).

Using n-gram analysis, one does need not even to understand the language (or context) the messages are written in.

Obviously, deployment of civilian cryptography raises the computational complexity of analysing every message that passes through this system by a significant work factor.

Today's systems are likely to be significantly more sophisticated.



# OTHER GLOBAL SURVEILLANCE SYSTEMS

ECHELON is by no means unique.

Many other countries also operate similar networks

Russia (SORM)










France

China



# PRISM (2007)

TOP SECRET//SI//ORCON//NOFORN

    Hotmail®    paltalk.com  AOL mail 

## PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Reporting*

Overview

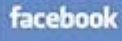
April 2013

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

# PRISM

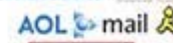
TOP SECRET//SI//ORCON//NOFORN



Hotmail®



YouTube

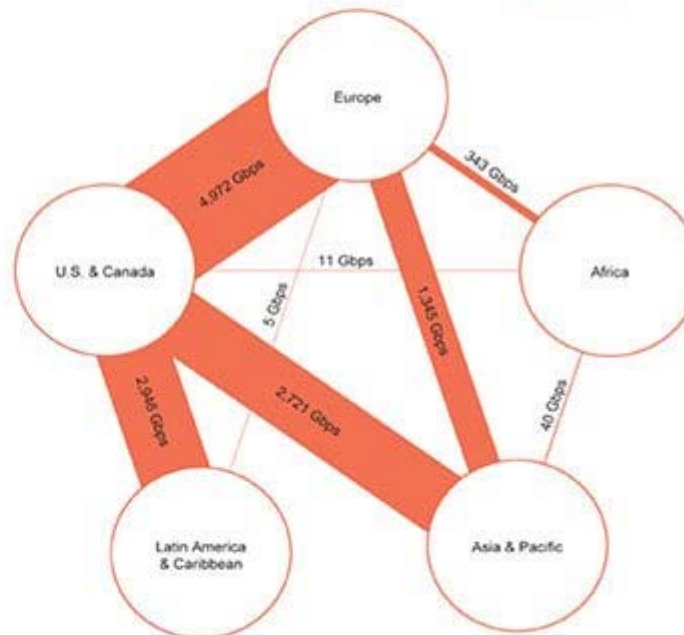


(TS//SI//NF) Introduction

*U.S. as World's Telecommunications Backbone*



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



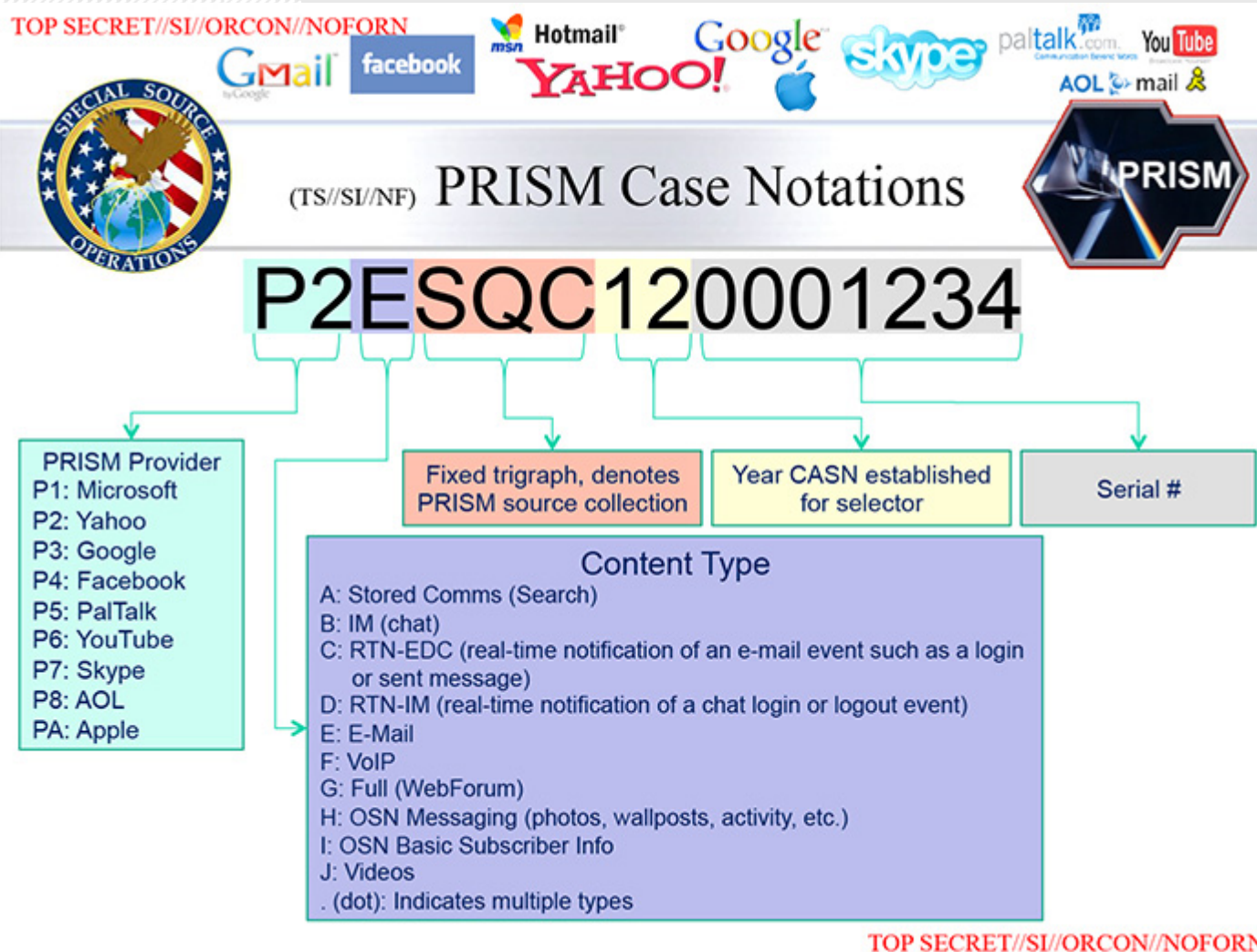
International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

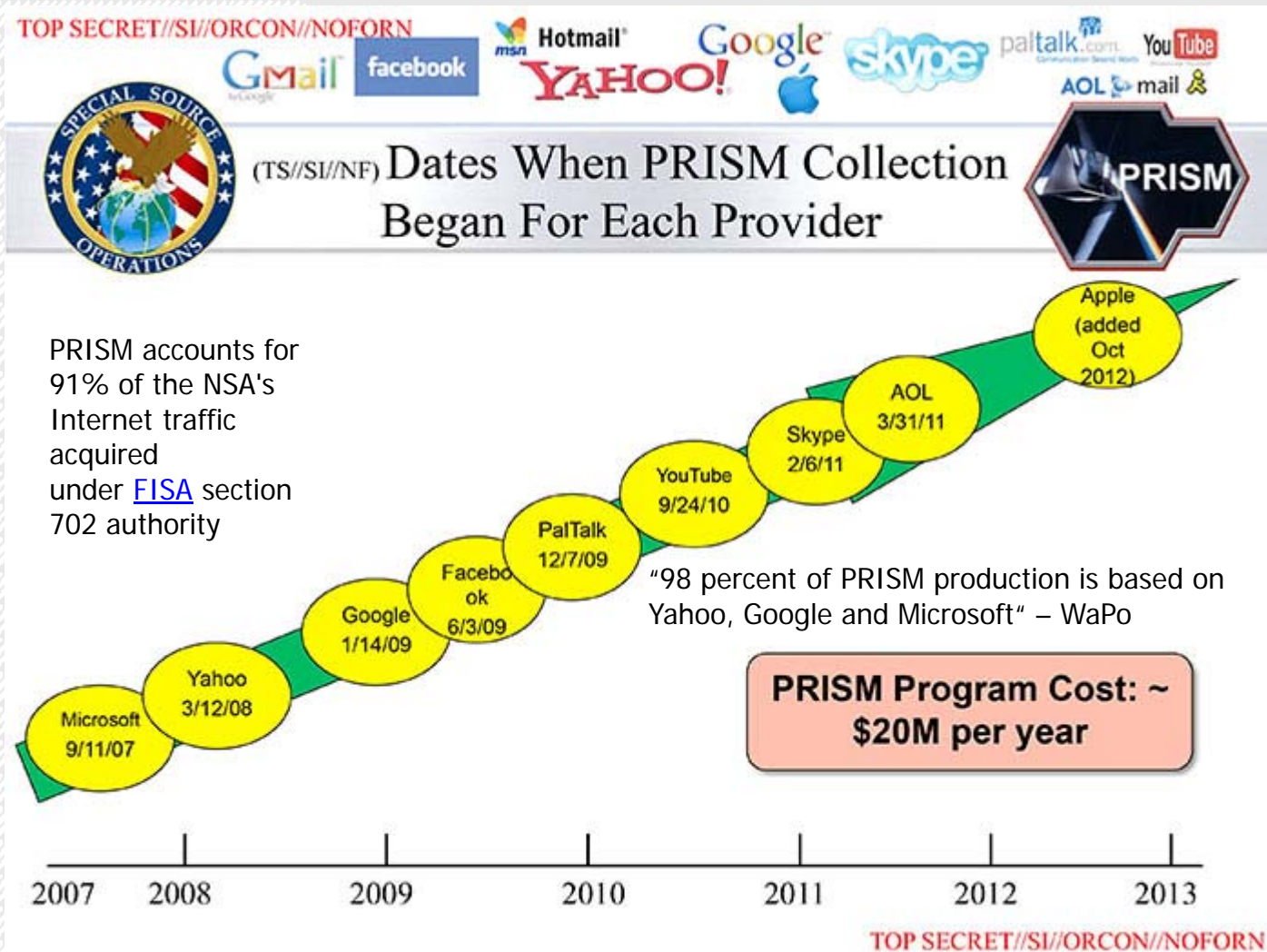
TOP SECRET//SI//ORCON//NOFORN



# PRISM

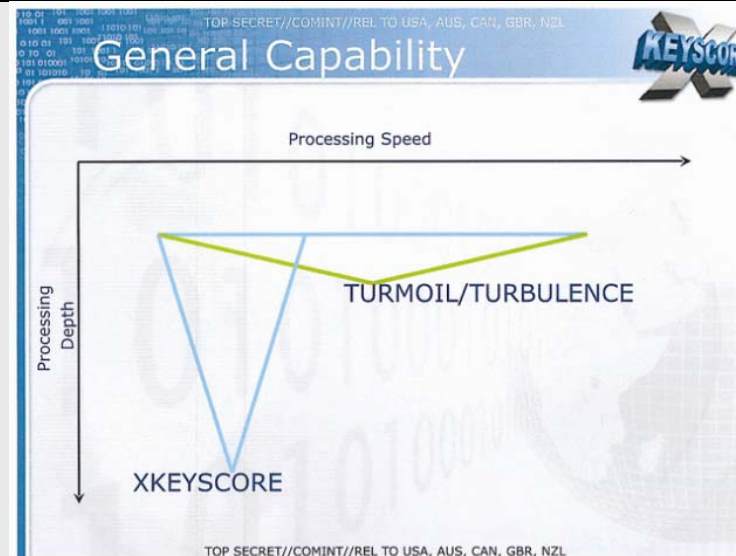
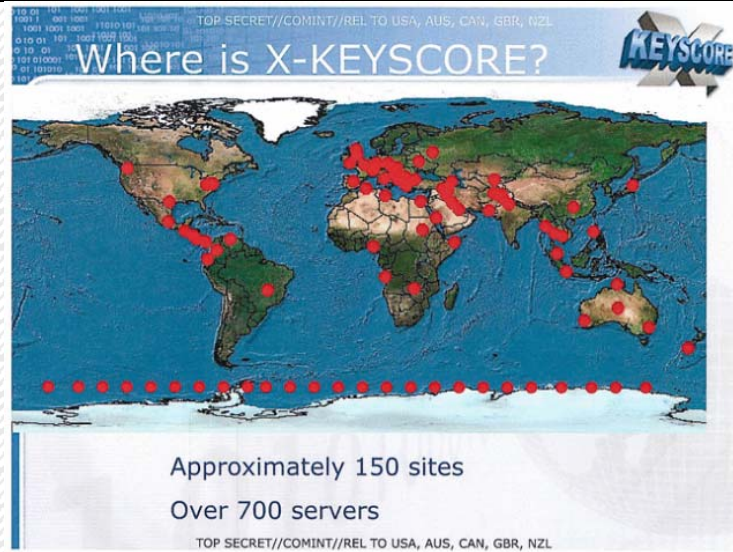


# PRISM





# XKEYSCORE (2008)



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tuple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## What Can Be Stored?

- Anything you wish to extract
  - Choose your metadata
  - Customizable storage times
  - Ex: HTTP Parser

```
GET /search?hl=en&q=islamabad&meta HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, application/vnd.ms-application/msword, application/x-shockwave-flash, */*
Referer: http://www.google.com.pk/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.com.pk
```

No username/strong selector

Connection: keep-alive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# XKEYSCORE (2008)

## Finding Targets

- How do I find a strong-selector for a known target?
- How do I find a cell of terrorists that has no connection to known strong-selectors?
- Answer: Look for anomalous events
  - E.g. Someone whose language is out of place for the region they are in
  - Someone who is using encryption
  - Someone searching the web for suspicious stuff

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Technology Detection

- Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users
- These events are easily browsable in XKEYSCORE
  - **No strong-selector**
- XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days
- **No other system** performs this on raw unselected bulk traffic, **data volumes prohibit forwarding**

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Encryption

- Show me all the encrypted word documents from Iran
- Show me all PGP usage in Iran
  - Once again – **data volume too high** so forwarding these back is not possible
  - **No strong-selector**
  - Can perform this kind of retrospective query, then simply pull content of interest from site as required

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Language Tracking

- My target speaks German but is in Pakistan – how can I find him?
- XKEYSCORE's HTTP Activity plugin extracts and stores all HTML language tags which can then be searched
- Not possible in any other system but XKEYSCORE, nor could it be –
  - **volumes are too great to forward**
  - **No strong-selector**

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



# XKEYSCORE (2008)

## Google Maps

- My target uses Google Maps to scope target locations – can I use this information to determine his email address? What about the web-searches – do any stand out and look suspicious?
  - XKEYSCORE extracts and databases these events including all web-based searches which can be **retrospectively** queried
  - **No strong-selector**
  - **Data volume too high to forward**

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## TAO

- Show me all the exploitable machines in country X
  - Fingerprints from TAO are loaded into XKEYSCORE's application/fingerprintID engine
  - Data is tagged and databased
  - No strong-selector
  - Complex boolean tasking and regular expressions required

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Interesting Document Discovery

- Show me all the Microsoft Excel spreadsheets containing MAC addresses coming out of Iraq so I can perform network mapping
  - New extractor allows different dictionaries to run on document/email bodies – these more complex dictionaries can generate and database this information
  - **No strong-selector**
  - **Data volume is high**
  - **Multiple dictionaries targeted at specific data types**

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Future

- **High speeds yet again (algorithmic and Cell Processor (R4))**
- **Better presentation**
- Entity Extraction
- **VoIP**
- More networking protocols
- Additional metadata
  - Expand on google-earth capability
  - EXIF tags
  - Integration of all CES-AppProcs
- **Easier to install/maintain/upgrade**

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

\_\_\_\_\_

TOP SECRET SC/COMINT/REL TO USA, AUS, CAN, GBR, NZL

# Email Address

**KEYSCORE**

**CMD Display** | **Item Data** | **CMD Search**

**Subject:** RE: Malaysia Tax

**From:** Security Alerts <mailto:securityalerts@malaysia.gov.my>

**To:** securityalerts@malaysia.gov.my

**Cc:** Security Alerts <mailto:securityalerts@malaysia.gov.my>

**Date:** Tue Jan 13 13:48:25 2009

**Attachments:** [VoiceCC-1942-001-0001](#)

**X-KEYSCORE C2C Session Viewer**

Database	Data Notation	From IP	To IP	Flow Port To Port	Session Len
2009-01-13 13:48:25	SMTP:TCP:25	192.168.1.1	192.168.1.1	25	40

**Session:** **From IP:** **192.168.1.1** **To IP:** **192.168.1.1**

**Attributes:** **email\_addresses.txt** **tech.html** **application\_id.txt** **apprec.asd** **xks\_suit.txt** **phone\_number.txt** **fingerprints.xml** **user\_activity.xml** **ip\_ic\_tric.txt**

**IC** **email\_addresses.txt** **FORWATER** **ALTO**

**Flow Port To Port:**

**Flow Port To Port:** 25


**Session Len:** 40

**XKEYSCORE parses out everything it "thinks" is an email address, so don't be fooled by mis-hits**

TO NZL

# Facebook Chat V4 Appid Example

## DNI Presenter Display:



The screenshot shows the DNI Presenter application interface. The main window is titled 'UIS Web Form Display'. On the left, there is a list of form fields: 'img\_id', 'client\_name', 'to', 'email', 'prev\_name', 'img\_text', 'post\_form\_id', 'fb\_id', 'post\_form\_id\_source', '...', 'note[id]', 'note[uid]', and 'note[ci]'. The right side of the window is mostly obscured by a large black redaction box. A red circle highlights the text 'don't still recognize me' within the redacted area, with a green arrow pointing to it. Below the redaction box, text reads 'This information has been redacted'.



# PRISM ONE OF MANY SIGADS

## SIGINT Activity Designator (SIGAD)

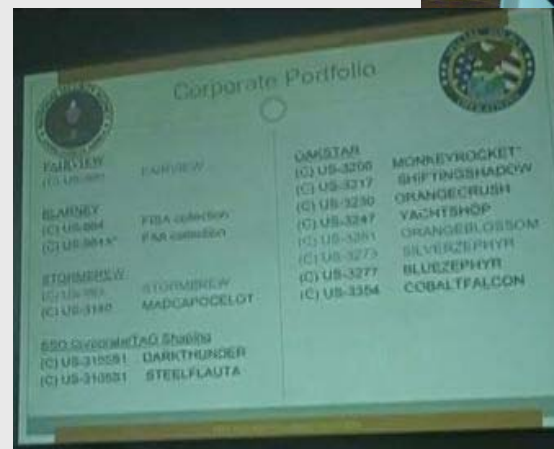
- US-984XN (PRISM) – ISP Level
- US-984 and US-984X (BLARNEY) – includes room 641A

## OAKSTAR – “Upstream”

- US-3206 (MONKEYROCKET) - “Foreign access point”
- US-3217 (SHIFTINGSHADOW) – “Foreign access point”
- US-3230 (ORANGECRUSH)
- US-3247 (YACHTSHOP)
- US-3273 (SILVERZEPHYR)
- US-3277 (BLUEZEPHYR)
- US-3354 (COBALTFALCON)

## STORMBREW - “Upstream”

- US-3140 (MADCAPOCELOT)
- US-983 (STORMBREW)
- DS-200B (MUSCULAR)





# MUSCULAR \* – 2X AS MUCH DATA

"MUSCULAR directly taps the unencrypted data inside the Google and Yahoo private clouds and collects more than twice as many data points ("selectors") compared to PRISM" – WaPo

Jointly operated by GCHQ and the NSA DS-200B

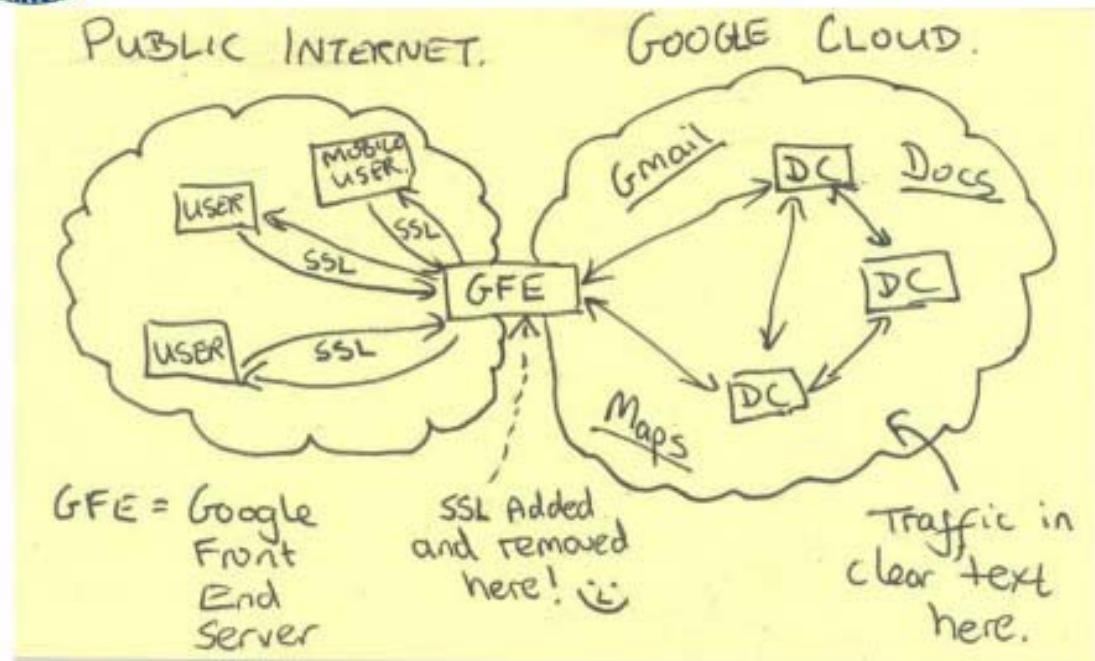
\* No FISA required (taps outside the USA)

TURMOIL processes data from MUSCULAR

Google has subsequently said they will encrypt their data centers



## Current Efforts - Google



TOP SECRET//SI//NOFORN

# WINDSTOP

MUSCULAR (DS-200B) dwarfed by WINDSTOP (DS-300)

Dec 2013 to Jan 2013 MUSCULAR recorded 181 million records. Over the same period WINDSTOP (codename INCENSER) recorded 14 billion.

## Speaker's Notes

From Feb 28 2013: Proposed/imminent latest DO/Volume reduction: Narchive

BLUF: Requested S2 concurrence at S2 TLC on 25 Feb with partial throttling of content from Yahoo, Narchive email traffic which contains data older than 6 months from MUSCULAR. Numerous S2 analysts have complained of its existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4th of the total daily collect).

Background: Since July of 2012, Yahoo has been transferring entire email accounts using the Narchive data format (a proprietary format for which NSA had to develop custom demultiplexers). To date, we are unsure why these accounts are being transferred – movement of individuals, backup of data from overseas servers to US servers, or some other reason. There is no way currently to predict if an account will be transferred via Yahoo Narchive.

Currently, Narchive traffic is collected and forwarded to NSA for memorialization in any quantity only from DS-200B. On any given day, Narchive traffic represents 25% (15GB) of DS 200B's daily PINWALE content allocation (60GB currently). DS 200B is scheduled to be upgraded in the summer of 2013; it is likely that memorialized Narchive traffic, if still present in the environment, will grow proportionally (i.e. double now, to 30 GB/day).

Narchive traffic is mailbox formatted email, meaning unlike Yahoo webmail, any attachments present would be collected as part of the message. This is a distinct advantage. However, it has not been determined what causes an Narchive transfer of an account, so these messages are rarely collected "live".

SECRET//SI//REL USA, GBR



## (U//FOUO) WINDSTOP/2P System Highlights



### MUSCULAR

- Minor circuit move, not collection suite move (so-2013-00762)
- XKS FP updates across TU systems / NArchive throttle update



### INCENSER

- INCS4 config issue (uo-2013-00471)

SECRET//SI//REL USA, GBR

# THE OVERLORD



29.7K



4.9K



798

## CIA's 'Facebook' Program Dramatically Cut Agency's Costs 3:23

The CIA's invention of Facebook has saved the government millions of dollars.

<http://www.theonion.com/video/cias-facebook-program-dramatically-cut-agencys-cos,19753/>

# SECURITY IS NOT AS SIMPLE AS IT SEEMS

---

This course has taught you how to design secure systems.

You've learnt that all systems can and will fail; it's a fact of dealing with the digital world; the key to security is simply to "raise the bar".

You've learnt that when systems fail it is rarely due to the technology and mostly due factors such as the humans using the system.



# SECURITY IS NOT AS SIMPLE AS IT SEEMS

However, you've also learnt that regardless of how secure we can build a system, virtually all major commercially deployed cryptosystems are weak and broken:

- Communications networks including all deployed mobile telephone networks

- Network security protocols e.g. 802.11 WEP

- Security mechanisms deployed in software e.g. Windows

- Commercially deployed cyphers e.g. DES

In addition, we've examined many useful systems we are capable of building that will never see the light of day (e.g. anonymous digital cash).

Furthermore as engineers, when we consider security, we are prevented from practicing fundamental engineering principles e.g. reverse engineering.



# THE ORDER OF SECURITY

## Why?

The interests of governments take precedence over the interests of corporations.

The interests of corporations take precedence over the rights of individuals.

## The Result?

Practically using anything you have learnt in this course might get you into trouble.

Take care and good luck

And remember...



# INFORMATION

## Security Begins With You!

The success of America's campaign against terror depends on you. Don't help America's enemies plan another

attack. Please do everything you can to protect our information, people and critical infra-

structure. Communicate and share information. Protect your computer security when accessing the

Internet. Our enemies are active and we are encouraged before. Don't give them what we need to fight back.



With your help,  
we can keep  
America safe.

# REFERENCES

## Security Engineering

§20 - §21

## For Interest

Wassenaar Arrangement <http://www.parrhesia.com/wassenaar>

Australian Crypto FAQ <http://www.efa.org.au/Issues/Crypto/cryptfaq.html>

DSD <http://www.dsd.gov.au>

NSA <http://nsa.gov>

The Electronic Frontier Foundation <http://eff.org>

ECHELON <http://www.heise.de/tp/english/inhalt/te/6929/1.html>

CRYPTOME <http://www.cryptome.org>

TCPA/Palladium FAQ <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

XBox Case Study <http://www.xenatera.com/bunnie/proj/anatak/>