Crypto Won’t Save You Either

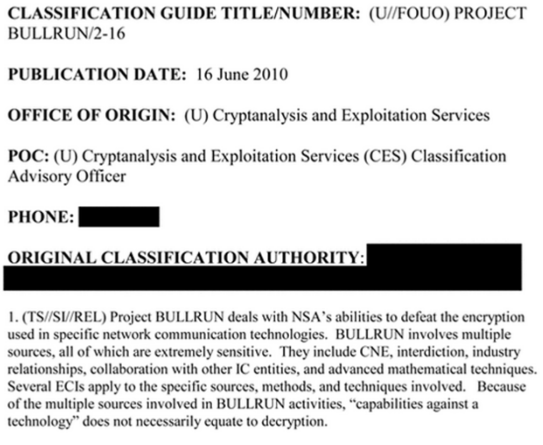
Peter Gutmann

University of Auckland

Sound Advice from the USG

Saw Something, Said Something

Saw Something, Said Something (ctd)



CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

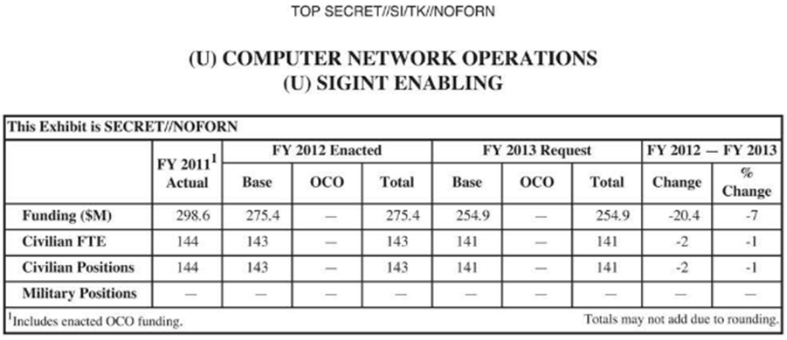
PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

You're not paranoid, they really are out to get you

BULLRUN



TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN

	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1] Includes enacted OCO funding.

Totals may not add due to rounding.

Funded to the tune of $250-300M/year

BULLRUN (ctd)

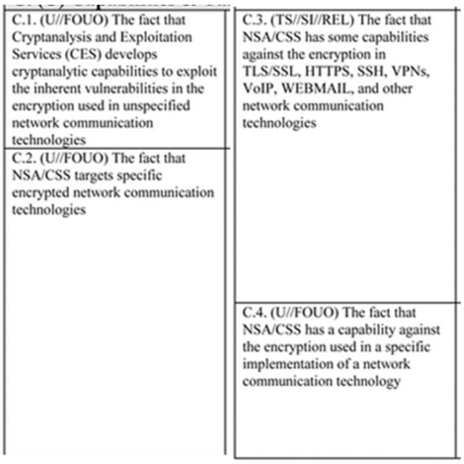
This is fantastic value for money!

Compare the BULLRUN cost to the JSF

- $60 billion development
- $260 billion procurement
- $100-200 million each
(lots of different cost estimates)
- $600-700 million each over
operational lifetime

BULLRUN is a bargain by comparison

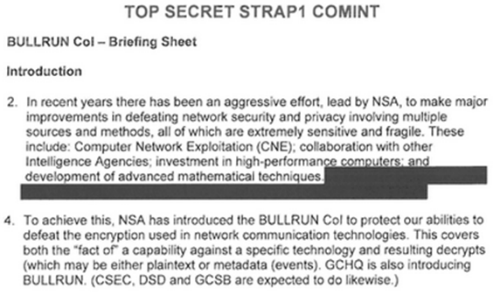
BULLRUN (ctd)



C.1. (U//FOUO) The fact that Cryptanalysis and Exploitation Services (CES) develops cryptanalytic capabilities to exploit the inherent vulnerabilities in the encryption used in unspecified network communication technologies	C.3. (TS//SI//REL) The fact that NSA/CSS has some capabilities against the encryption in TLS/SSL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies
C.2. (U//FOUO) The fact that NSA/CSS targets specific encrypted network communication technologies	C.4. (U//FOUO) The fact that NSA/CSS has a capability against the encryption used in a specific implementation of a network communication technology

"capabilities against TLS/SSL, HTTPS, SSH, VPNs, VoIP, webmail, ..."

BULLRUN (ctd)



TOP SECRET STRAP1 COMINT

BULLRUN CoI – Briefing Sheet

Introduction

2. In recent years there has been an aggressive effort, lead by NSA, to make major improvements in defeating network security and privacy involving multiple sources and methods, all of which are extremely sensitive and fragile. These include: Computer Network Exploitation (CNE); collaboration with other Intelligence Agencies; investment in high-performance computers; and development of advanced mathematical techniques. [redacted]

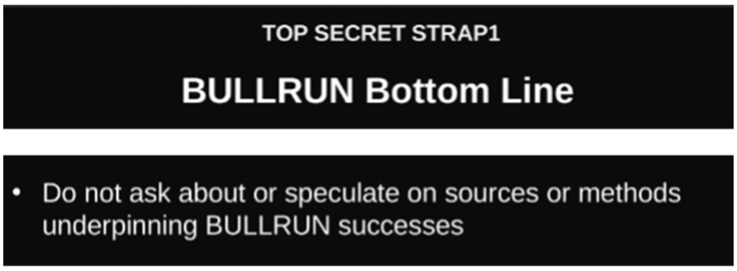
4. To achieve this, NSA has introduced the BULLRUN CoI to protect our abilities to defeat the encryption used in network communication technologies. This covers both the "fact of" a capability against a specific technology and resulting decrypts (which may be either plaintext or metadata (events). GCHQ is also introducing BULLRUN. (CSEC, DSD and GCSB are expected to do likewise.)

"aggressive effort to defeat network security and privacy"

"defeat the encryption used in network communication technologies"

BULLRUN (ctd)

The first rule of BULLRUN club…



TOP SECRET STRAP1

BULLRUN Bottom Line

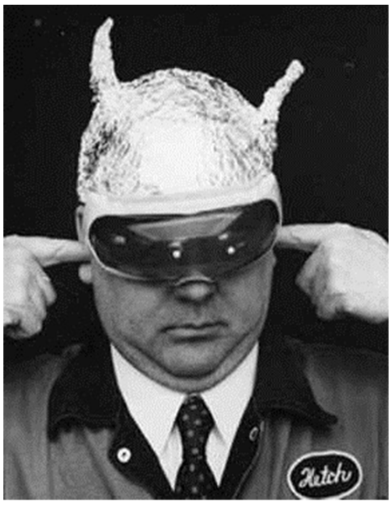
- Do not ask about or speculate on sources or methods underpinning BULLRUN successes

What's that NSAie? Crypto's fallen in the well?

I Know, Bigger Keys!

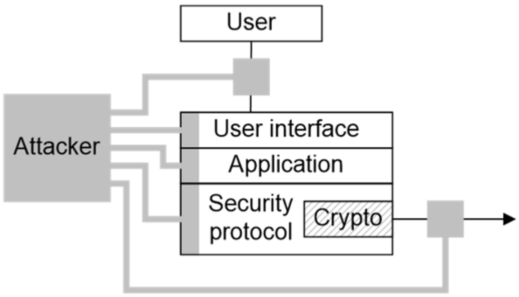
We need to get bigger keys. BIG F**ING KEYS!
— "Split Second", 1992

Quick, do something!



Cue the stannomillinery

Crypto Won’t Save You



Shamir’s Law: Crypto is bypassed, not penetrated

> Cryptography is usually bypassed. I am not aware of any major world-class security system employing cryptography in which the hackers penetrated the system by actually going through the cryptanalysis […] usually there are much simpler ways of penetrating the security system — Adi Shamir

Example: Games Consoles

All of the major consoles use fairly extensive amounts of sophisticated cryptography

- PS3
- Wii
- Xbox
- Xbox 360

Example: Games Consoles (ctd)

Measures include

- Signed executables
- Encrypted storage
- Full-media encryption and signing
- Memory encryption and integrity-protection
- On-die key storage and/or use of security coprocessors
  - If you asked someone a decade ago what this was describing, they'd have guessed an NSA-designed crypto box

All of them have been hacked

- In none of the cases was it necessary to break the cryptography

Crypto Won't Save You

Amazon Kindle 2

- All binaries signed with a 1024-bit RSA key
- Jailbreakers replaced it with their own one
- Later versions of the Kindle were similarly jailbroken without breaking the crypto

HTC Thunderbolt

- Signed binaries
- Signed kernel
- Signed system-recovery/restart code
- Remove the signature-checking code

Crypto Won’t Save You (ctd)

Samsung Galaxy

- Firmware signed with 2048-bit RSA key
  - Round up twice the usual number of key bits!
- Modify firmware metadata to load it over the top of the signature-checking code

Nikon Cameras

- Sign images using a 1024-bit RSA key
- Signature encoded in photo EXIF data
- Signing key encoded in camera firmware…

Crypto Won’t Save You (ctd)

Canon Cameras

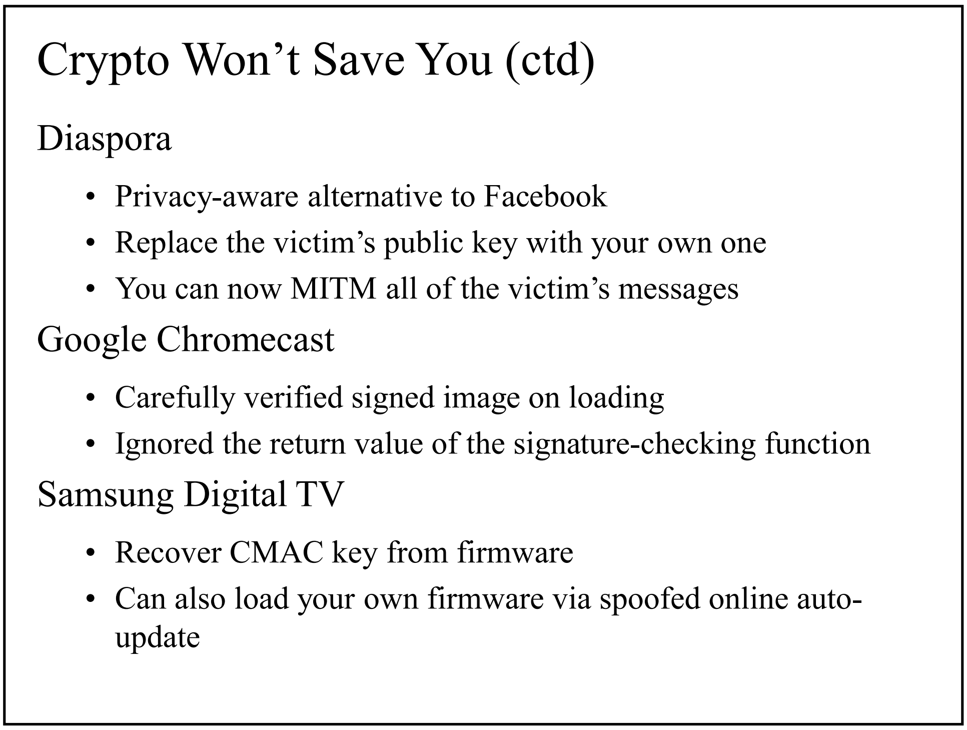
- Authenticate images using HMAC (keyed hash function)
- HMAC is symmetric: Verifier needs to know the key as well
- Shared HMAC key encoded in camera firmware…

Airport Express

- Signs data with a 2048-bit RSA key
- Recover the private key from the firmware image

Asus Transformer

- Obtain AES Secure Boot Key via unspecified means



Crypto Won’t Save You (ctd)

Diaspora

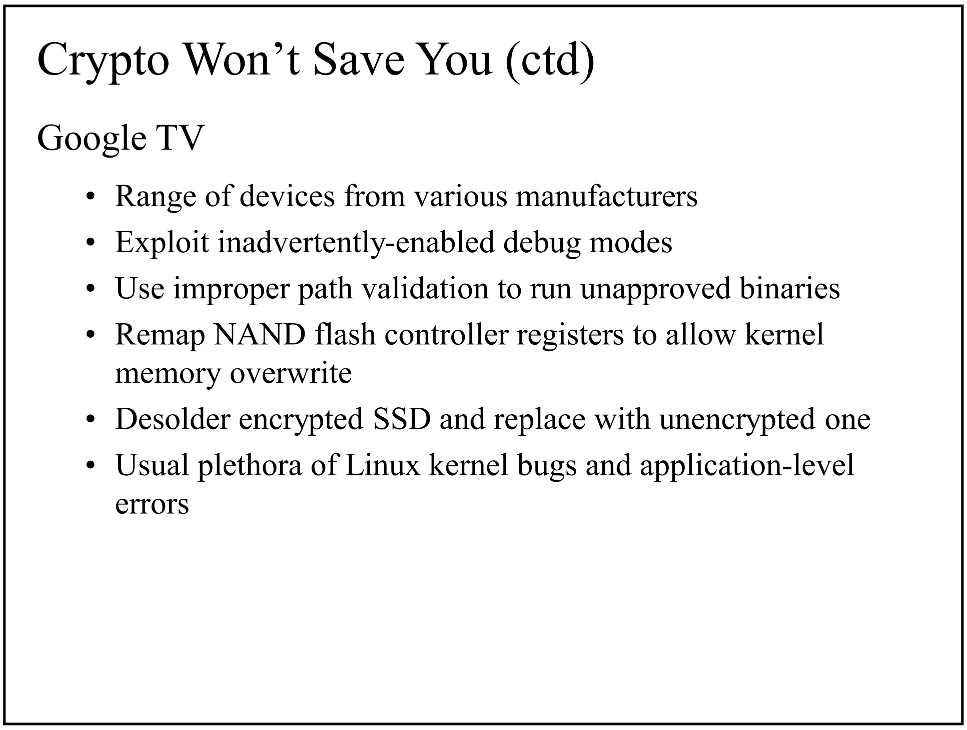
- Privacy-aware alternative to Facebook
- Replace the victim’s public key with your own one
- You can now MITM all of the victim’s messages

Google Chromecast

- Carefully verified signed image on loading
- Ignored the return value of the signature-checking function

Samsung Digital TV

- Recover CMAC key from firmware
- Can also load your own firmware via spoofed online auto-update



Crypto Won’t Save You (ctd)

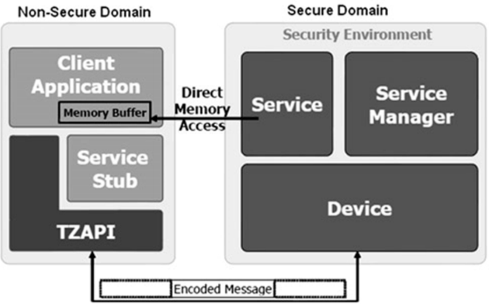
Google TV

- Range of devices from various manufacturers
- Exploit inadvertently-enabled debug modes
- Use improper path validation to run unapproved binaries
- Remap NAND flash controller registers to allow kernel memory overwrite
- Desolder encrypted SSD and replace with unencrypted one
- Usual plethora of Linux kernel bugs and application-level errors

Crypto Won't Save You (ctd)

Motorola cellphones

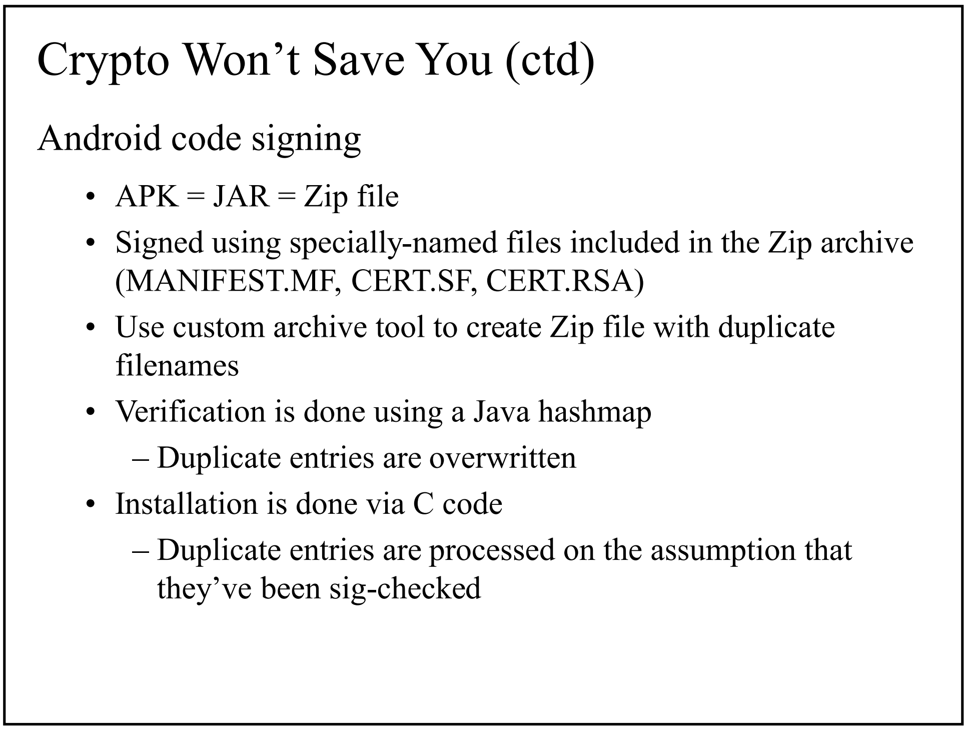
- Careful chaining of hashes, MACs (keyed hashes), and digital signatures
- Ignore the crypto and target the ARM TrustZone hardware-enforced security system
- "It's secure, because we say it is!"



Crypto Won't Save You (ctd)

Find an exploit in the trusted, secure kernel and attack the untrusted code from inside the trusted kernel

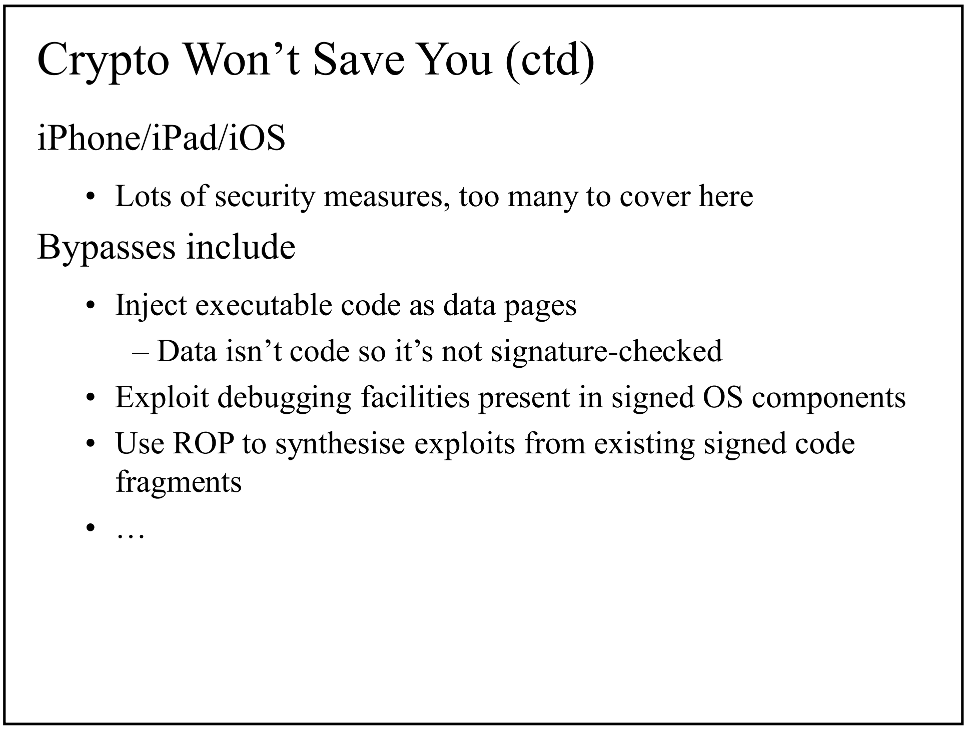
- The bootloader code was (apparently) quite good, it was the trusted security kernel that was insecure



Crypto Won’t Save You (ctd)

Android code signing

- APK = JAR = Zip file
- Signed using specially-named files included in the Zip archive (MANIFEST.MF, CERT.SF, CERT.RSA)
- Use custom archive tool to create Zip file with duplicate filenames
- Verification is done using a Java hashmap
  - Duplicate entries are overwritten
- Installation is done via C code
  - Duplicate entries are processed on the assumption that they’ve been sig-checked



Crypto Won’t Save You (ctd)

iPhone/iPad/iOS

- Lots of security measures, too many to cover here

Bypasses include

- Inject executable code as data pages
  - Data isn’t code so it’s not signature-checked
- Exploit debugging facilities present in signed OS components
- Use ROP to synthesise exploits from existing signed code fragments
- …

Crypto Won’t Save You (ctd)

Windows RT UEFI

- Exploit privilege escalation vulnerability in the RT kernel to bypass signing

Windows 8 UEFI

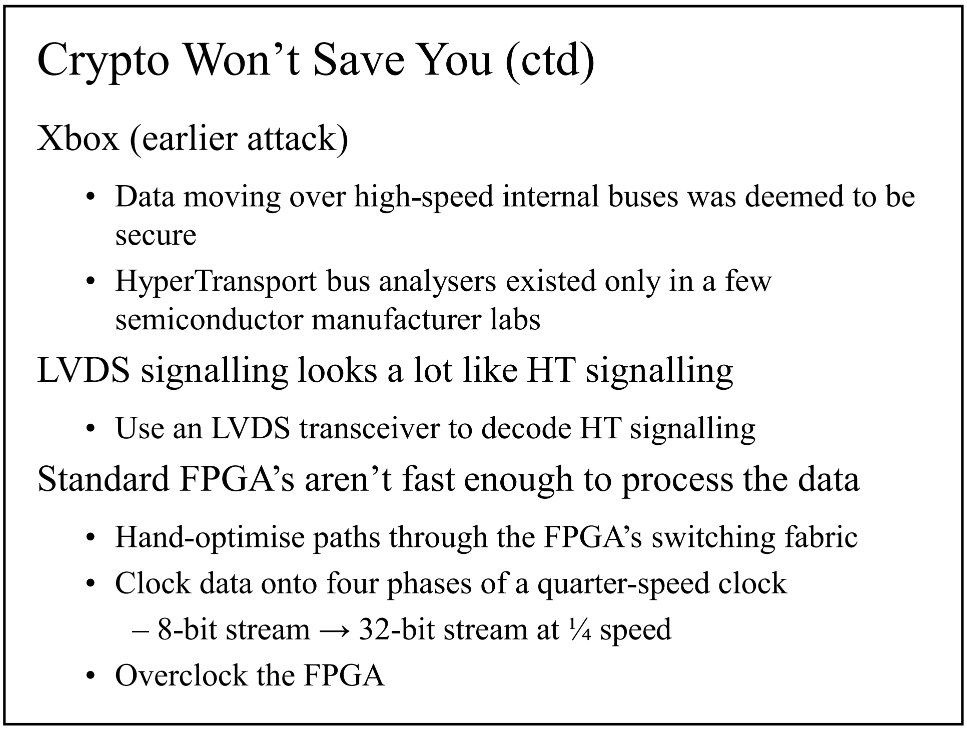
- Patch SPI flash memory holding UEFI firmware to skip the signature-check
- Clear flags in system NVRAM to disable signature checks

Crypto Won’t Save You (ctd)

CCC 2011 Badge

- Used Corrected Block TEA/XXTEA block cipher with 128-bit key
- Various exploits that all bypassed the need to deal with XXTEA
- Eventually, loaded custom code to extract the 128-bit key

It’s probably at least some sort of sign of the end times when your conference badge has a rootkit



Crypto Won’t Save You (ctd)

Xbox (earlier attack)

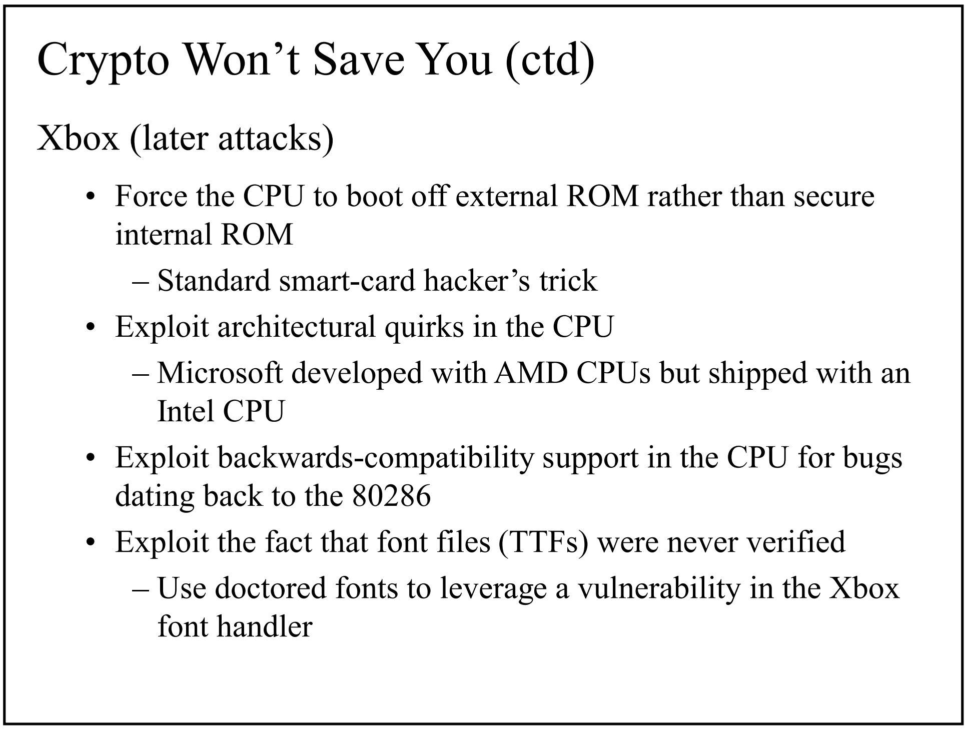
- Data moving over high-speed internal buses was deemed to be secure
- HyperTransport bus analysers existed only in a few semiconductor manufacturer labs

LVDS signalling looks a lot like HT signalling

- Use an LVDS transceiver to decode HT signalling

Standard FPGA’s aren’t fast enough to process the data

- Hand-optimise paths through the FPGA’s switching fabric
- Clock data onto four phases of a quarter-speed clock
  - 8-bit stream → 32-bit stream at ¼ speed
- Overclock the FPGA



Crypto Won’t Save You (ctd)

Xbox (later attacks)

- Force the CPU to boot off external ROM rather than secure internal ROM
  - Standard smart-card hacker’s trick
- Exploit architectural quirks in the CPU
  - Microsoft developed with AMD CPUs but shipped with an Intel CPU
- Exploit backwards-compatibility support in the CPU for bugs dating back to the 80286
- Exploit the fact that font files (TTFs) were never verified
  - Use doctored fonts to leverage a vulnerability in the Xbox font handler

Crypto Won’t Save You (ctd)

PS3

- Variant of the first Xbox attack
- Don’t try and pull data off the bus, just glitch it
- Processor now has an incorrect view of what’s stored in memory
  - Data in cache doesn’t match what’s actually in memory

Xbox 360

- Another glitch attack
- Ensure that a hash comparison always returns a hash-matched result

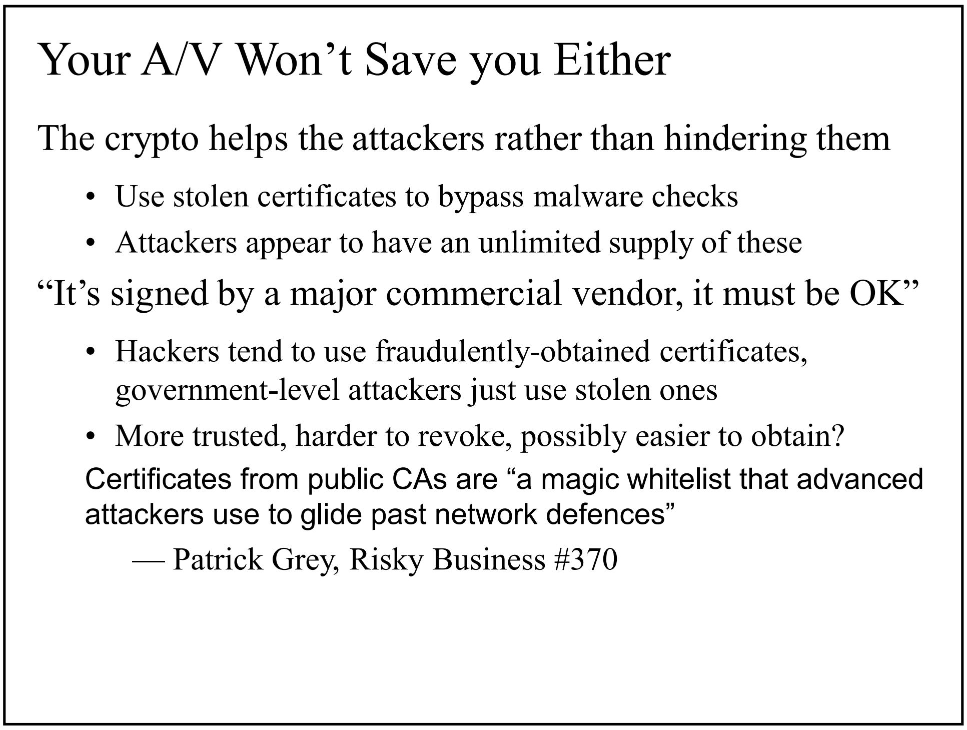
Crypto Won’t Save You (ctd)

Jailbreakers are rediscovering 15-20 year old smart card attacks

> I never met a smart-card I couldn’t glitch
> — European smart card hacker

Example: Clock glitches

- Send multiple clock pulses in the time interval when a single pulse should occur
- Fast-reacting parts of the CPU like the program counter respond
- Slower-reacting parts of the CPU like the ALU don’t have time
- Skip instructions, e.g. ones that perform access-control checks



Your A/V Won’t Save you Either

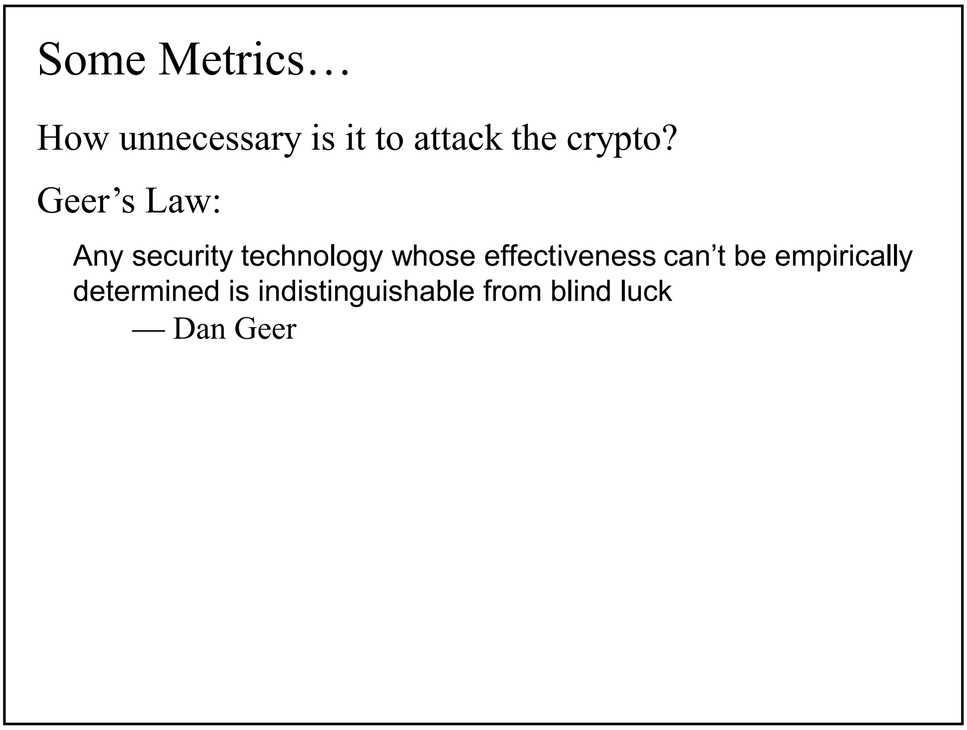
The crypto helps the attackers rather than hindering them

- Use stolen certificates to bypass malware checks
- Attackers appear to have an unlimited supply of these

“It’s signed by a major commercial vendor, it must be OK”

- Hackers tend to use fraudulently-obtained certificates, government-level attackers just use stolen ones
- More trusted, harder to revoke, possibly easier to obtain?

> Certificates from public CAs are “a magic whitelist that advanced attackers use to glide past network defences”
>
> — Patrick Grey, Risky Business #370



Some Metrics…

How unnecessary is it to attack the crypto?

Geer’s Law:

> Any security technology whose effectiveness can’t be empirically determined is indistinguishable from blind luck
>
> — Dan Geer

Some Metrics… (ctd)

Large-scale experiment carried out by a who's-who of companies

- Amazon
- Apple
- Dell
- eBay
- HP
- HSBC
- LinkedIn
- Paypal
- Twitter

Some Metrics… (ctd)

In late 2012, researchers noticed that these organisations, and many others, were using toy keys for DKIM signing

- 12,000 organisations
- 4,000 were using keys so weak that an individual attacker could have broken them

If this crypto was so weak, why didn't anyone attack it?

- It wasn't necessary

Some Metrics… (ctd)

There were so many other ways to render DKIM ineffective that no-one bothered attacking the crypto

- Anyone with a bit of technical knowledge could have broken the crypto
- No-one did because it was so easy to bypass that it wasn't worth attacking

"Crypto is bypassed, …"

Strong crypto will Save Us!

AES-256, because we want keys that go to 11

Original image, unencrypted

Strong crypto will Save Us! (ctd)

AES-256, because we want keys that go to 11

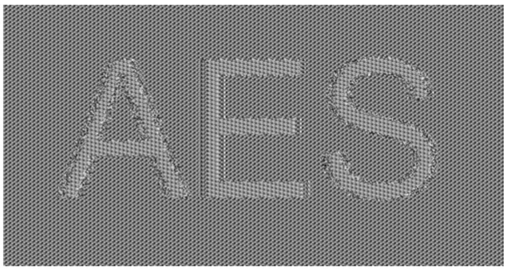


Image encrypted with AES-256, ECB mode

- This is the default if you call Java's `CipherUtilities.GetCipher("AES")`

HSMs will Save Us!

Hardware Security Module

- All crypto and keys are locked inside the HSM

Banks use these in large quantities for ATMs and PIN processing

HSMs will Save Us! (ctd)

HSM used for PIN processing

- Encrypt the customer’s primary account number (PAN) under the PIN derivation key (PDK) to get the PIN
- Result is a set of values in the range 0x0 – 0xF
- Use a decimalisation table to convert to PIN digits in 0…9 range

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Dec	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	6

- $\text{encrypt}_{\text{PDK}}$(PAN) = 2A3F…
- Decimalise 2A3F → 2036

HSMs will Save Us! (ctd)

Customer-defined PINs are handled by adding an offset to the PIN

- Not security-critical, since it’s useless without the PIN

PIN verification

- Take an encrypted PIN block from the ATM
- Feed it to the HSM in the bank alongside the decimalisation table
- HSM verifies the PIN and returns “failure” or “success”

All inside the HSM

- No keys or plaintext ever leaves the HSM

Secure, right?

HSMs will Save Us! (ctd)

Decimalisation tables are customer-defined

- Use a modified table to guess each PIN digit

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Dec	1	1	2	3	4	5	6	7	8	9	1	1	2	3	4	6

- Enter PIN block
- If the HSM still reports “success” then the PIN contains no zeroes

Repeat for all digits

- Now you know the digits in the PIN, but not their location

HSMs will Save Us! (ctd)

To find the digit locations, adjust the PIN offset

- Use offset to cancel out the decimalisation-table modification

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Dec	1	1	2	3	4	5	6	7	8	9	1	1	2	3	4	6

  – This table converts 0s to 1s in the PIN

- Taking PIN 2036 (from previous slides), offset 0000

Offset	HSM result	PIN
0001	failure	????
0010	failure	????
0100	success	?0??

HSMs will Save Us! (ctd)

Iterate for each digit in the PIN

- Recovers the PIN without knowing any encryption keys or having access to the HSM’s internals

For more on bypassing banking HSM and Chip and PIN security, see `http://www.cl.cam.ac.uk/research/security/-publications`

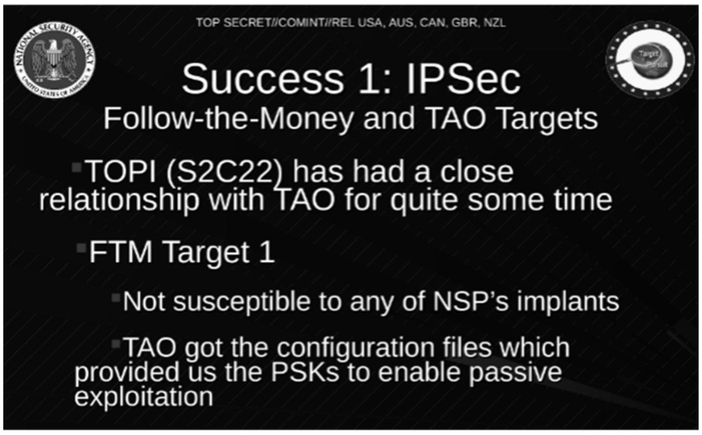
Crypto Summary

Number of attacks that broke the crypto: 0

Number of attacks that bypassed the crypto: All the rest

- No matter how strong the crypto was, or how large the keys were, the attackers walked around it

Crypto Summary (ctd)



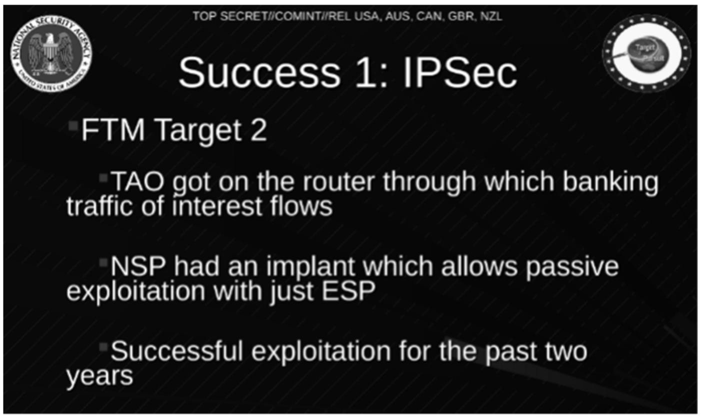
TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

Success 1: IPSec

Follow-the-Money and TAO Targets

- TOPI (S2C22) has had a close relationship with TAO for quite some time
  - FTM Target 1
    - Not susceptible to any of NSP's implants
    - TAO got the configuration files which provided us the PSKs to enable passive exploitation

Crypto Summary (ctd)

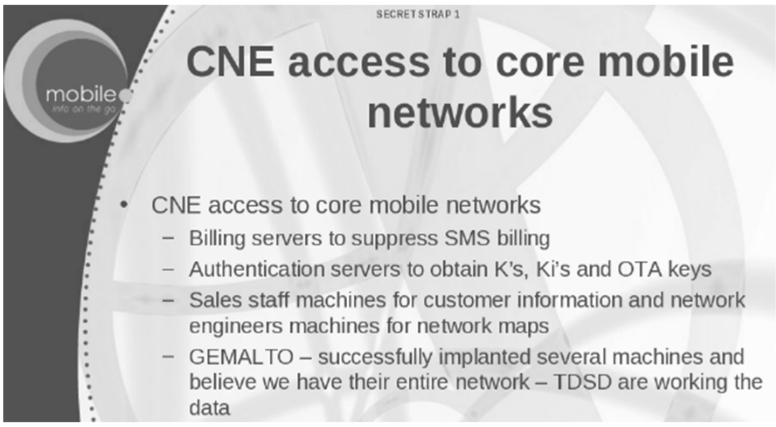


TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

Success 1: IPSec

- FTM Target 2
  - TAO got on the router through which banking traffic of interest flows
  - NSP had an implant which allows passive exploitation with just ESP
  - Successful exploitation for the past two years

Crypto Summary (ctd)



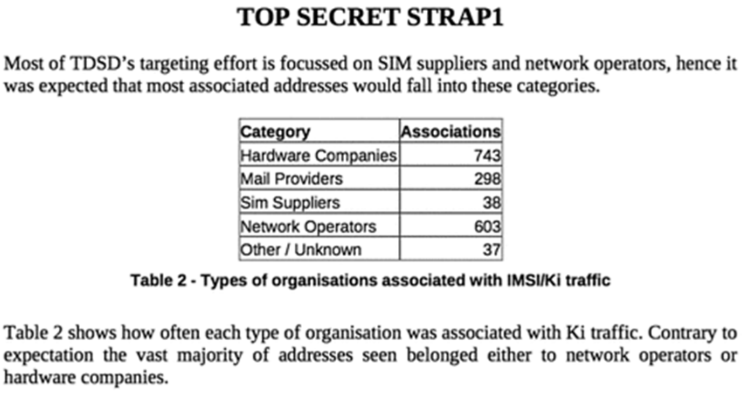
mobile
info on the go

SECRET STRAP 1

CNE access to core mobile networks

- CNE access to core mobile networks
  - Billing servers to suppress SMS billing
  - Authentication servers to obtain K's, Ki's and OTA keys
  - Sales staff machines for customer information and network engineers machines for network maps
  - GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data

Crypto Summary (ctd)



TOP SECRET STRAP1

Most of TDSD's targeting effort is focussed on SIM suppliers and network operators, hence it was expected that most associated addresses would fall into these categories.

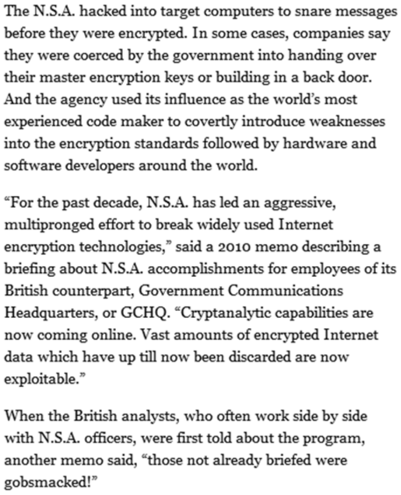
Category	Associations
Hardware Companies	743
Mail Providers	298
Sim Suppliers	38
Network Operators	603
Other / Unknown	37

Table 2 - Types of organisations associated with IMSI/Ki traffic

Table 2 shows how often each type of organisation was associated with Ki traffic. Contrary to expectation the vast majority of addresses seen belonged either to network operators or hardware companies.

Getting Back to BULLRUN…

New York Times:



The N.S.A. hacked into target computers to snare messages before they were encrypted. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.

"For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."

When the British analysts, who often work side by side with N.S.A. officers, were first told about the program, another memo said, "those not already briefed were gobsmacked!"

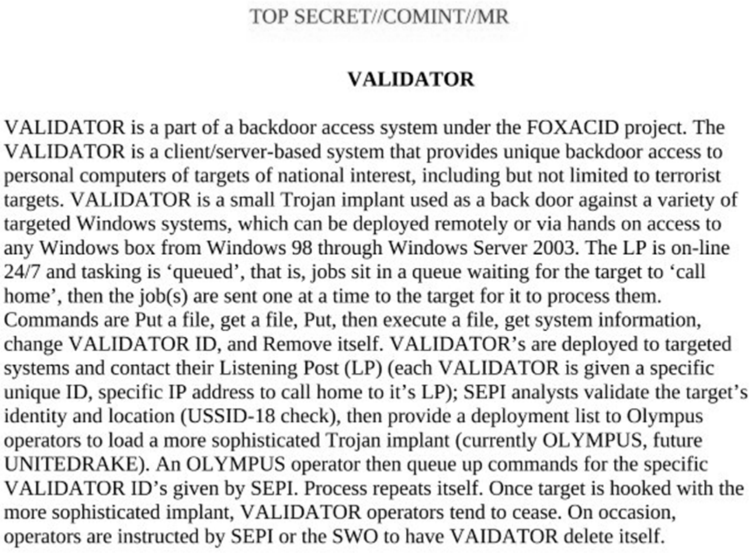
"the NSA hacked into target computers"

"companies were coerced by the government into handing over master encryption keys"

One-week CERT Summary (SB13-273)

"obtain administrative privileges by leveraging read access to the configuration file", "allows remote authenticated users to bypass an unspecified authentication step", "allows remote attackers to discover usernames and passwords via an HTTP request", "allows remote attackers to execute arbitrary commands", "allows remote attackers to read arbitrary files", "allows remote attackers to read arbitrary text files", "allows remote authenticated users to execute arbitrary code", "allows local users to gain privileges", "allows remote attackers to obtain sensitive information or modify data", "allows remote attackers to execute arbitrary SQL commands", "allows remote attackers to execute arbitrary SQL commands", "allows local users to gain privileges", "allows man-in-the-middle attackers to spoof SSL servers", "allows man-in-the-middle attackers to spoof servers", "allows man- in-the-middle attackers to obtain sensitive information or modify the data stream", "allows local users to gain privileges", "allows remote attackers to enumerate valid usernames", "allows remote attackers to execute arbitrary commands", "allows remote attackers to execute arbitrary commands", "allows local users to execute arbitrary Baseboard Management Controller (BMC) commands", "allows man-in-the-middle attackers to read or modify an inter-device data stream", "allows local users to gain privileges", "allow remote attackers to inject arbitrary web script or HTML", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to obtain sensitive query string or cookie information", "allows remote attackers to hijack the authentication of administrators", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to inject arbitrary web script or HTML", "allows local users to obtain sensitive information", "allows remote attackers to conduct cross-site request forgery (CSRF) attacks", "allows remote attackers to inject arbitrary web script or HTML via an HTML", "allows remote attackers to execute arbitrary code", "allows remote attackers to execute arbitrary code", "allow remote attackers to inject arbitrary web script or HTML", "allows local users to bypass intended access restrictions", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to obtain sensitive information", "allows remote attackers to obtain sensitive information", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to read session cookies", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to obtain privileged access", "allows local users to gain privileges", "allows remote attackers to execute arbitrary code", "allows remote attackers to inject arbitrary web script or HTML", "allows local users to gain privileges", "allows remote attackers to obtain sensitive information", "allows remote attackers to inject arbitrary web script or HTML", "allows local users to gain privileges", "allows local users to gain privileges", "allows remote attackers to obtain sensitive information", "allow remote attackers to bypass intended access restrictions", "allows remote authenticated users to bypass intended payment requirements", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to inject arbitrary web script or HTML", "allows remote attackers to bypass TLS verification", "allows remote attackers to inject arbitrary web script or HTML", "allows remote

BULLRUN in Practice

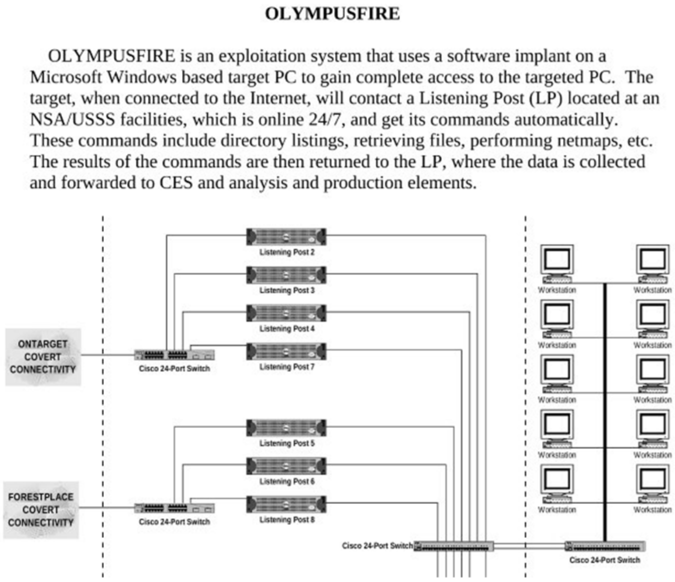


TOP SECRET//COMINT//MR

VALIDATOR

VALIDATOR is a part of a backdoor access system under the FOXACID project. The VALIDATOR is a client/server-based system that provides unique backdoor access to personal computers of targets of national interest, including but not limited to terrorist targets. VALIDATOR is a small Trojan implant used as a back door against a variety of targeted Windows systems, which can be deployed remotely or via hands on access to any Windows box from Windows 98 through Windows Server 2003. The LP is on-line 24/7 and tasking is 'queued', that is, jobs sit in a queue waiting for the target to 'call home', then the job(s) are sent one at a time to the target for it to process them. Commands are Put a file, get a file, Put, then execute a file, get system information, change VALIDATOR ID, and Remove itself. VALIDATOR's are deployed to targeted systems and contact their Listening Post (LP) (each VALIDATOR is given a specific unique ID, specific IP address to call home to it's LP); SEPI analysts validate the target's identity and location (USSID-18 check), then provide a deployment list to Olympus operators to load a more sophisticated Trojan implant (currently OLYMPUS, future UNITEDRAKE). An OLYMPUS operator then queue up commands for the specific VALIDATOR ID's given by SEPI. Process repeats itself. Once target is hooked with the more sophisticated implant, VALIDATOR operators tend to cease. On occasion, operators are instructed by SEPI or the SWO to have VAIDATOR delete itself.

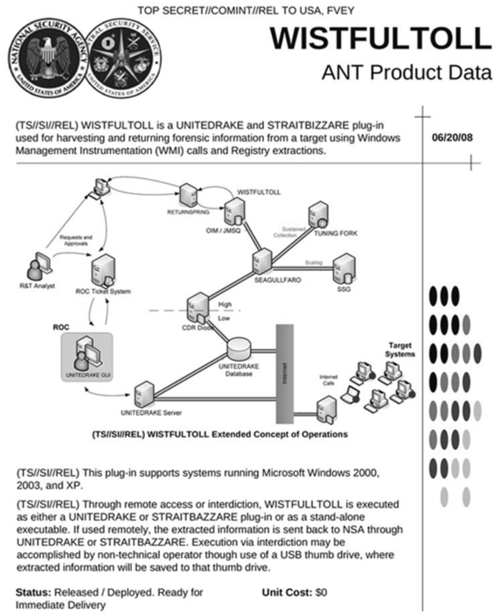
BULLRUN in Practice (ctd)



OLYMPUSFIRE

OLYMPUSFIRE is an exploitation system that uses a software implant on a Microsoft Windows based target PC to gain complete access to the targeted PC. The target, when connected to the Internet, will contact a Listening Post (LP) located at an NSA/USSS facilities, which is online 24/7, and get its commands automatically. These commands include directory listings, retrieving files, performing netmaps, etc. The results of the commands are then returned to the LP, where the data is collected and forwarded to CES and analysis and production elements.

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

WISTFULTOLL

ANT Product Data

06/20/08

(TS//SI//REL) WISTFULTOLL is a UNITEDRAKE and STRAITBIZZARE plug-in used for harvesting and returning forensic information from a target using Windows Management Instrumentation (WMI) calls and Registry extractions.

WISTFULTOLL
RETURNSPRING
OIM / JMSQ
Sustained Collection
TUNING FORK
Requests and Approvals
R&T Analyst
ROC Ticket System
SEAGULLFARO
Scaling
SSG
High
Low
CDR Diode
ROC
UNITEDRAKE GUI
UNITEDRAKE Database
Internet
Internet Cafe
Target Systems
UNITEDRAKE Server

(TS//SI//REL) WISTFULTOLL Extended Concept of Operations

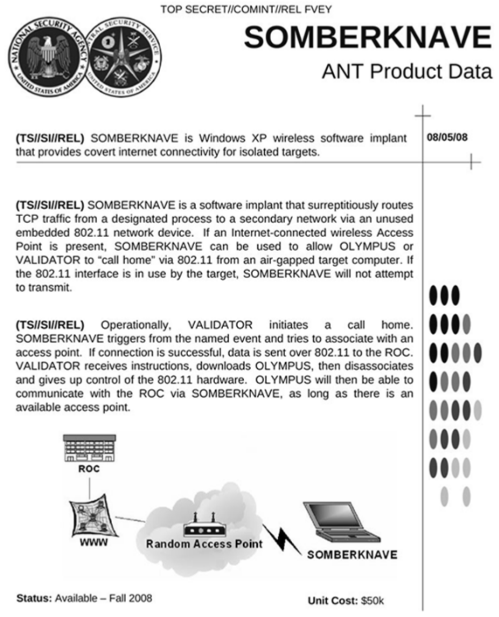
(TS//SI//REL) This plug-in supports systems running Microsoft Windows 2000, 2003, and XP.

(TS//SI//REL) Through remote access or interdiction, WISTFULLTOLL is executed as either a UNITEDRAKE or STRAITBAZZARE plug-in or as a stand-alone executable. If used remotely, the extracted information is sent back to NSA through UNITEDRAKE or STRAITBAZZARE. Execution via interdiction may be accomplished by non-technical operator though use of a USB thumb drive, where extracted information will be saved to that thumb drive.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL FVEY

SOMBERKNAVE

ANT Product Data

08/05/08

(TS//SI//REL) SOMBERKNAVE is Windows XP wireless software implant that provides covert internet connectivity for isolated targets.

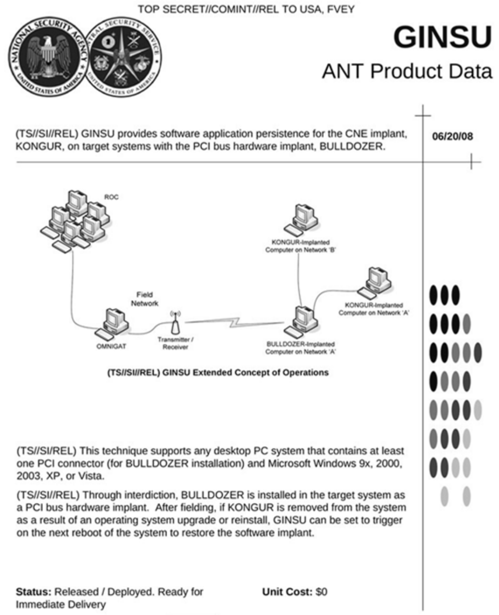
(TS//SI//REL) SOMBERKNAVE is a software implant that surreptitiously routes TCP traffic from a designated process to a secondary network via an unused embedded 802.11 network device. If an Internet-connected wireless Access Point is present, SOMBERKNAVE can be used to allow OLYMPUS or VALIDATOR to "call home" via 802.11 from an air-gapped target computer. If the 802.11 interface is in use by the target, SOMBERKNAVE will not attempt to transmit.

(TS//SI//REL) Operationally, VALIDATOR initiates a call home. SOMBERKNAVE triggers from the named event and tries to associate with an access point. If connection is successful, data is sent over 802.11 to the ROC. VALIDATOR receives instructions, downloads OLYMPUS, then disassociates and gives up control of the 802.11 hardware. OLYMPUS will then be able to communicate with the ROC via SOMBERKNAVE, as long as there is an available access point.

Status: Available – Fall 2008

Unit Cost: $50k

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

GINSU

ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

06/20/08

ROC
KONGUR-Implanted Computer on Network 'B'
Field Network
KONGUR-Implanted Computer on Network 'A'
OMNIGAT
Transmitter / Receiver
BULLDOZER-Implanted Computer on Network 'A'

(TS//SI//REL) GINSU Extended Concept of Operations

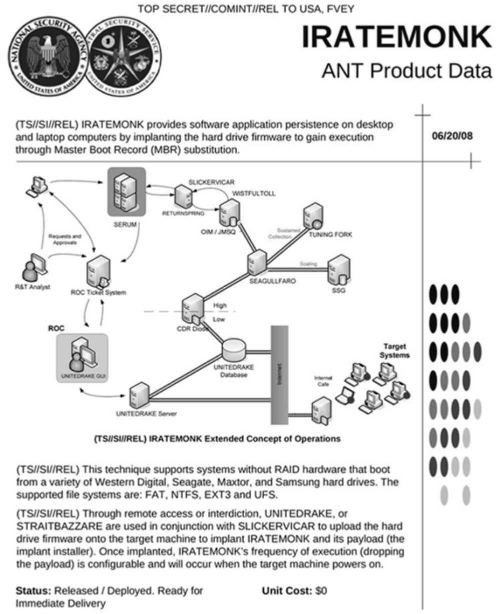
(TS//SI/REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08

SLICKERVICAR
WISTFULTOLL
RETURNSPRING
SERUM
OIM / JMSQ
Sustained Collection
TUNING FORK
Requests and Approvals
Scaling
R&T Analyst
ROC Ticket System
SEAGULLFARO
SSG
High
Low
ROC
CDR Diode
Target Systems
UNITEDRAKE Database
Internet
UNITEDRAKE GUI
Internet Cafe
UNITEDRAKE Server

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)

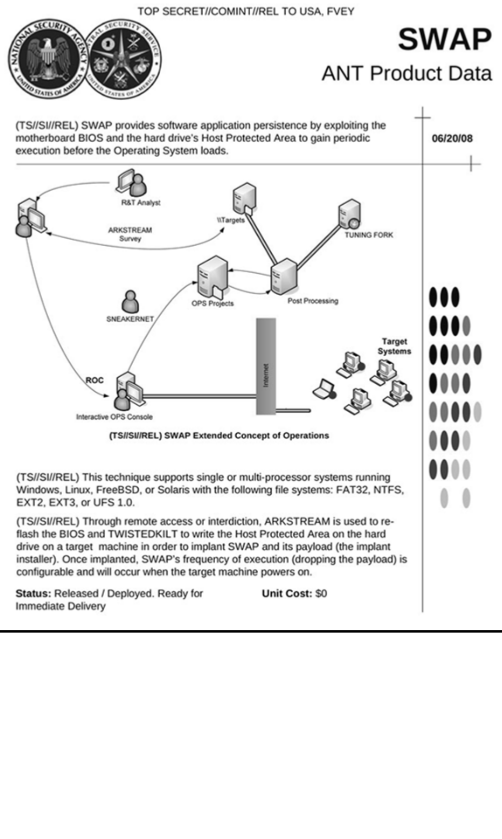
IRATEMONK was almost certainly used by a group that Kaspersky Labs dubbed Equation Group due to their use of strong cryptography

- Equation Group are tied to the Stuxnet and Flame developers

  > Equation Group are the ones with the coolest toys. Every now and then they share them with the Stuxnet group and the Flame group, but they are originally available only to the Equation Group people
  >
  > — Costin Raiu, Director of Kaspersky Lab's Global Research and Analysis Team

- More details in Ars Technica, "How 'omnipotent' hackers tied to NSA hid for 14 years — and were found at last"

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

SWAP

ANT Product Data

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.

06/20/08

R&T Analyst
\\Targets
ARKSTREAM Survey
TUNING FORK
OPS Projects
Post Processing
SNEAKERNET
Target Systems
ROC
Internet
Interactive OPS Console

(TS//SI//REL) SWAP Extended Concept of Operations

(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)

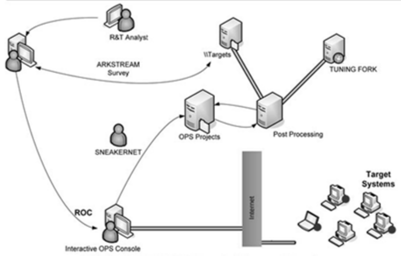
SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE

ANT Product Data

(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

06/20/08



(TS//SI//REL) DEITYBOUNCE Extended Concept of Operations

(TS//SI//REL) This technique supports multi-processor systems with RAID hardware and Microsoft Windows 2000, 2003, and XP. It currently targets Dell PowerEdge 1850/2850/1950/2950 RAID servers, using BIOS versions A02, A05, A06, 1.1.0, 1.2.0, or 1.3.7.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS on a target machine to implant DEITYBOUNCE and its payload (the implant installer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)

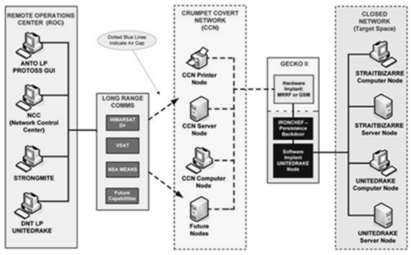
TOP SECRET//COMINT//REL TO USA, FVEY

IRONCHEF

ANT Product Data

(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

07/14/08


REMOTE OPERATIONS CENTER (ROC)
ANTO LP PROTOSS GUI
NCC (Network Control Center)
STRONGMITE
DNT LP UNITEDRAKE
Dotted Blue Lines Indicate Air Gap
LONG RANGE COMMS
INMARSAT D+
VSAT
NSA MEANS
Future Capabilities
CRUMPET COVERT NETWORK (CCN)
CCN Printer Node
CCN Server Node
CCN Computer Node
Future Nodes
GECKO II
Hardware Implant: MRRF or GSM
IRONCHEF – Persistence Backdoor
Software Implant UNITEDRAKE Node
CLOSED NETWORK (Target Space)
STRAITBIZARRE Computer Node
STRAITBIZARRE Server Node
UNITEDRAKE Computer Node
UNITEDRAKE Server Node

(TS//SI//REL) IRONCHEF Extended Concept of Operations

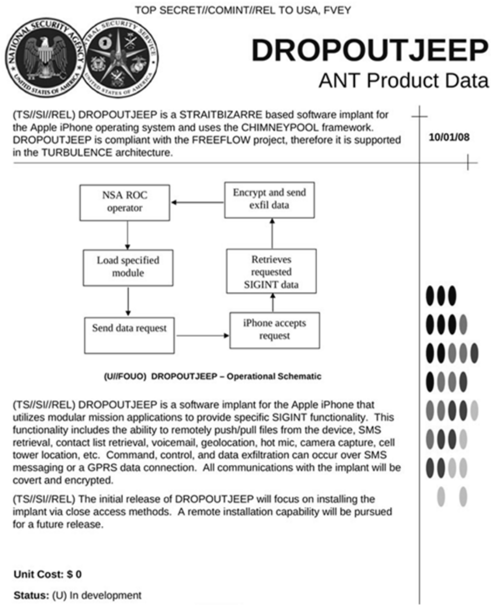
(TS//SI/REL) This technique supports the HP Proliant 380DL G5 server, onto which a hardware implant has been installed that communicates over the I^2C Interface (WAGONBED).

(TS//SI//REL) Through interdiction, IRONCHEF, a software CNE implant and the hardware implant are installed onto the system. If the software CNE implant is removed from the target machine, IRONCHEF is used to access the machine, determine the reason for removal of the software, and then reinstall the software from a listening post to the target system.

Status: Ready for Immediate Delivery

Unit Cost: $0

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

DROPOUTJEEP

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08

NSA ROC operator

Load specified module

Send data request

iPhone accepts request

Retrieves requested SIGINT data

Encrypt and send exfil data

(U//FOUO) DROPOUTJEEP – Operational Schematic

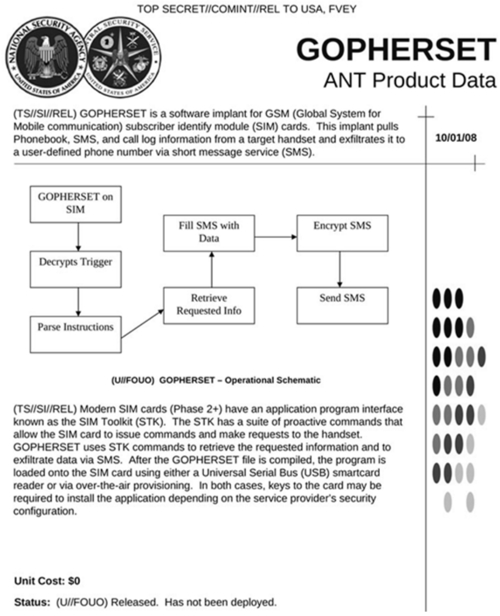
(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: $ 0

Status: (U) In development

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

GOPHERSET on SIM

Decrypts Trigger

Parse Instructions

Retrieve Requested Info

Fill SMS with Data

Encrypt SMS

Send SMS

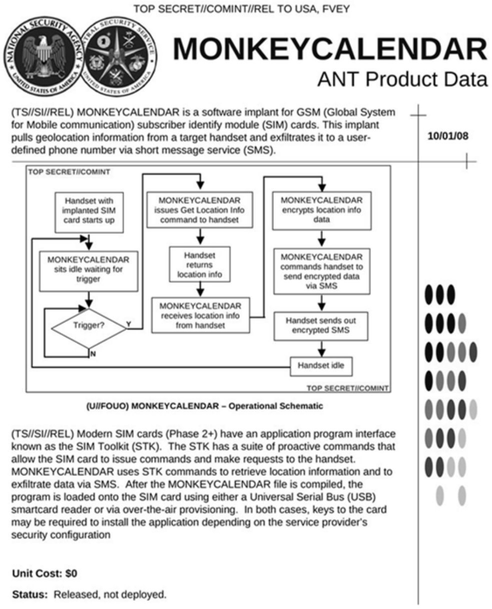
(U//FOUO) GOPHERSET – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. GOPHERSET uses STK commands to retrieve the requested information and to exfiltrate data via SMS. After the GOPHERSET file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration.

Unit Cost: $0

Status: (U//FOUO) Released. Has not been deployed.

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

MONKEYCALENDAR

ANT Product Data

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

TOP SECRET//COMINT
Handset with implanted SIM card starts up
MONKEYCALENDAR sits idle waiting for trigger
Trigger?
Y
N
MONKEYCALENDAR issues Get Location Info command to handset
Handset returns location info
MONKEYCALENDAR receives location info from handset
MONKEYCALENDAR encrypts location info data
MONKEYCALENDAR commands handset to send encrypted data via SMS
Handset sends out encrypted SMS
Handset idle
TOP SECRET//COMINT

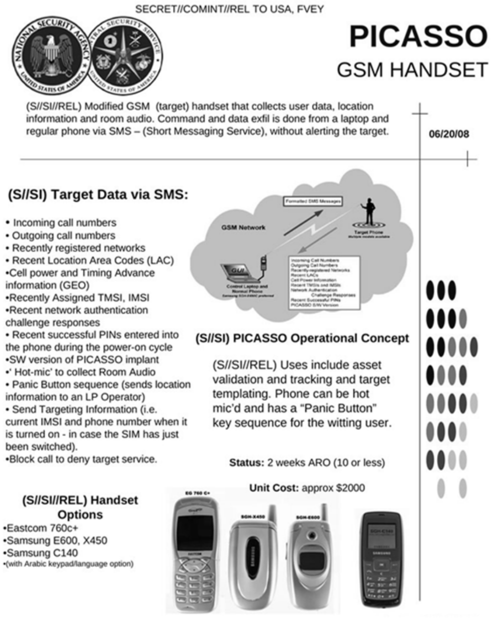
(U//FOUO) MONKEYCALENDAR – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. MONKEYCALENDAR uses STK commands to retrieve location information and to exfiltrate data via SMS. After the MONKEYCALENDAR file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration

Unit Cost: $0

Status: Released, not deployed.

BULLRUN in Practice (ctd)



SECRET//COMINT//REL TO USA, FVEY

PICASSO

GSM HANDSET

(S//SI//REL) Modified GSM (target) handset that collects user data, location information and room audio. Command and data exfil is done from a laptop and regular phone via SMS – (Short Messaging Service), without alerting the target.

06/20/08

(S//SI) Target Data via SMS:

- Incoming call numbers
- Outgoing call numbers
- Recently registered networks
- Recent Location Area Codes (LAC)
- Cell power and Timing Advance information (GEO)
- Recently Assigned TMSI, IMSI
- Recent network authentication challenge responses
- Recent successful PINs entered into the phone during the power-on cycle
- SW version of PICASSO implant
- ' Hot-mic' to collect Room Audio
- Panic Button sequence (sends location information to an LP Operator)
- Send Targeting Information (i.e. current IMSI and phone number when it is turned on - in case the SIM has just been switched).
- Block call to deny target service.

(S//SI) PICASSO Operational Concept

(S//SI//REL) Uses include asset validation and tracking and target templating. Phone can be hot mic'd and has a "Panic Button" key sequence for the witting user.

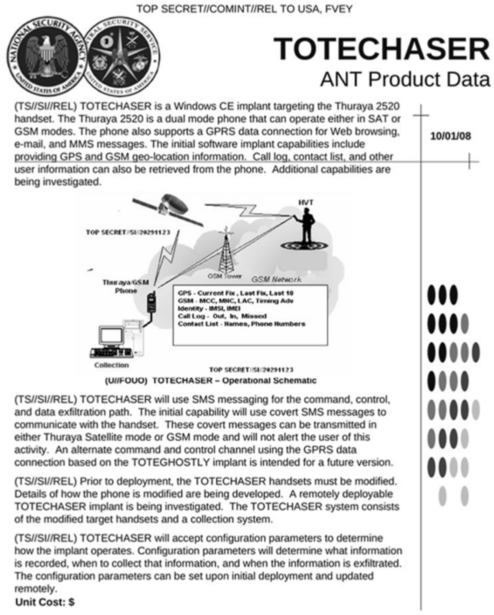
Status: 2 weeks ARO (10 or less)

Unit Cost: approx $2000

(S//SI//REL) Handset Options

- Eastcom 760c+
- Samsung E600, X450
- Samsung C140
- (with Arabic keypad/language option)

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

TOTECHASER

ANT Product Data

(TS//SI//REL) TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. The Thuraya 2520 is a dual mode phone that can operate either in SAT or GSM modes. The phone also supports a GPRS data connection for Web browsing, e-mail, and MMS messages. The initial software implant capabilities include providing GPS and GSM geo-location information. Call log, contact list, and other user information can also be retrieved from the phone. Additional capabilities are being investigated.

10/01/08

TOP SECRET//SI//20291123
HVT
GSM Tower
GSM Network
Thuraya/GSM Phone
GPS - Current Fix , Last Fix, Last 10
GSM - MCC, MNC, LAC, Timing Adv
Identity - IMSI, IMEI
Call Log - Out, In, Missed
Contact List - Names, Phone Numbers
Collection
TOP SECRET//SI//20291123

(U//FOUO) TOTECHASER – Operational Schematic

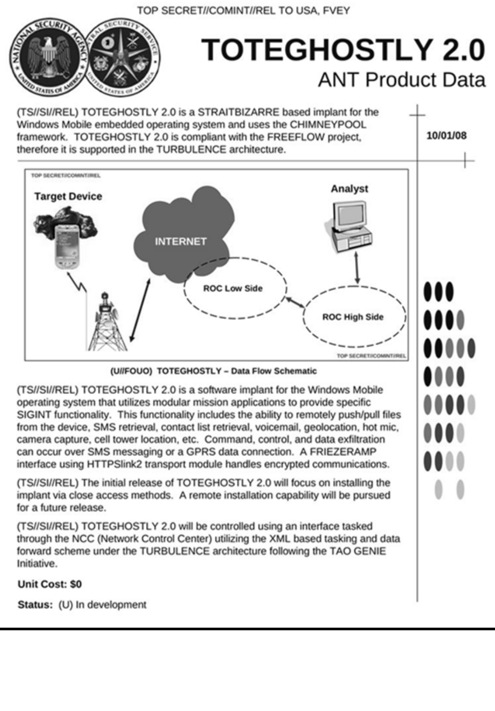
(TS//SI//REL) TOTECHASER will use SMS messaging for the command, control, and data exfiltration path. The initial capability will use covert SMS messages to communicate with the handset. These covert messages can be transmitted in either Thuraya Satellite mode or GSM mode and will not alert the user of this activity. An alternate command and control channel using the GPRS data connection based on the TOTEGHOSTLY implant is intended for a future version.

(TS//SI//REL) Prior to deployment, the TOTECHASER handsets must be modified. Details of how the phone is modified are being developed. A remotely deployable TOTECHASER implant is being investigated. The TOTECHASER system consists of the modified target handsets and a collection system.

(TS//SI//REL) TOTECHASER will accept configuration parameters to determine how the implant operates. Configuration parameters will determine what information is recorded, when to collect that information, and when the information is exfiltrated. The configuration parameters can be set upon initial deployment and updated remotely.

Unit Cost: $

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

TOTEGHOSTLY 2.0

ANT Product Data

(TS//SI//REL) TOTEGHOSTLY 2.0 is a STRAITBIZARRE based implant for the Windows Mobile embedded operating system and uses the CHIMNEYPOOL framework. TOTEGHOSTLY 2.0 is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08

TOP SECRET//COMINT//REL
Target Device
INTERNET
Analyst
ROC Low Side
ROC High Side
TOP SECRET//COMINT//REL

(U//FOUO) TOTEGHOSTLY – Data Flow Schematic

(TS//SI//REL) TOTEGHOSTLY 2.0 is a software implant for the Windows Mobile operating system that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. A FRIEZERAMP interface using HTTPSlink2 transport module handles encrypted communications.

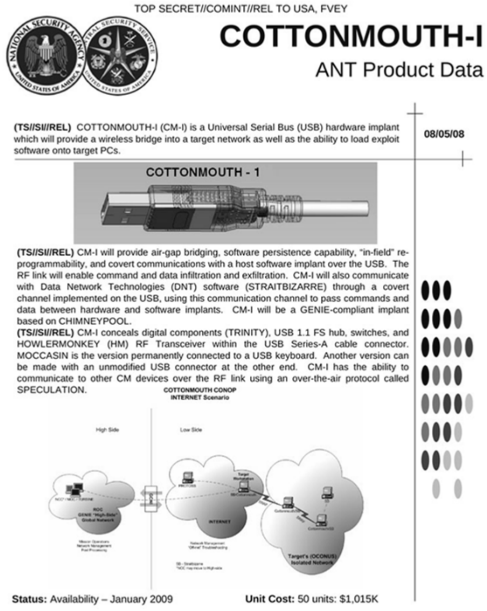
(TS//SI//REL) The initial release of TOTEGHOSTLY 2.0 will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

(TS//SI//REL) TOTEGHOSTLY 2.0 will be controlled using an interface tasked through the NCC (Network Control Center) utilizing the XML based tasking and data forward scheme under the TURBULENCE architecture following the TAO GENIE Initiative.

Unit Cost: $0

Status: (U) In development

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

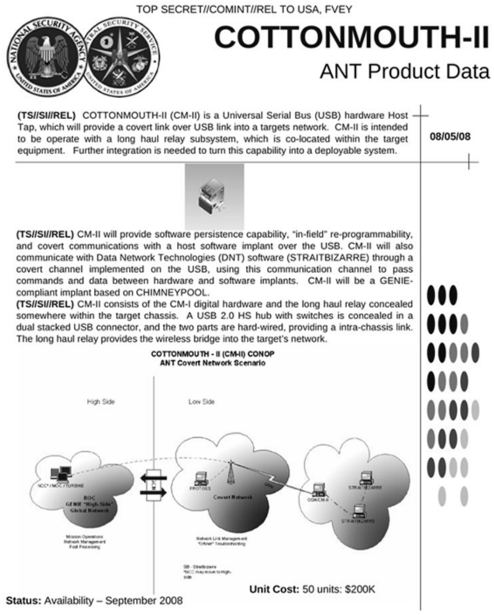
COTTONMOUTH CONOP
INTERNET Scenario

High Side
Low Side
ROC
GENIE "High-Side" Global Network
INTERNET
Target Workstation
Target's (OCONUS) Isolated Network

Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-II

ANT Product Data

(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

08/05/08

(TS//SI//REL) CM-II will provide software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. CM-II will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-II will be a GENIE-compliant implant based on CHIMNEYPOOL.

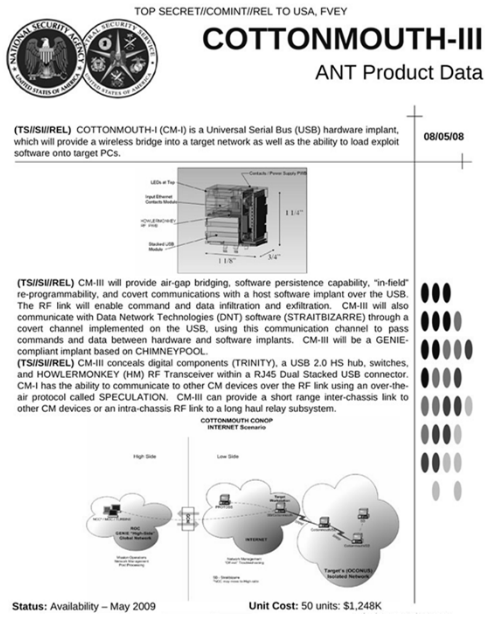
(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay concealed somewhere within the target chassis. A USB 2.0 HS hub with switches is concealed in a dual stacked USB connector, and the two parts are hard-wired, providing a intra-chassis link. The long haul relay provides the wireless bridge into the target's network.

COTTONMOUTH - II (CM-II) CONOP
ANT Covert Network Scenario

Unit Cost: 50 units: $200K

Status: Availability – September 2008

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-III

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant, which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

Contacts / Power Supply PWB
LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
1 1/4"
1 1/8"
3/4"

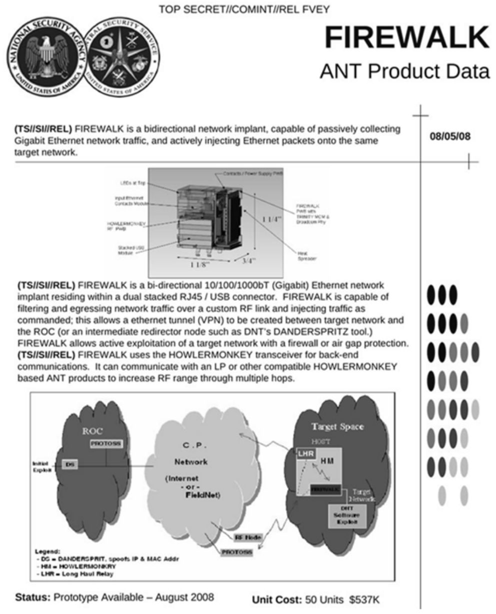
(TS//SI//REL) CM-III will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-III will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-III will be a GENIE-compliant implant based on CHIMNEYPOOL.
(TS//SI//REL) CM-III conceals digital components (TRINITY), a USB 2.0 HS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within a RJ45 Dual Stacked USB connector. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION. CM-III can provide a short range inter-chassis link to other CM devices or an intra-chassis RF link to a long haul relay subsystem.

COTTONMOUTH CONOP
INTERNET Scenario

High Side
Low Side
ROC
GENIE "High-Side" Global Network
INTERNET
Target Workstation
Target's (OCONUS) Isolated Network

Status: Availability – May 2009 **Unit Cost:** 50 units: $1,248K

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL FVEY

FIREWALK

ANT Product Data

(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.

08/05/08

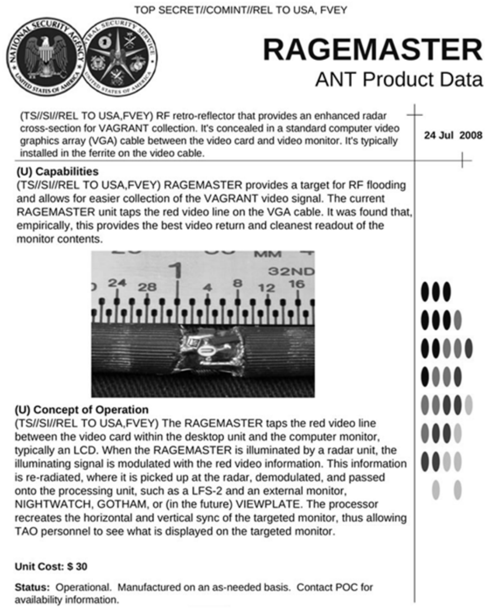
Contacts / Power Supply PWB
LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
FIREWALK PWB with TRINITY MCM & Broadcom Phy
Heat Spreader
1 1/4"
1 1/8"
3/4"

(TS//SI//REL) FIREWALK is a bi-directional 10/100/1000bT (Gigabit) Ethernet network implant residing within a dual stacked RJ45 / USB connector. FIREWALK is capable of filtering and egressing network traffic over a custom RF link and injecting traffic as commanded; this allows a ethernet tunnel (VPN) to be created between target network and the ROC (or an intermediate redirector node such as DNT's DANDERSPRITZ tool.) FIREWALK allows active exploitation of a target network with a firewall or air gap protection.
(TS//SI//REL) FIREWALK uses the HOWLERMONKEY transceiver for back-end communications. It can communicate with an LP or other compatible HOWLERMONKEY based ANT products to increase RF range through multiple hops.

Legend:
- DS = DANDERSPRIT, spoofs IP & MAC Addr
- HM = HOWLERMONKRY
- LHR = Long Haul Relay

Status: Prototype Available – August 2008 **Unit Cost:** 50 Units $537K

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

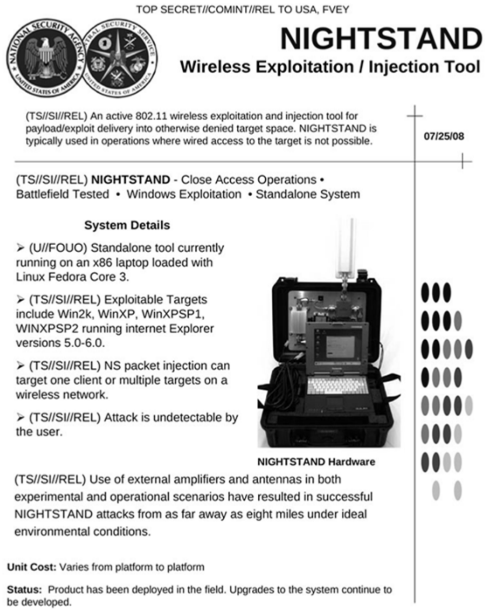
(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

BULLRUN in Practice (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

BULLRUN in Practice (ctd)

It’s not just the NSA that does this

> The British Government has admitted its intelligence services have the broad power to hack into personal phones, computers, and communications networks, and claims they are legally justified to hack anyone, anywhere in the world, even if the target is not a threat to national security nor suspected of any crime
>
> — Privacy International summary of ~130 pages of UK government court documents

National Security Letters

The legalised form of rubber-hose cryptanalysis

- Requirement to hand over data, or else
- Built-in gag order to prevent you talking about it
  - Details of both vary depending on court challenges to their constitutionality

National Security Letters (ctd)

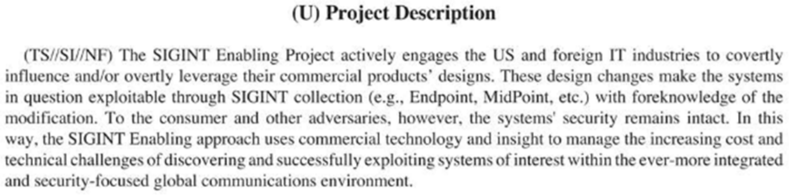
Bypass any crypto at the service provider by requiring them to hand over plaintext

- FBI over-used them while under-reporting their use to Congress
- In 2013, issued over 19,000 NSLs with nearly 39,000 requests for information (Statistical Transparency Report Regarding Use of National Security Authorities, June 2014)

Several providers (LavaBit, Silent Mail, CryptoSeal, CertiVox) have shut down in the face of NSLs

- Larger, more commercially-oriented providers complied with them

BULLRUN Again…



(U) Project Description

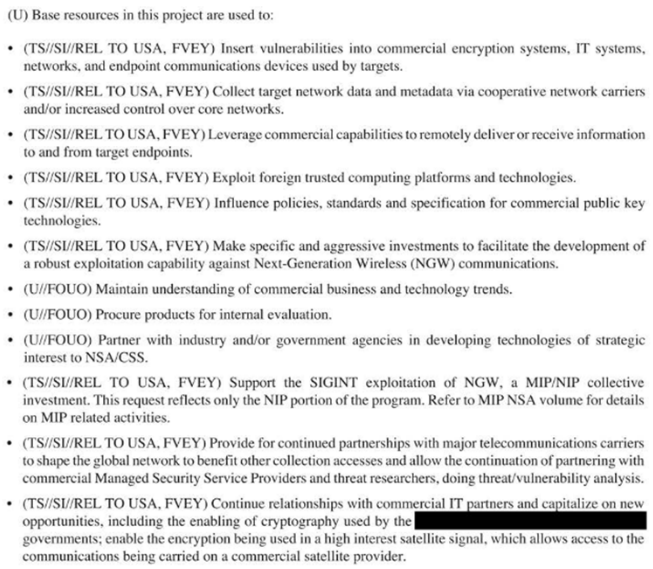
(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

"covertly influence and/or overtly leverage commercial products' designs"

"design changes make the systems in question exploitable"

"to the consumer, however, the systems' security remains intact"

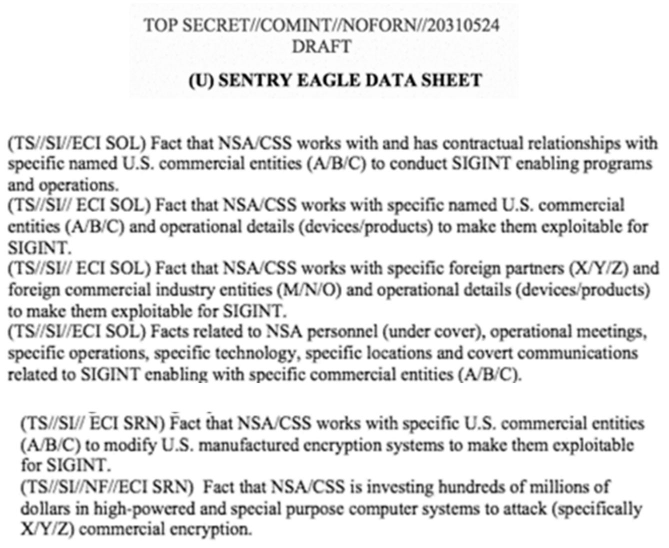
BULLRUN Again… (ctd)



(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.
- (U//FOUO) Maintain understanding of commercial business and technology trends.
- (U//FOUO) Procure products for internal evaluation.
- (U//FOUO) Partner with industry and/or government agencies in developing technologies of strategic interest to NSA/CSS.
- (TS//SI//REL TO USA, FVEY) Support the SIGINT exploitation of NGW, a MIP/NIP collective investment. This request reflects only the NIP portion of the program. Refer to MIP NSA volume for details on MIP related activities.
- (TS//SI//REL TO USA, FVEY) Provide for continued partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses and allow the continuation of partnering with commercial Managed Security Service Providers and threat researchers, doing threat/vulnerability analysis.
- (TS//SI//REL TO USA, FVEY) Continue relationships with commercial IT partners and capitalize on new opportunities, including the enabling of cryptography used by the [redacted] governments; enable the encryption being used in a high interest satellite signal, which allows access to the communications being carried on a commercial satellite provider.

BULLRUN Again… (ctd)



TOP SECRET//COMINT//NOFORN//20310524
DRAFT

(U) SENTRY EAGLE DATA SHEET

(TS//SI//ECI SOL) Fact that NSA/CSS works with and has contractual relationships with specific named U.S. commercial entities (A/B/C) to conduct SIGINT enabling programs and operations.
(TS//SI// ECI SOL) Fact that NSA/CSS works with specific named U.S. commercial entities (A/B/C) and operational details (devices/products) to make them exploitable for SIGINT.
(TS//SI// ECI SOL) Fact that NSA/CSS works with specific foreign partners (X/Y/Z) and foreign commercial industry entities (M/N/O) and operational details (devices/products) to make them exploitable for SIGINT.
(TS//SI//ECI SOL) Facts related to NSA personnel (under cover), operational meetings, specific operations, specific technology, specific locations and covert communications related to SIGINT enabling with specific commercial entities (A/B/C).

(TS//SI// ECI SRN) Fact that NSA/CSS works with specific U.S. commercial entities (A/B/C) to modify U.S. manufactured encryption systems to make them exploitable for SIGINT.
(TS//SI//NF//ECI SRN) Fact that NSA/CSS is investing hundreds of millions of dollars in high-powered and special purpose computer systems to attack (specifically X/Y/Z) commercial encryption.

Dual_EC_DRBG

In 1985, ANSI X9.17 specified a pseudorandom number generator (PRNG) for banking use

```
temp = encrypt( seed );
out = encrypt( temp ^ $V_n$ );
$V_{n+1}$ = encrypt( out ^ temp );
```

Based on triple DES, the state of the art at the time

- Security relies on the strength of 3DES secret keys

Dual_EC_DRBG (ctd)

In 1998, NIST adopted it verbatim in X9.31, adding the option to use AES

Subsequently, over a period of several years many people at NIST hacked around on a bunch of PRNGs

- Design-by-committee, but in series rather than parallel

Finally published in 2012 as NIST SP 800-90A

Dual_EC_DRBG (ctd)

Some SP 800-90 generators are straightforward and sensible

- X9.17/X9.31 updated to use HMAC
- Half a page in X9.17

Some are not

- Hash_DRBG
- Five pages in SP 800-90

Dual_EC_DRBG (ctd)

Others are just stupid

- Dual_EC_DRBG
- Sixteen pages in SP 800-90
  - Pages and pages of maths
  - Where’s the RNG?
- Complex, awkward, incredibly slow, …

Dual_EC_DRBG (ctd)

NSA also pushed hard to get this particular PRNG into other standards

- ANSI X9.82
- ISO 18031

ANSI is a US national standards body, but ISO is an international body

- Something similar happened in the 1990s when they were “persuaded” not to standardise encryption algorithms

Dual_EC_DRBG (ctd)

ISO had spent years developing their RNG standard

- 19 of 24 countries involved had already approved the draft standard…
- … but not the US

> We do feel that ANSI X9.82 Random Bit Generation standardization work is much further developed and should be used as the basis for this ISO standard
>
> — US national body comments on ISO/IEC 2nd Committee Draft for 18031

Two years later, ISO 18031:2005 was released in the form the NSA wanted

Dual_EC_DRBG (ctd)

ANSI/ISO standards are even worse than SP 800-90

- No way to generate your own parameters

In any case the NSA had a solution for SP 800-90

> The Dual_EC_DRBG requires the specifications of an elliptic curve and two points on the elliptic curve […] CAVS Dual_EC_DRBG tests use only the NIST Approved curves and associated points
>
> — "The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS)"

- (This is standard NIST wording, meaning if you find a flaw, you can't fix it without voiding your certification, a long-standing problem with FIPS 140)

Dual_EC_DRBG (ctd)

It's OK, no-one in their right mind would implement this

> I've never met anyone who would actually use Dual-EC-DRBG. (Blum-Blum-Shub-fanatics show up all the time, but they are all nutcases)
>
> — Kristian Gjøsteen, Norwegian University of Science and Technology

- (Kristian submitted a comment paper to NIST as far back as 2006 pointing out that the EC DRBG was cryptographically unsound and shouldn't be used)

Dual_EC_DRBG (ctd)

So we've established that no-one would ever take this thing seriously

You were serious about dat?
— "My Cousin Vinnie", 1992

Dual_EC_DRBG (ctd)

Well, except for a pile of US companies, including

- Blackberry
- Certicom (holders of ECC patents)
- Cisco
- GE Healthcare
- Juniper (see later slides)
- Lancope (who *only* provide EC_DRBG)
- McAfee
- Microsoft
- Mocana
- Openpeak

continues

Dual_EC_DRBG (ctd)

continued

- OpenSSL (umbrella use by numerous organisations)
- RSA
- Safenet
- SafeLogic
- Samsung (must have had USG customers)
- Symantec
- Thales (see Samsung entry)

RSA made it the default in their crypto library

Dual_EC_DRBG (ctd)

OpenSSL didn't actually use it, though

- Implementation contained "a fatal bug in the Dual EC DRBG implementation"

> This bug is fatal in the sense that it prevents all use of the Dual EC DRBG algorithm […] we do not plan to correct the bug. A FIPS 140-2 validated module cannot be changed without considerable expense and effort
>
> — "Flaw in Dual EC DRBG (no, not that one)",
> Steve Marquess

Presumably no-one had ever used this generator in OpenSSL, since no-one complained that it didn't work

- *Presumably...*

Dual_EC_DRBG (ctd)

FIPS 140 doesn't allow you to fix things

> We did specifically ask if we had any discretion at all in the choice of points and were told that we were required to use the compromised points […] if you want to be FIPS 140-2 compliant you MUST use the compromised points
>
> — "Flaw in Dual EC DRBG (no, not that one)",
> Steve Marquess

But wouldn't the FIPS validation have caught the fact that the OpenSSL implementation didn't work?

> Not only the original validation but many subsequent validations have successfully passed the algorithm tests… several hundred times now. That's a lot of fail […] the FIPS 140-2 validation testing isn't very useful for catching real-world problems
>
> — "Flaw in Dual EC DRBG (no, not that one)",
> Steve Marquess

Dual_EC_DRBG (ctd)

So what's the problem (apart from it being a stupid design)?

- How long do you have?
- Read "The Many Flaws of Dual_EC_DRBG", `http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html`
- (You are not expected to understand this)

> Dual EC DRBG should not have been included in X9.82 or SP 800-90 in current form
>
> — "Dual EC DRBG and NIST Crypto Process Review",
> John Kelsey, NIST

Dual_EC_DRBG (ctd)

Short summary of just one issue

- Public value sent at start of SSL/TLS handshake, Client Random, is 32 bytes (256 bits)
  - Used to randomise each new exchange
- If generated with Dual_EC_DRBG you can predict the SSL/TLS premaster secret
- All crypto keys in SSL/TLS are derived from this value

Dual_EC_DRBG (ctd)

NSA attempted to make this attack even easier

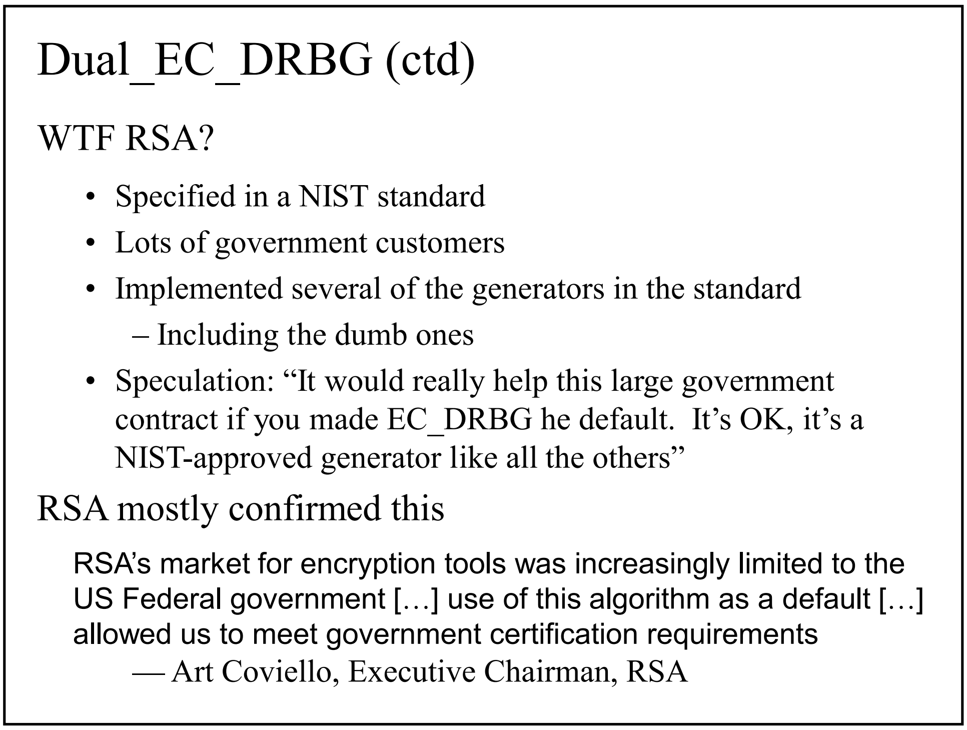
> The United States DoD has requested a TLS mode which allows the use of longer public randomness values
>
> — `draft-rescorla-tls-extended-random-00`

- (Eric Rescorla is co-chair of the TLS working group, draft co-authored by Margaret Salter of the NSA)

- NSA then authored, co-authored, or sponsored three more standards drafts that had the same effect

> Each of these extensions has the side effect of removing the most obvious difficulty in exploiting [the Dual EC DRBG]
>
> — "On the Practical Exploitability of Dual EC in TLS Implementations"

Failsafe, multiple-redundant compromise



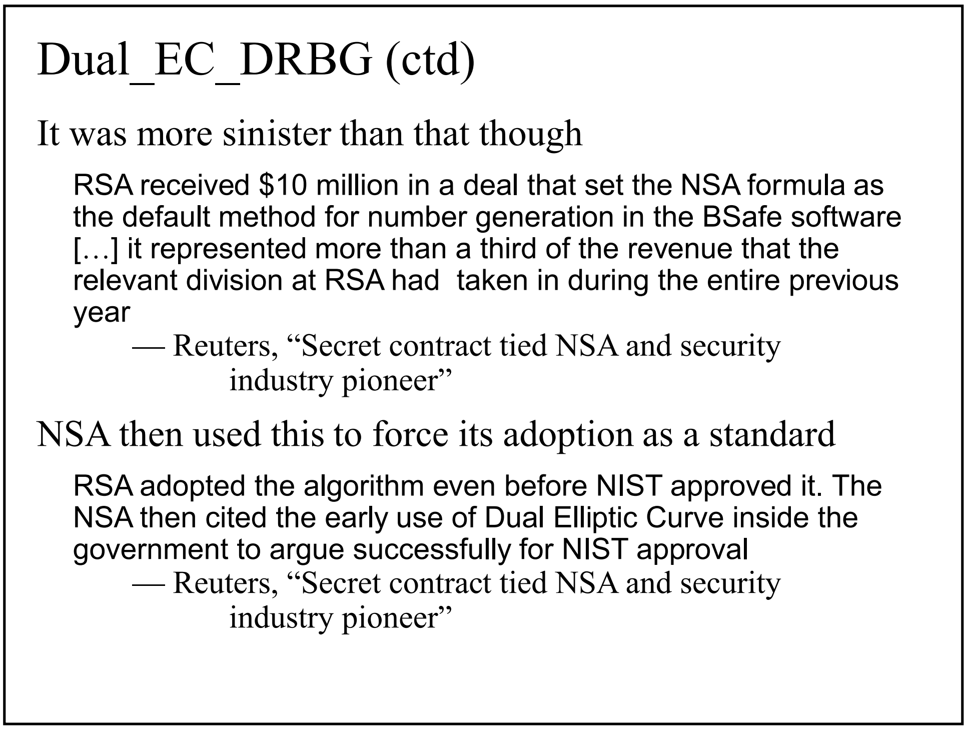
Dual_EC_DRBG (ctd)

WTF RSA?

- Specified in a NIST standard
- Lots of government customers
- Implemented several of the generators in the standard
  - Including the dumb ones
- Speculation: “It would really help this large government contract if you made EC_DRBG he default. It’s OK, it’s a NIST-approved generator like all the others”

RSA mostly confirmed this

> RSA’s market for encryption tools was increasingly limited to the US Federal government […] use of this algorithm as a default […] allowed us to meet government certification requirements
>
> — Art Coviello, Executive Chairman, RSA



Dual_EC_DRBG (ctd)

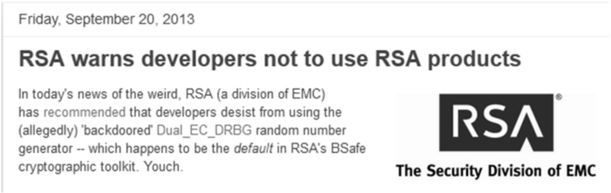
It was more sinister than that though

> RSA received $10 million in a deal that set the NSA formula as the default method for number generation in the BSafe software […] it represented more than a third of the revenue that the relevant division at RSA had taken in during the entire previous year
>
> — Reuters, “Secret contract tied NSA and security industry pioneer”

NSA then used this to force its adoption as a standard

> RSA adopted the algorithm even before NIST approved it. The NSA then cited the early use of Dual Elliptic Curve inside the government to argue successfully for NIST approval
>
> — Reuters, “Secret contract tied NSA and security industry pioneer”

Dual_EC_DRBG (ctd)



Friday, September 20, 2013

RSA warns developers not to use RSA products

In today's news of the weird, RSA (a division of EMC) has recommended that developers desist from using the (allegedly) 'backdoored' Dual_EC_DRBG random number generator -- which happens to be the *default* in RSA's BSafe cryptographic toolkit. Youch.

Dual_EC_DRBG (ctd)

Microsoft's reason for adding it parallels the RSA one (without the bribe):

> Microsoft decided to include the algorithm in its operating system because a major customer was asking for it
>
> — Kim Zetter, Wired

As does OpenSSL's

> It was requested by a sponsor as one of several deliverables. The reasoning at the time was that we would implement any algorithm based on official published standards
>
> — "Flaw in Dual EC DRBG (no, not that one)",
> Steve Marquess

Dual_EC_DRBG (ctd)

It's OK though, apart from RSA (and Lancope) no-one made it the default

- It has to be explicitly configured to be the default

Surely no-one would do that

- Except perhaps a large government organisation…

  … the NSA hacked into target computers…

  … to the consumer the systems' security remains intact…

Just the mere *presence* of such a facility is already a security risk

How to Backdoor Dual_EC_DRBG

Backdoor capability was first pointed out in 2005

> If P and Q are established in a security domain controlled by an administrator, and the entity who generates Q for the domain does so with knowledge of e (or indirectly via knowledge of d), the administrator will have an escrow key for every ECRNG that follows that standard
>
> — "Elliptic curve random number generation",
> Patent Application CA2594670 A1, 21 January 2005

How to Backdoor Dual_EC_DRBG (ctd)

In December 2013, Aris Adamantiadis released OpenSSL-based proof-of-concept code to backdoor the EC_DRBG

> It is quite obvious in light of the recent revelations from Snowden that this weakness was introduced by purpose by the NSA. It is very elegant and leaks its complete internal state in only 32 bytes of output […] It is obviously complete madness to use the reference implementation from NIST
>
> — Aris Adamantiadis, "Dual_EC_DRBG backdoor: a proof of concept"

Used his own EC parameters (not the NIST ones)

- Only the NSA can break the one with the NIST parameters, since it requires knowledge of the secret value *d* used to generate them

How to Backdoor Dual_EC_DRBG (ctd)

Researchers later created a proof-of-concept using real-world crypto implementations

- Patched Dual EC DRBG in RSA's BSAFE, Windows SChannel, and OpenSSL
- Substituted ECC parameters for which they knew the private key for the ones where the NSA knew the private key

Key recovery for RSA's BSAFE-C takes 4 seconds

- Support for the NSA's crypto-weakening extensions makes this even worse

> [A server] which supports Extended Random exposes a sufficient quantity of contiguous key bytes to enable quick recovery of the session keys
>
> — "On the Practical Exploitability of Dual EC in TLS Implementations"

How to Backdoor Dual_EC_DRBG (ctd)

> The Dual EC disaster led to a rethink of how we manage computer security standards at NIST
>
> NSA-developed algorithms will require public review and analysis to be considered for inclusion in NIST standards/guidelines
>
> — "Dual EC DRBG and NIST Crypto Process Review",
> John Kelsey, NIST

How Dual_EC_DRBG was Backdoored

In 2015, it was revealed that Juniper's used of the backdoored Dual_EC_DRBG had in turn been backdoored

- Juniper routers used Dual_EC_DRBG as their PRNG
- Attackers replaced the NSA-generated values with their oen ones

Juniper tried to protect against this by following the Dual_EC_DRBG with the ANSI X9.17/X9.31 PRNG

- This should have masked the output of the backdoored PRNG

How Dual_EC_DRBG was Backdoored (ctd)

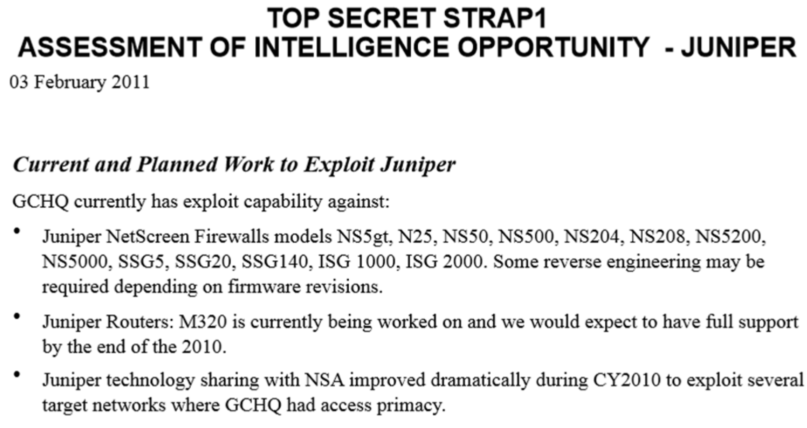
The implementation had a bug, so the second PRNG was never invoked

- Raw output from the double-backdoored PRNG was fed to attackers

> The error appears to predate the unauthorized changing of the Q point by unknown attackers and can be viewed as a backdoor itself
>
> — "The Juniper VPN backdoor: buggy code with a dose of shady NSA crypto", CSO Online,

How Dual_EC_DRBG was Backdoored (ctd)

Who could have done this?



TOP SECRET STRAP1
ASSESSMENT OF INTELLIGENCE OPPORTUNITY - JUNIPER

03 February 2011

Current and Planned Work to Exploit Juniper

GCHQ currently has exploit capability against:

- Juniper NetScreen Firewalls models NS5gt, N25, NS50, NS500, NS204, NS208, NS5200, NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. Some reverse engineering may be required depending on firmware revisions.
- Juniper Routers: M320 is currently being worked on and we would expect to have full support by the end of the 2010.
- Juniper technology sharing with NSA improved dramatically during CY2010 to exploit several target networks where GCHQ had access primacy.

How Dual_EC_DRBG was Backdoored (ctd)

Actually we have no idea…

- Backdoors are user-agnostic

Given the number that were present, it could have been ones from both our "friends" and our enemies

> The weakness in the VPN itself that enables passive decryption is only of benefit to a national surveillance agency like the British, the US, the Chinese, or the Israelis
>
> — "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors", Wired

We say backdoor, you say דלת אחורית, they say 后门

- The backdoor doesn't care who uses it, or how

NIST ECC Curves

ECC isn't so much an algorithm as a set of toothpicks and a tube of glue

- All the bells, whistles, and gongs you'll ever need

Need to define standardised parameters ("curves") for interoperability

- NIST defined several
- Most common are P256, P384, and P512

NIST ECC Curves (ctd)

Example: P256 curve over a prime field

Prime p = 11579208921035624876269744694940757353008614341529031419
5533631308867097853951

Parameter a = 11579208921035624876269744694940757353008614341529031
4195533631308867097853948

Parameter b = 41058363725152142129326129780047268409114441015993725
554835256314039467401291

Base point xG = 484395612939064517590525852527979142027629495260417
47995844080717082404635286

Base point yG = 36134250956749795798585127919587881956611106672985
015071877198253568414405109

Order q of the point G = 1157920892103562487626974469494075735299969
55224135760342422259061068512044369

- (You are not expected, etc)

NIST ECC Curves (ctd)

How were these generated?

- Deterministically (i.e. verifiably), from a public seed value

What’s the seed value?

- C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

Where did that come from?

- Jerry Solinas at the NSA
- (Jerry is a known ECC mathematician at the NSA)

NIST ECC Curves (ctd)

So how would you use this to backdoor the NIST curves?

- Suppose the NSA knew of (say) a 2^{64} attack that breaks one 256-bit curve in a billion
- The NSA can recognise from the group order whether an attack on the curve will be successful (reasonable assumption)

This isn't as unlikely as it seems

- Whole classes of elliptic curves are vulnerable to various attacks that make them (relatively) easy to break
- Generating curve parameters is a lengthy, involved process to find one that isn't vulnerable to the catalogue of known attacks

NIST ECC Curves (ctd)

Time to generate a chosen curve that passes the NIST checks: 78 minutes on a single-core AMD CPU

> We found a desired curve which we call BADA55-R-256 with b = 0x5AFEBADA55ECC5AFEBADA55ECC5AFEBADA5 5ECC5AFEBADA55ECC5AFEBADA5A57
>
> — "How to Manipulate Curve Standards"

Extending this to hashed curves required 7 hours on a GPU cluster

> Acknowledgements: This work did not receive the funding that it so richly deserves from the US National Security Agency
>
> — "How to Manipulate Curve Standards"

NIST ECC Curves (ctd)

NSA generates billions of seeds, from which they generate curves until they find one that’s vulnerable to this attack

- Get it adopted as a NIST standard…
- … which is the de facto standard used by US software vendors …
- … which is the de facto global standard
  – (Speculation courtesy Dan Bernstein)

The curve is “verifiable” in the sense that it was verifiably generated from the seed

- At that point, things stop

Scenario fits the NIST curves

NIST ECC Curves (ctd)

Other standards are even worse

- Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI, France)
- b = 0xEE353FCA5428A9300D4ABA754A44C00FDFE C0C9AE4B1A1803075ED967B7BB73F
- p = 0xF1FD178C0B3AD58F10126DE8CE42435B3961 ADBCABC8CA6DE8FCF353D86E9C03
- Office of the State Commercial Cryptography Administration (OSCCA, China)
- b = 0x28E9FA9E9D9F5E344D5A9E4BCF6509A7F397 89F515AB8F92DDBCBD414D940E93
- p = 0xFFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFF00000000FFFFFFFFFFFFFFFF

These could be anything…

NIST ECC Curves (ctd)

European Brainpool curve designers recognised this in 2005

> The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open
>
> No proofs are provided that the proposed curves do not belong to those classes of curves for which more efficient cryptanalytic attacks are possible
>
> — "ECC Brainpool Standard Curves and Curve Generation"

Brainpool curves compute their seeds from π

- Newer designs like Dan Bernstein's Curve25519 have even more defences built in

Nothing up my sleeve (NUMS) values

NIST ECC Curves (ctd)

In October 2013, RFC 7027 on using the Brainpool curves in TLS was published

- Announced on the TLS mailing list on 15 October 2013

Support added in OpenSSL, cryptlib, PolarSSL on the same day

- Other implementations added support within days

The TLS working group has never moved so quickly on an issue before…

Reflections on Trusting Trust

In 1984, Ken Thompson delivered his Turing Award acceptance speech (which probably merited a second Turing Award)

How do you undetectably backdoor an OS?

- Backdoor the login program

This is a pretty obvious hole…

- Backdoor the compiler
- When it detects that it's building the login program, it inserts the backdoor

Login program is backdoored but source code is clean

Reflections on Trusting Trust (ctd)

What if someone audits the compiler?

- Backdoor the compiler as well

Compiler detects when it's compiling itself

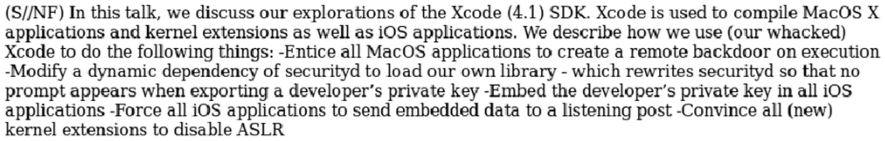
- Inserts code to backdoor the login program into the compiler binary

Compiler compiles itself, compiler source is cleaned up, now you have a backdoor that's undetectable without binary analysis of most of the OS and its utilities

- (The backdoor could be somewhere other than the login program, or could be inserted by the linker or loader)

Reflections on Trusting Trust (ctd)

What if you backdoored Apple’s Xcode SDK in this manner?



(S//NF) In this talk, we discuss our explorations of the Xcode (4.1) SDK. Xcode is used to compile MacOS X applications and kernel extensions as well as iOS applications. We describe how we use (our whacked) Xcode to do the following things: -Entice all MacOS applications to create a remote backdoor on execution -Modify a dynamic dependency of securityd to load our own library - which rewrites securityd so that no prompt appears when exporting a developer’s private key -Embed the developer’s private key in all iOS applications -Force all iOS applications to send embedded data to a listening post -Convince all (new) kernel extensions to disable ASLR

- Force apps to create a remote backdoor on execution
- Rewrite `securityd` to allow silent private key export
- Embed the developer's private key in apps they build
- Force apps to exfiltrate data to remote listening posts
- Make kernel extensions disable security measures

IPsec

It can’t have got that bad by accident

> IPsec was a great disappointment to us […] virtually nobody is satisfied with the process or the result […] the documentation is very hard to understand […] the ISAKMP specifications [the NSA’s main overt contribution to IPsec] contain numerous errors, essential explanations are missing, and the document contradicts itself in various places […] none of the IPsec documentation provides any rationale for any of the choices that were made […] the reviewer is left to guess […]
>
> —“A Cryptographic Evaluation of IPsec”,
> Niels Ferguson and Bruce Schneier,
> from the first 5 pages of 28

You mean they did this *on purpose*?

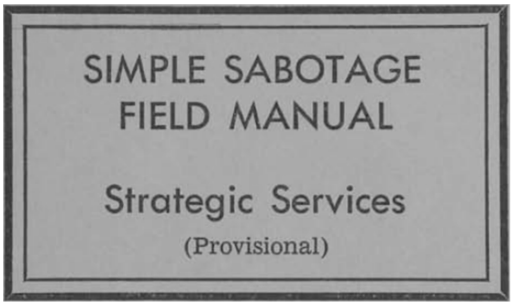
IPsec (ctd)

Hello? I've just committed IPsec and I did it on purpose!
— "Last Action Hero", 1993

Apparently so…

IPsec (ctd)

There's a long history behind this sort of thing

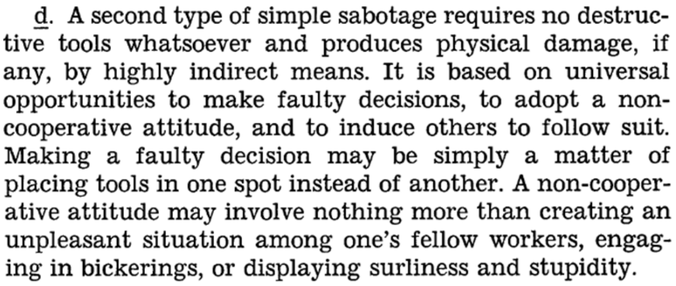


SIMPLE SABOTAGE
FIELD MANUAL

Strategic Services
(Provisional)

OSS field manual, 1945

IPsec (ctd)



d. A second type of simple sabotage requires no destructive tools whatsoever and produces physical damage, if any, by highly indirect means. It is based on universal opportunities to make faulty decisions, to adopt a non-cooperative attitude, and to induce others to follow suit. Making a faulty decision may be simply a matter of placing tools in one spot instead of another. A non-cooperative attitude may involve nothing more than creating an unpleasant situation among one's fellow workers, engaging in bickerings, or displaying surliness and stupidity.

IPsec (ctd)

(a) Organizations and Conferences

(1) Insist on doing everything through "channels." Never permit short-cuts to be taken in order to, expedite decisions.

(2) Make "speeches." Talk as frequently as possible and at great length. Illustrate your "points" by long anecdotes and accounts of personal experiences. Never hesitate to make a few appropriate "patriotic" comments.

(3) When possible, refer all matters to committees, for "further study and consideration." Attempt to make the committees as large as possible - never less than five.

(4) Bring up irrelevant issues as frequently as possible.

(5) Haggle over precise wordings of communications, minutes, resolutions.

(6) Refer back to matters decided upon at the last meeting and attempt to reopen the question of the advisability of that decision.

(7) Advocate "caution." Be "reasonable" and urge your fellow-conferees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.

(8) Be worried about the propriety of any decision -raise the question of whether such action as is contemplated lies within the jurisdiction of the group or whether it might conflict with the policy of some higher echelon.

IPsec (ctd)

(b) Managers and Supervisors

(1) Demand written orders.

(2) "Misunderstand" orders. Ask endless questions or engage in long correspondence about such orders. Quibble over them when you can.

(3) Do everything possible to delay the delivery of orders. Even though parts of an order may be ready beforehand, don't deliver it until it is completely ready.

(4) Don't order new working materials until your current stocks have been virtually exhausted, so that the slightest delay in filling your order will mean a shutdown.

(5) Order high-quality materials which are hard to get. If you don't get them argue about it. Warn that inferior materials will mean inferior work.

(6) In making work assignments, always sign out the unimportant jobs first. See that the important jobs are assigned to inefficient workers of poor machines.

(7) Insist on perfect work in relatively unimportant products; send back for refinishing those which have the least flaw. Approve other defective parts whose flaws are not visible to the naked eye.

(8) Make mistakes in routing so that parts and materials will be sent to the wrong place in the plant.

(9) When training new workers, give incomplete or misleading instructions.

(10) To lower morale and with it, production, be pleasant to inefficient workers; give them undeserved promotions. Discriminate against efficient workers; complain unjustly about their work.

(11) Hold conferences when there is more critical work to be done.

(12) Multiply paper work in plausible ways. Start duplicate files.

(13) Multiply the procedures and clearances involved in issuing instructions, pay checks, and so on. See that three people have to approve everything where one would do.

IPsec (ctd)

Hey, I resemble that remark!

- This process may be hard to distinguish from SOP for many organisations

(For people who want this list for use at work: `http://svn.cacert.org/CAcert/CAcert_Inc/Board/oss/OSS_Simple_Sabotage_Manual.pdf`)

IPsec (ctd)

So was IPsec deliberately sabotaged?

- Probably not

Never attribute to malice what is adequately explained by ~~stupidity~~ a committee

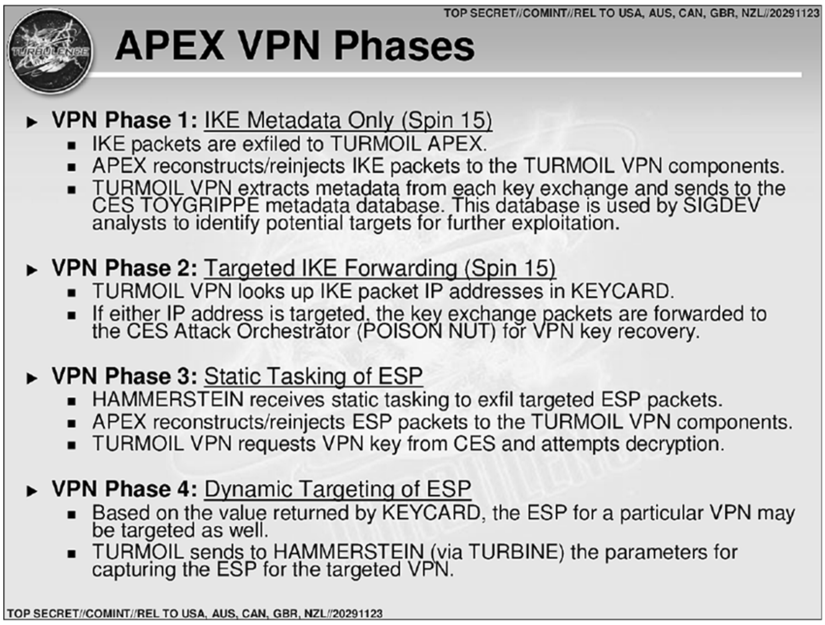
> Lesson 1: Cryptographic protocols should not be developed by a committee
>
> — "A Cryptographic Evaluation of IPsec",
> Niels Ferguson and Bruce Schneier

BULLRUN Again…

In any case IPsec doesn't matter much…

- The NSA have tools for subverting it

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

APEX VPN Phases

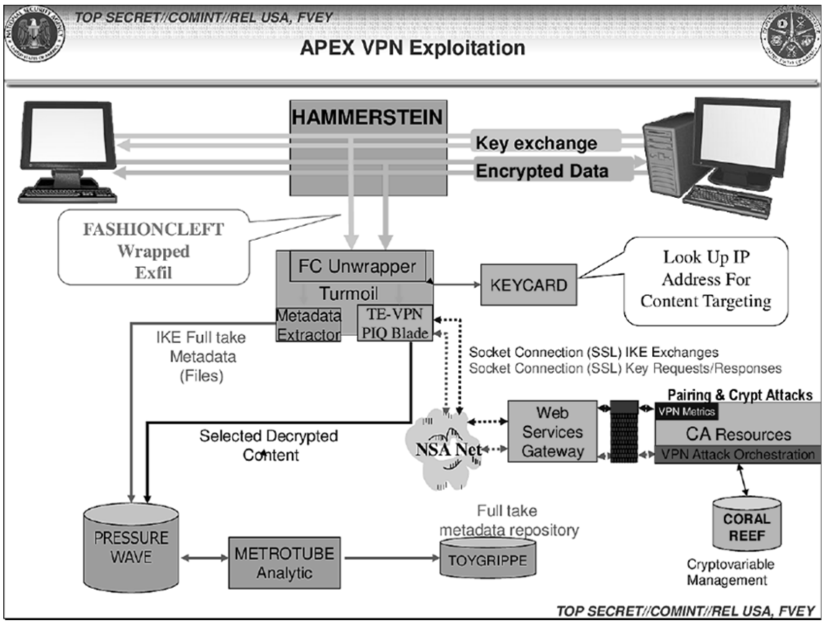
- **VPN Phase 1:** IKE Metadata Only (Spin 15)
  - IKE packets are exfiled to TURMOIL APEX.
  - APEX reconstructs/reinjects IKE packets to the TURMOIL VPN components.
  - TURMOIL VPN extracts metadata from each key exchange and sends to the CES TOYGRIPPE metadata database. This database is used by SIGDEV analysts to identify potential targets for further exploitation.
- **VPN Phase 2:** Targeted IKE Forwarding (Spin 15)
  - TURMOIL VPN looks up IKE packet IP addresses in KEYCARD.
  - If either IP address is targeted, the key exchange packets are forwarded to the CES Attack Orchestrator (POISON NUT) for VPN key recovery.
- **VPN Phase 3:** Static Tasking of ESP
  - HAMMERSTEIN receives static tasking to exfil targeted ESP packets.
  - APEX reconstructs/reinjects ESP packets to the TURMOIL VPN components.
  - TURMOIL VPN requests VPN key from CES and attempts decryption.
- **VPN Phase 4:** Dynamic Targeting of ESP
  - Based on the value returned by KEYCARD, the ESP for a particular VPN may be targeted as well.
  - TURMOIL sends to HAMMERSTEIN (via TURBINE) the parameters for capturing the ESP for the targeted VPN.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

BULLRUN Again… (ctd)

TOP SECRET//COMINT//REL USA, FVEY

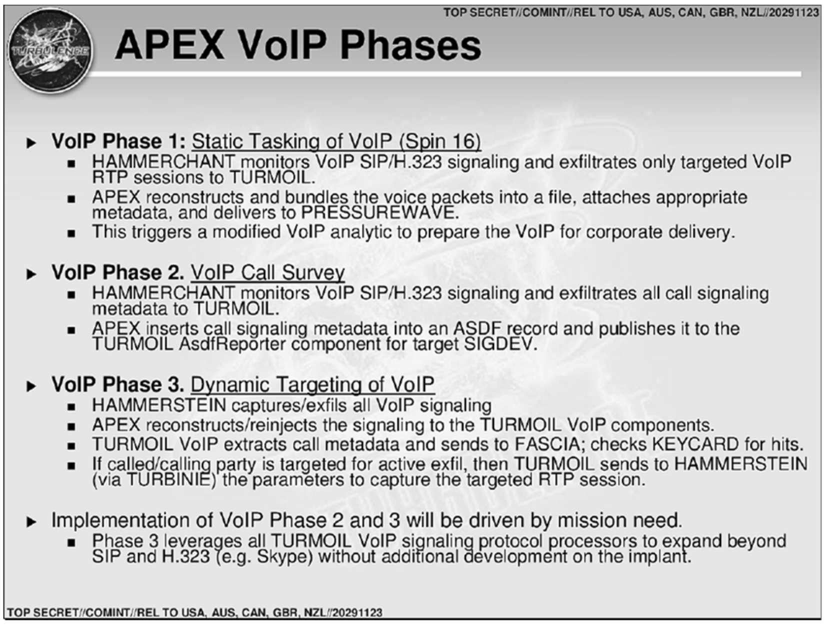
APEX VPN Exploitation



HAMMERSTEIN
Key exchange
Encrypted Data
FASHIONCLEFT Wrapped Exfil
FC Unwrapper
Turmoil
Metadata Extractor
TE-VPN PIQ Blade
KEYCARD
Look Up IP Address For Content Targeting
IKE Full take Metadata (Files)
Socket Connection (SSL) IKE Exchanges
Socket Connection (SSL) Key Requests/Responses
Pairing & Crypt Attacks
VPN Metrics
CA Resources
VPN Attack Orchestration
Web Services Gateway
NSA Net
Selected Decrypted Content
Full take metadata repository
CORAL REEF
Cryptovariable Management
PRESSURE WAVE
METROTUBE Analytic
TOYGRIPPE

TOP SECRET//COMINT//REL USA, FVEY

BULLRUN Again… (ctd)



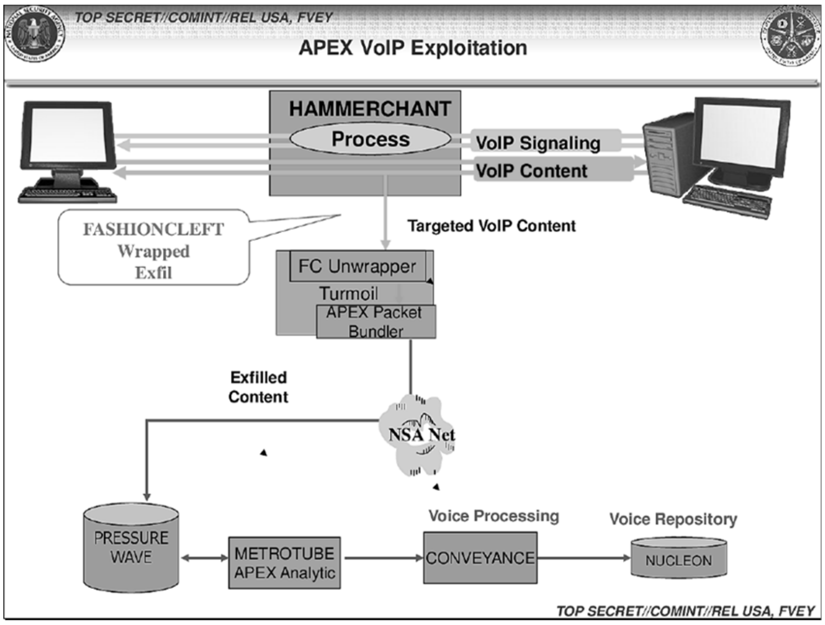
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

APEX VoIP Phases

- **VoIP Phase 1:** Static Tasking of VoIP (Spin 16)
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates only targeted VoIP RTP sessions to TURMOIL.
  - APEX reconstructs and bundles the voice packets into a file, attaches appropriate metadata, and delivers to PRESSUREWAVE.
  - This triggers a modified VoIP analytic to prepare the VoIP for corporate delivery.
- **VoIP Phase 2.** VoIP Call Survey
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates all call signaling metadata to TURMOIL.
  - APEX inserts call signaling metadata into an ASDF record and publishes it to the TURMOIL AsdfReporter component for target SIGDEV.
- **VoIP Phase 3.** Dynamic Targeting of VoIP
  - HAMMERSTEIN captures/exfils all VoIP signaling
  - APEX reconstructs/reinjects the signaling to the TURMOIL VoIP components.
  - TURMOIL VoIP extracts call metadata and sends to FASCIA; checks KEYCARD for hits.
  - If called/calling party is targeted for active exfil, then TURMOIL sends to HAMMERSTEIN (via TURBINIE) the parameters to capture the targeted RTP session.
- Implementation of VoIP Phase 2 and 3 will be driven by mission need.
  - Phase 3 leverages all TURMOIL VoIP signaling protocol processors to expand beyond SIP and H.323 (e.g. Skype) without additional development on the implant.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL USA, FVEY

APEX VoIP Exploitation

HAMMERCHANT

Process

VoIP Signaling

VoIP Content

FASHIONCLEFT Wrapped Exfil

Targeted VoIP Content

FC Unwrapper

Turmoil

APEX Packet Bundler

Exfilled Content

NSA Net

PRESSURE WAVE

METROTUBE APEX Analytic

Voice Processing

CONVEYANCE

Voice Repository

NUCLEON

TOP SECRET//COMINT//REL USA, FVEY

BULLRUN Again… (ctd)

As well as the routers that run it…

- When you own the router that does the crypto, IPsec becomes irrelevant

NSA owns

- Cisco
  - BANANAGLEE, JETPLOW
- Juniper
  - BANANAGLEE, FEEDTROUGH, GOURMETTROUGH, SCHOOLMONTANA, SIERRAMONTANA, SOUFFLETROUGH, VALIDATOR
- Huawei
  - HAMMERMILL, HALLUXWATER, HEADWATER

BULLRUN Again… (ctd)

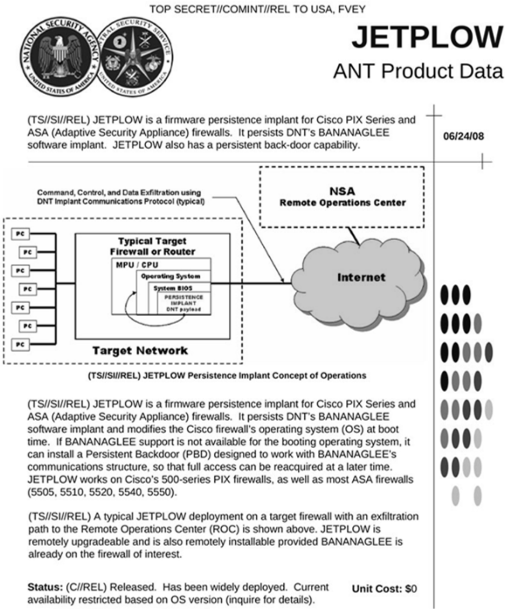
Speaking of routers and security risks…

> Q: Does Huawei represent an unambiguous national security threat to the US and Australia?
> A: Yes, I believe it does
>
> — NSA Director Michael Hayden, interviewed in the Australian Financial Review

> Chinese telecom provider Huawei represents an unambiguous national security threat to the United States and Australia
>
> — "Huawei Is a Security Threat and There's Proof, Says Hayden", eWeek

We'd better go with (expensive) US networking equipment, since we can't trust (cheaper) Huawei gear

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target
Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT DNT payload
Internet
Target Network

(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

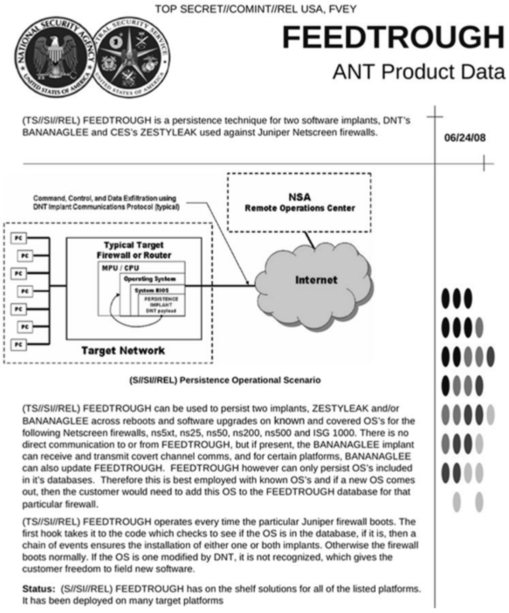
(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details).

Unit Cost: $0

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL USA, FVEY

FEEDTROUGH

ANT Product Data

(TS//SI//REL) FEEDTROUGH is a persistence technique for two software implants, DNT's BANANAGLEE and CES's ZESTYLEAK used against Juniper Netscreen firewalls.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target
Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT DNT payload
Internet
Target Network

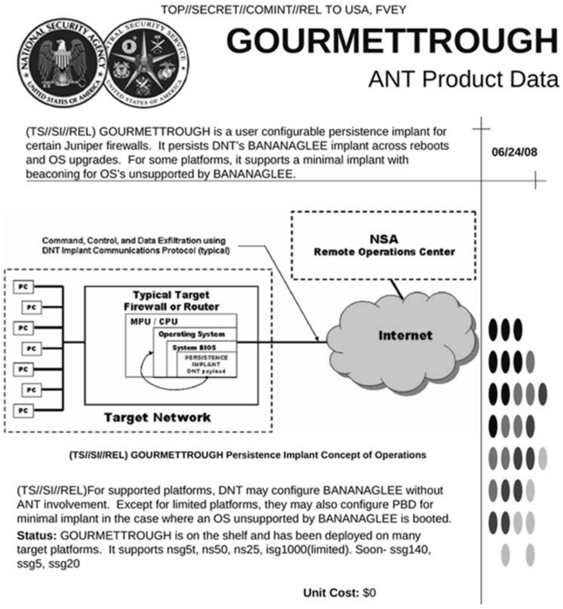
(S//SI//REL) Persistence Operational Scenario

(TS//SI//REL) FEEDTROUGH can be used to persist two implants, ZESTYLEAK and/or BANANAGLEE across reboots and software upgrades on known and covered OS's for the following Netscreen firewalls, ns5xt, ns25, ns50, ns200, ns500 and ISG 1000. There is no direct communication to or from FEEDTROUGH, but if present, the BANANAGLEE implant can receive and transmit covert channel comms, and for certain platforms, BANANAGLEE can also update FEEDTROUGH. FEEDTROUGH however can only persist OS's included in it's databases. Therefore this is best employed with known OS's and if a new OS comes out, then the customer would need to add this OS to the FEEDTROUGH database for that particular firewall.

(TS//SI//REL) FEEDTROUGH operates every time the particular Juniper firewall boots. The first hook takes it to the code which checks to see if the OS is in the database, if it is, then a chain of events ensures the installation of either one or both implants. Otherwise the firewall boots normally. If the OS is one modified by DNT, it is not recognized, which gives the customer freedom to field new software.

Status: (S//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

BULLRUN Again… (ctd)


Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT DNT payload
Target Network
Internet

TOP//SECRET//COMINT//REL TO USA, FVEY

GOURMETTROUGH

ANT Product Data

(TS//SI//REL) GOURMETTROUGH is a user configurable persistence implant for certain Juniper firewalls. It persists DNT's BANANAGLEE implant across reboots and OS upgrades. For some platforms, it supports a minimal implant with beaconing for OS's unsupported by BANANAGLEE.

06/24/08

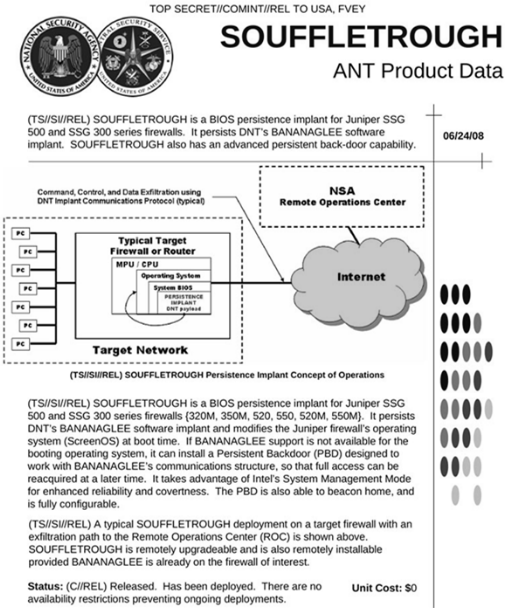
(TS//SI//REL) GOURMETTROUGH Persistence Implant Concept of Operations

(TS//SI//REL)For supported platforms, DNT may configure BANANAGLEE without ANT involvement. Except for limited platforms, they may also configure PBD for minimal implant in the case where an OS unsupported by BANANAGLEE is booted.

Status: GOURMETTROUGH is on the shelf and has been deployed on many target platforms. It supports nsg5t, ns50, ns25, isg1000(limited). Soon- ssg140, ssg5, ssg20

Unit Cost: $0

BULLRUN Again… (ctd)


Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT DNT payload
Target Network
Internet

TOP SECRET//COMINT//REL TO USA, FVEY

SOUFFLETROUGH

ANT Product Data

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls. It persists DNT's BANANAGLEE software implant. SOUFFLETROUGH also has an advanced persistent back-door capability.

06/24/08

(TS//SI//REL) SOUFFLETROUGH Persistence Implant Concept of Operations

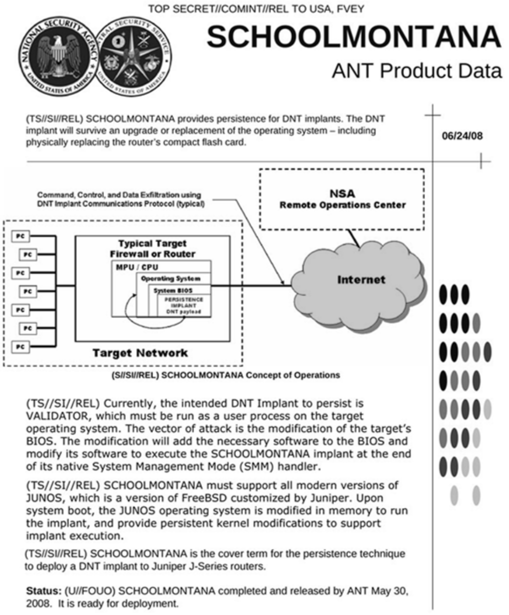
(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls {320M, 350M, 520, 550, 520M, 550M}. It persists DNT's BANANAGLEE software implant and modifies the Juniper firewall's operating system (ScreenOS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. It takes advantage of Intel's System Management Mode for enhanced reliability and covertness. The PBD is also able to beacon home, and is fully configurable.

(TS//SI//REL) A typical SOUFFLETROUGH deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. SOUFFLETROUGH is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been deployed. There are no availability restrictions preventing ongoing deployments.

Unit Cost: $0

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

SCHOOLMONTANA

ANT Product Data

(TS//SI//REL) SCHOOLMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Internet
Target Network

(S//SI//REL) SCHOOLMONTANA Concept of Operations

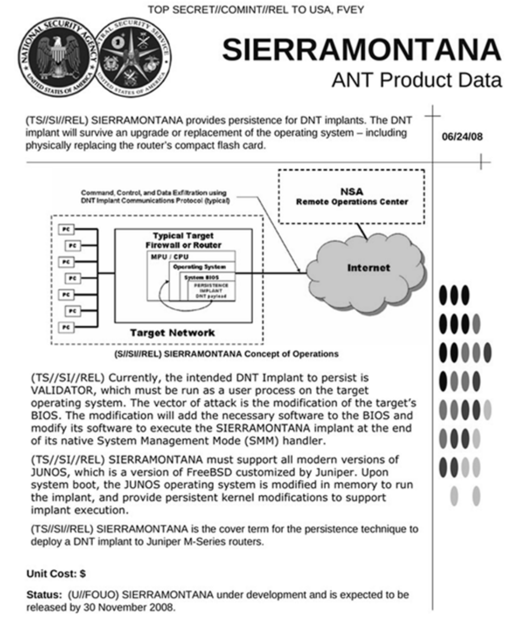
(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the SCHOOLMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) SCHOOLMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) SCHOOLMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper J-Series routers.

Status: (U//FOUO) SCHOOLMONTANA completed and released by ANT May 30, 2008. It is ready for deployment.

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

SIERRAMONTANA

ANT Product Data

(TS//SI//REL) SIERRAMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Internet
Target Network

(S//SI//REL) SIERRAMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the SIERRAMONTANA implant at the end of its native System Management Mode (SMM) handler.

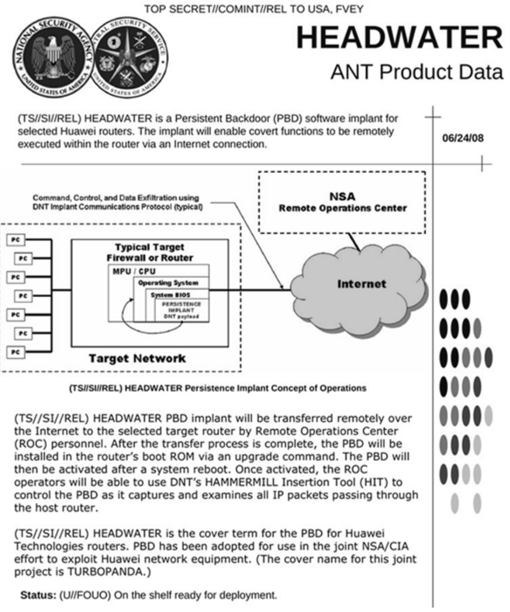
(TS//SI//REL) SIERRAMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) SIERRAMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper M-Series routers.

Unit Cost: $

Status: (U//FOUO) SIERRAMONTANA under development and is expected to be released by 30 November 2008.

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

HEADWATER

ANT Product Data

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

06/24/08

Command, Control, and Data Exfiltration using
DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
Typical Target
Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE
IMPLANT
DNT payload
Internet
Target Network

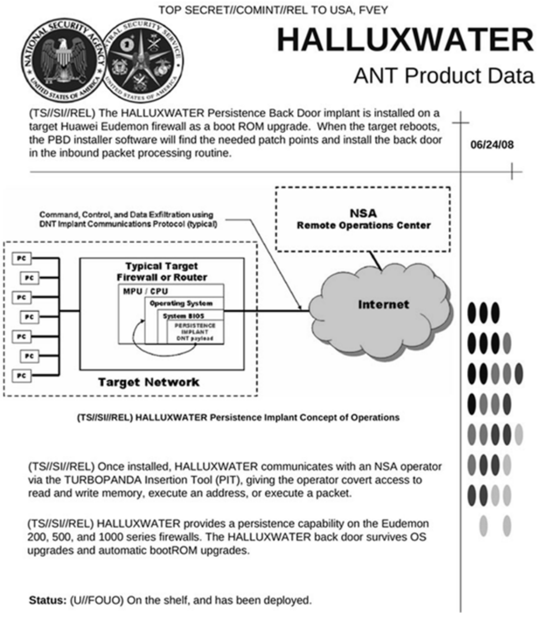
(TS//SI//REL) HEADWATER Persistence Implant Concept of Operations

(TS//SI//REL) HEADWATER PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center (ROC) personnel. After the transfer process is complete, the PBD will be installed in the router's boot ROM via an upgrade command. The PBD will then be activated after a system reboot. Once activated, the ROC operators will be able to use DNT's HAMMERMILL Insertion Tool (HIT) to control the PBD as it captures and examines all IP packets passing through the host router.

(TS//SI//REL) HEADWATER is the cover term for the PBD for Huawei Technologies routers. PBD has been adopted for use in the joint NSA/CIA effort to exploit Huawei network equipment. (The cover name for this joint project is TURBOPANDA.)

Status: (U//FOUO) On the shelf ready for deployment.

BULLRUN Again… (ctd)



TOP SECRET//COMINT//REL TO USA, FVEY

HALLUXWATER

ANT Product Data

(TS//SI//REL) The HALLUXWATER Persistence Back Door implant is installed on a target Huawei Eudemon firewall as a boot ROM upgrade. When the target reboots, the PBD installer software will find the needed patch points and install the back door in the inbound packet processing routine.

06/24/08

Command, Control, and Data Exfiltration using
DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
Typical Target
Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE
IMPLANT
DNT payload
Internet
Target Network

(TS//SI//REL) HALLUXWATER Persistence Implant Concept of Operations

(TS//SI//REL) Once installed, HALLUXWATER communicates with an NSA operator via the TURBOPANDA Insertion Tool (PIT), giving the operator covert access to read and write memory, execute an address, or execute a packet.

(TS//SI//REL) HALLUXWATER provides a persistence capability on the Eudemon 200, 500, and 1000 series firewalls. The HALLUXWATER back door survives OS upgrades and automatic bootROM upgrades.

Status: (U//FOUO) On the shelf, and has been deployed.

BULLRUN Again… (ctd)

While American companies were being warned away from supposedly untrustworthy Chinese routers, foreign organisations would have been well advised to beware of American-made ones. The NSA routinely receives — or intercepts — routers, servers and other computer network devices being exported from the US before they are delivered to the international customers. The agency then implants backdoor surveillance tools, repackages the devices with a factory seal and sends them on

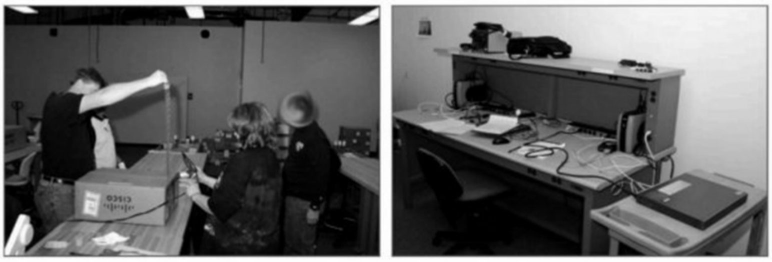
— The Guardian

BULLRUN Again… (ctd)

Here's how it works: shipments of computer network devices (servers, routers, etc,) being delivered to our targets throughout the world are intercepted. Next, they are redirected to a secret location where Tailored Access Operations/Access Operations (AO-S326) employees, with the support of the Remote Operations Center (S321), enable the installation of beacon implants directly into our targets' electronic devices. These devices are then re-packaged and placed back into transit to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO

— NSA's Access and Target Development
June 2010 newsletter

BULLRUN Again… (ctd)



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Source: arstechnica.com

BULLRUN Again… (ctd)

What about the FIPS 140 option for Cisco routers?

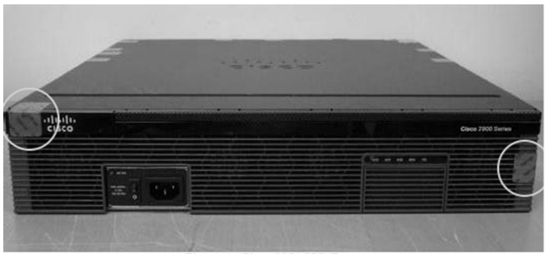


Figure 1: Cisco 2951 ISR Front

- FIPS kit consists of stickers (seals) that you apply after you receive the hardware

BULLRUN Again… (ctd)

Process flow for your FIPS 140-certified router

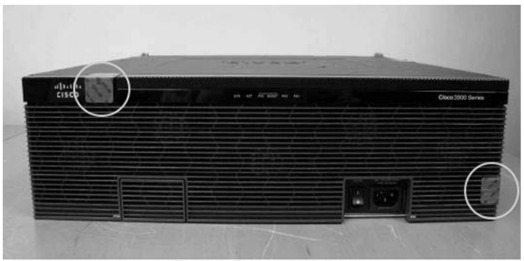


Figure 13: Cisco 3945 ISR Front

- Cisco ships the hardware
- NSA tampers the hardware
- You apply stickers/seals to the hardware to show it's secure

Result: **F**arcical **I**nformation **P**rocessing **S**ecurity

BULLRUN Again… (ctd)

An equally important motive seems to have been preventing Chinese devices from supplanting American-made ones, which would have limited the NSA's own reach

— The Guardian

We simply cannot operate this way; our customers trust us to be able to deliver to their doorsteps products that meet the highest standards of integrity and security

— John Chambers, Cisco CEO, letter to President Obama

BULLRUN Again… (ctd)

Cisco resorted to shipping hardware to fake addresses to avoid NSA tampering

> We ship [boxes] to an address that has nothing to do with the customer and then you have no idea who it is going to
>
> — Cisco security chief John Stewart, "Cisco posts kit to empty houses to dodge NSA chop shops"

- Presumably they subcontract "shipping to an address that has nothing to do with the customer" to DHL Global…

> A world class company shipping to decoy addresses to avoid illegal government spying? What the f**, America?
>
> — Reader comment

Of course since the NSA monitors all communications channels over which the shipping is arranged…

BULLRUN Redux

So this…

> Chinese telecom provider Huawei represents an unambiguous national security threat to the United States and Australia
>
> — "Huawei Is a Security Threat and There's Proof, Says Hayden", eWeek

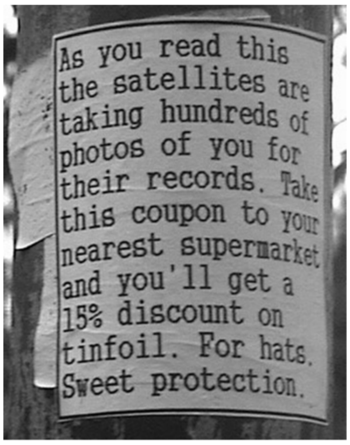
… is really this:

> US intelligence agency NSA represents an unambiguous national security threat to the United States and Australia
>
> — "NSA Is a Security Threat and There's Proof, Says Snowden", TBA

NSA-proof Crypto

We don't need any new "NSA-proof protocols"

- Any well-designed, appropriately-deployed protocol is "NSA-proof"



As you read this the satellites are taking hundreds of photos of you for their records. Take this coupon to your nearest supermarket and you'll get a 15% discount on tinfoil. For hats. Sweet protection.

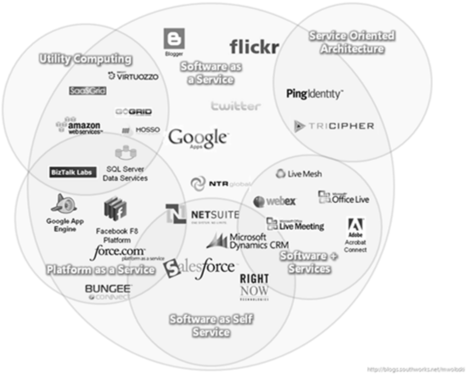
NSA-proof Crypto (ctd)

Any properly-designed and implemented protocol will stop

- The NSA
- The CIA
- The GCSB
- The FSB (née KGB)
- …
- Your mother
- Your cat

NSA-proof Data

Sometimes we don’t need crypto at all



http://blogs.southworks.net/mwoloski

Let’s leverage the synergy of the cloud!

NSA-proof Data (ctd)

What is the cloud anyway?

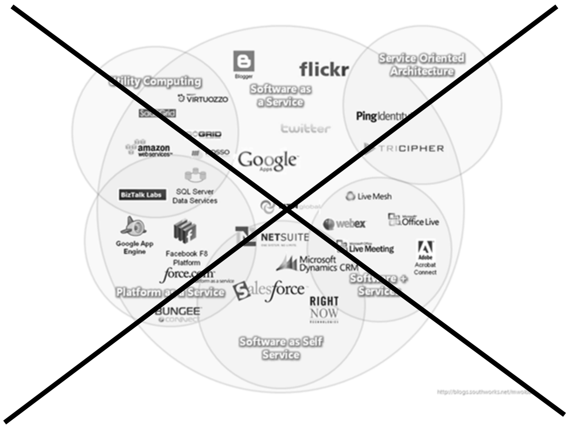
“The cloud” is “someone else’s computer”

- Let's store everyone’s medical records on someone else’s computer
- Let's put our corporate data on someone else’s computer
- Let's archive all our email on someone else’s computer

Have you ever heard a bank say “I know, we’ll put all of our financial information into the cloud”?

NSA-proof Data (ctd)

On second thoughts…



Let’s not.

NSA-proof Data (ctd)

Leverage the safety of your local server

- Getting data from Gmail via an NSL is much easier than getting it from a PC at 81 Princes St, Putaruru 3411, New Zealand

(Counterpoint: Google is better at running a mail server than most companies are)

NSA-proof Data (ctd)

Long-standing financial maxim

If you don’t hold it, you don’t own it

- Preached (if not practiced) by bullion investors everywhere

IT corollary

- If you don’t hold it, maybe the NSA does

NSA-proof Data (ctd)

Goes back to a pre-crypto principle called geographic entitlement

- More modern term: location-limited channel

You have to be at least this close to the data in order to access it

- Works best with short-range links, not long-distance routable protocols

NSA-proof Data (ctd)

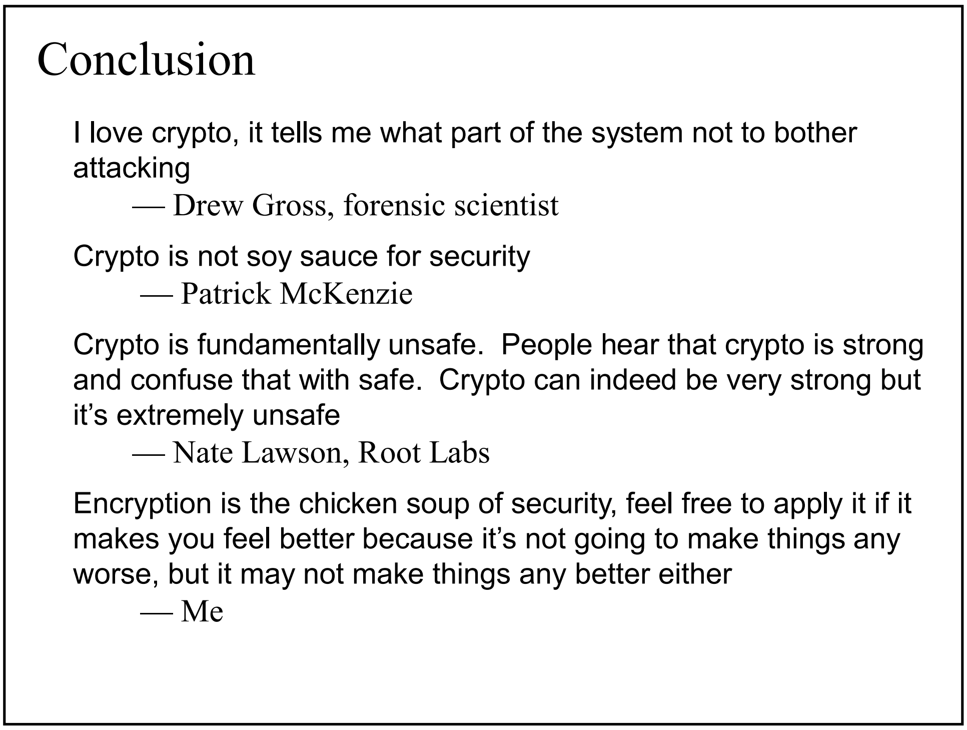
Access to data is predicated on physical access to the location

NSA-proof Data (ctd)

In plain English: Don’t put your data where the NSA can get it

There’s already pushback in Europe against exporting data to the US

- (So now only your local spooks can get it)



Conclusion

I love crypto, it tells me what part of the system not to bother attacking

— Drew Gross, forensic scientist

Crypto is not soy sauce for security

— Patrick McKenzie

Crypto is fundamentally unsafe. People hear that crypto is strong and confuse that with safe. Crypto can indeed be very strong but it's extremely unsafe

— Nate Lawson, Root Labs

Encryption is the chicken soup of security, feel free to apply it if it makes you feel better because it's not going to make things any worse, but it may not make things any better either

— Me