



Supply Chain (In-) Security

Graeme Neilson & Enno Rey

Contact us: graeme@aurasoftwaresecurity.co.nz, erey@ernw.de

Graeme & Enno

■ Graeme Neilson

- Security Consultant & Researcher
- Networking, Reverse engineering, appliances



Graeme & Enno

■ Enno Rey

- Old-school network guy & founder of ERNW
- Blogs at www.insinuator.net
- Regularly rants at **Day-Con**
- Hosts **TROOPERS**



Why this talk

- Most cons have “some specific characteristic”...

- So does Day-Con

- Angus loves talks about “potential future attack paths”
- ... sometimes with a “spooky element” in them
- This talk is our contribution to this space ;-)



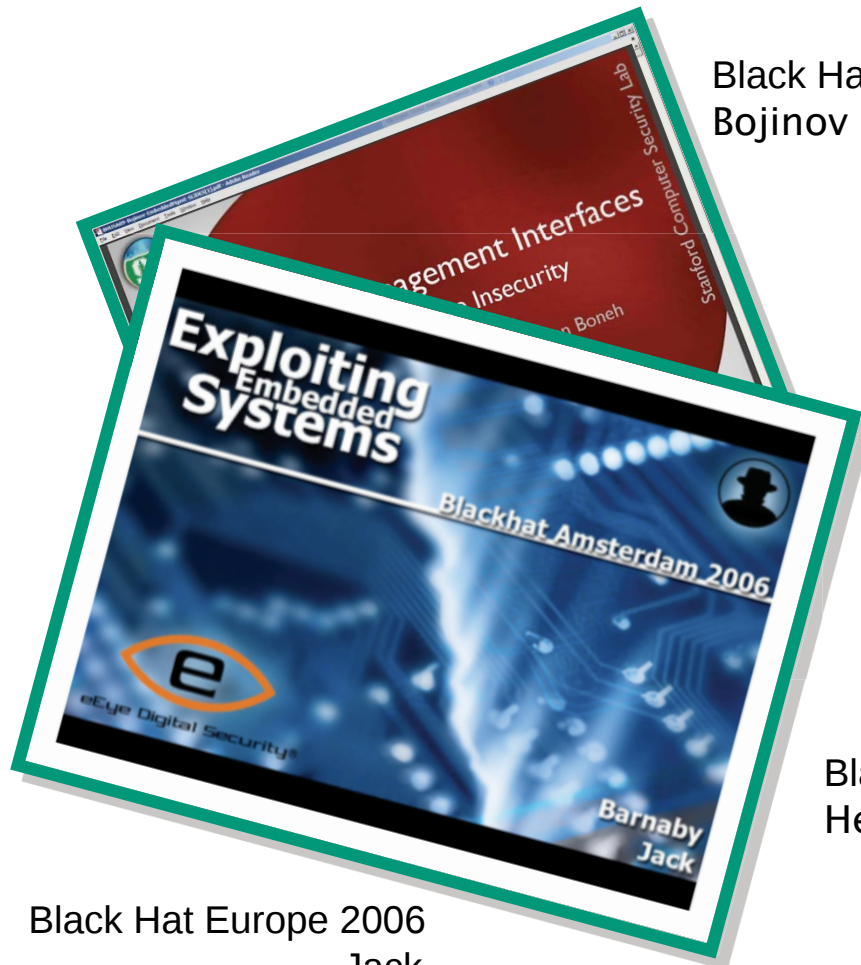
- What we love about Day-Con:
Pretty much all talks make you think.
 - Not just sit around: “cool demo, next one”...

Agenda

- **Supply Chain – Overview**
- **Threats ... & Vulnerabilities**
- **Some common appliances' internal architecture**
- **... and how to attack those**
- **Mitigation & Conclusion**



Device Compromise is a well-known threat...



Black Hat USA 2010
Bojinov



Black Hat USA 2010
Heffner

Black Hat Europe 2010
Mende, Rey

... and there's well known controls for this one

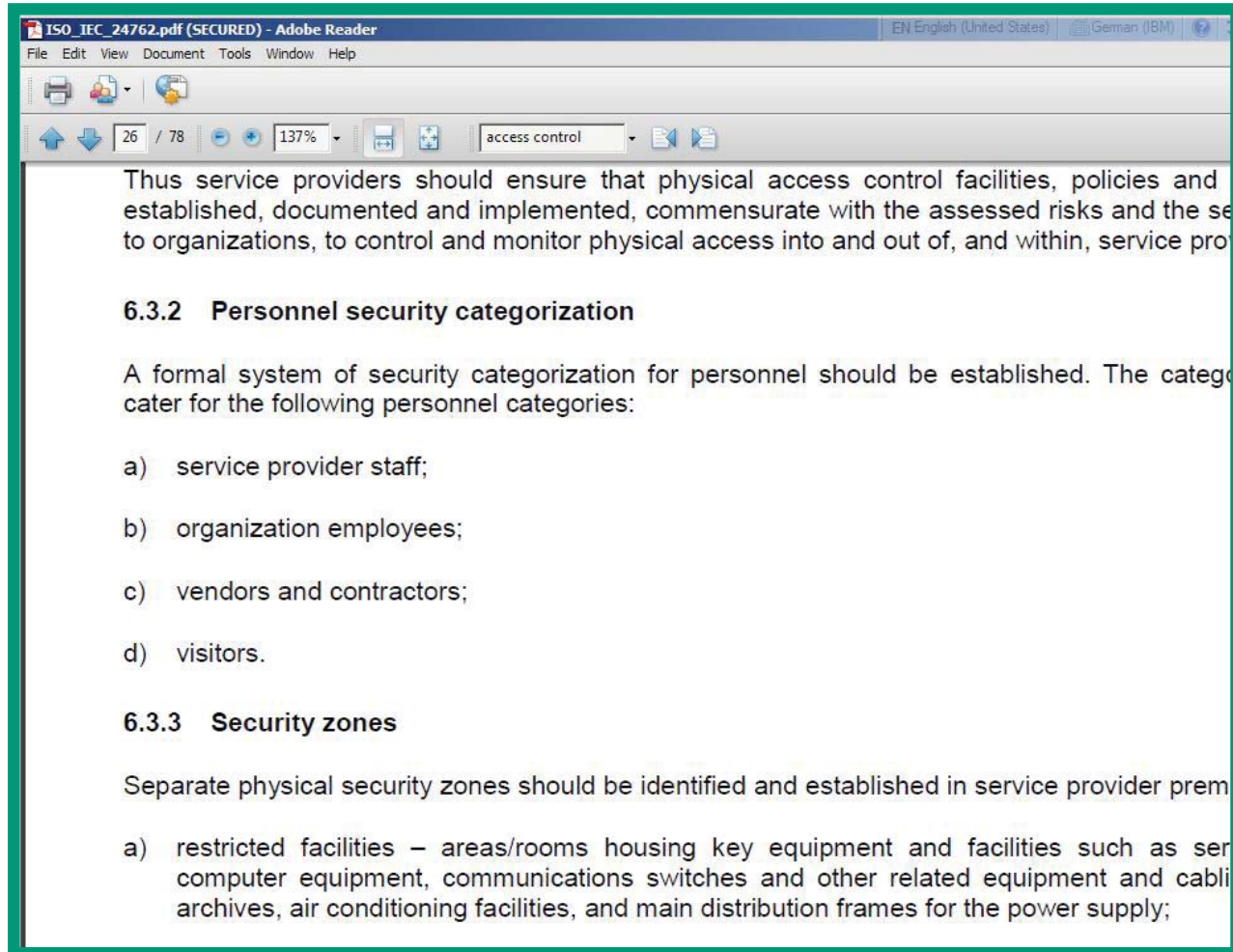
Kaeo Informational [Page 1]
RFC 4778 OPSEC Practices January 2007

Table of Contents

1.	Introduction	2
1.1.	Scope	2
1.2.	Threat Model	3
1.3.	Attack Sources	4
1.4.	Operational Security Impact from Threats	5
1.5.	Document Layout	7
2.	Protected Operational Functions	8
2.1.	Device Physical Access	8
2.2.	Device Management - In-Band and Out-of-Band (OOB)	10
2.3.	Data Path	16
2.4.	Routing Control Plane	18
2.5.	Software Upgrades and Configuration Integrity/Validation	22
2.6.	Logging Considerations	26
2.7.	Filtering Considerations	29
2.8.	Denial-of-Service Tracking/Tracing	30
3.	Security Considerations	32
4.	Acknowledgments	32
5.	References	33
5.1.	Normative References	33
5.2.	Informational References	33
Appendix A.	Protocol Specific Attacks	34
A.1.	Layer 2 Attacks	34
A.2.	IPv4 Protocol-Based Attacks	34
A.3.	IPv6 Attacks	36



... and there's well known controls for this one



... at least for some attack vectors

- **Remote Compromise**



- **Physical access to device
(on organization's premise)**



But...

... some thing may be overlooked here

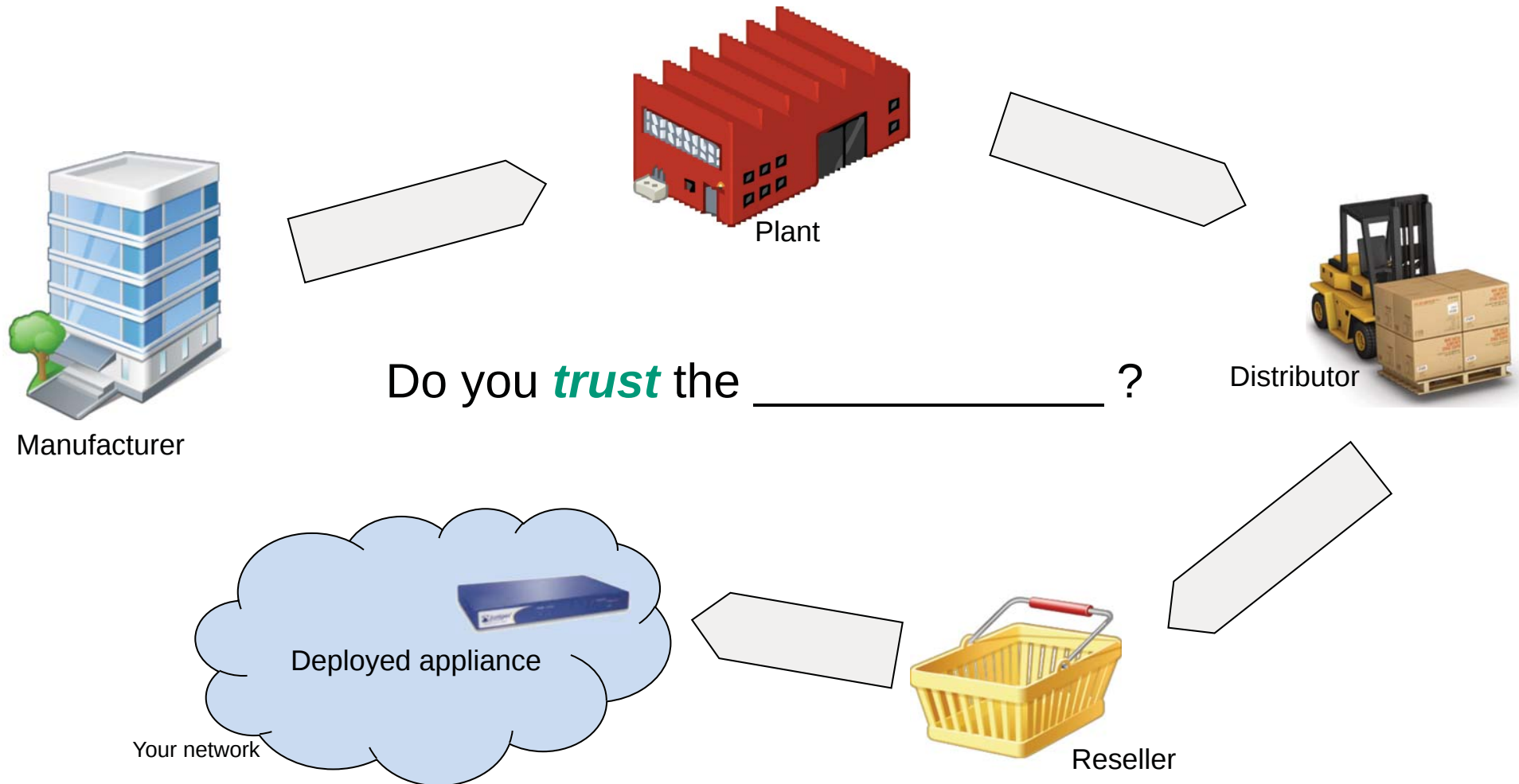


Ask yourselves

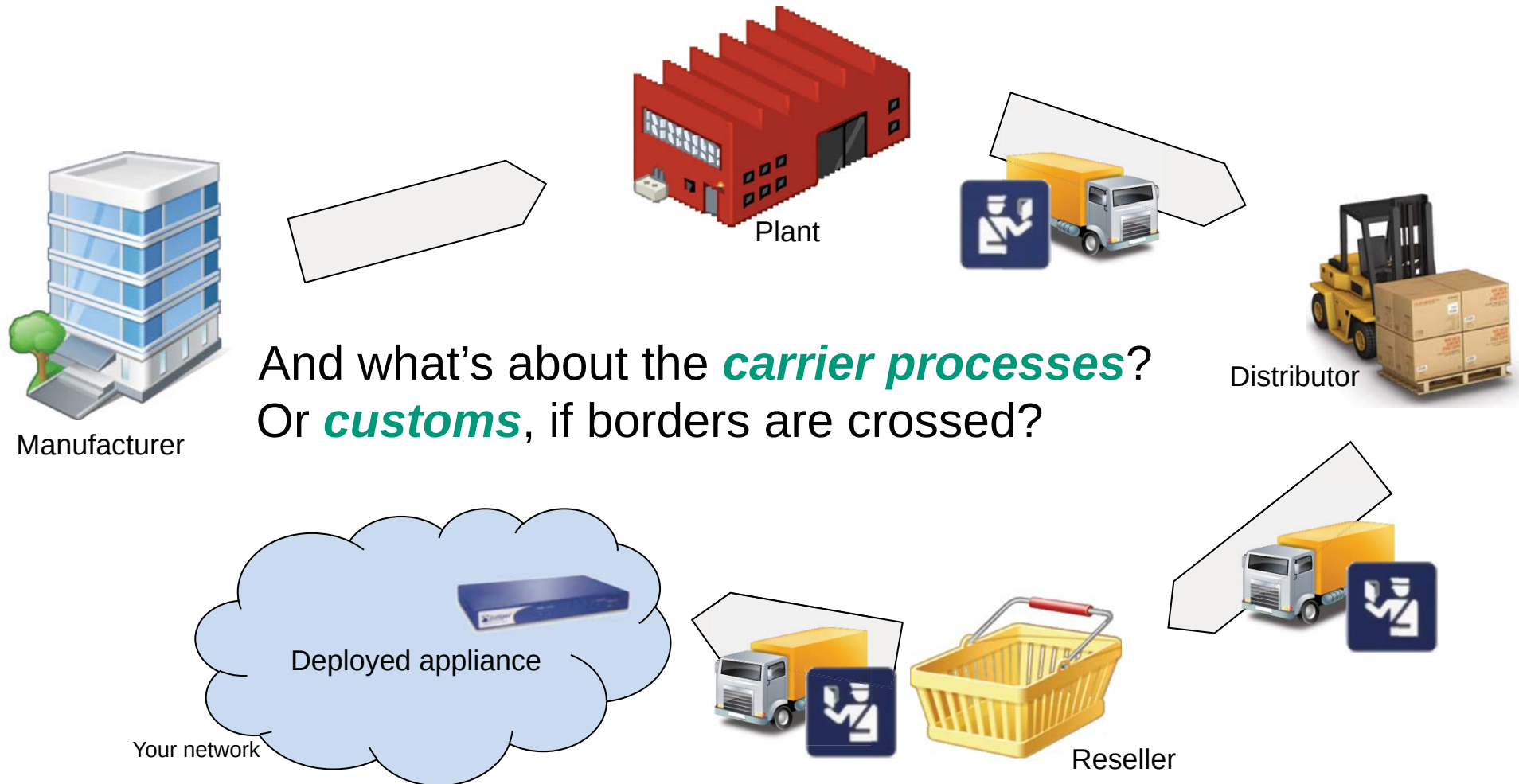
- **Who touches a device BEFORE it enters an organization's premises?**



Overview Supply Chain



Overview Supply Chain



We won't discuss "the malicious manufacturer scenario" here

[Home](#) / [News & Blogs](#) / [Zero Day](#)

Scammers caught backdooring chip and PIN terminals

By Dancho Danchev | August 19, 2008, 1:51pm PDT

Summary

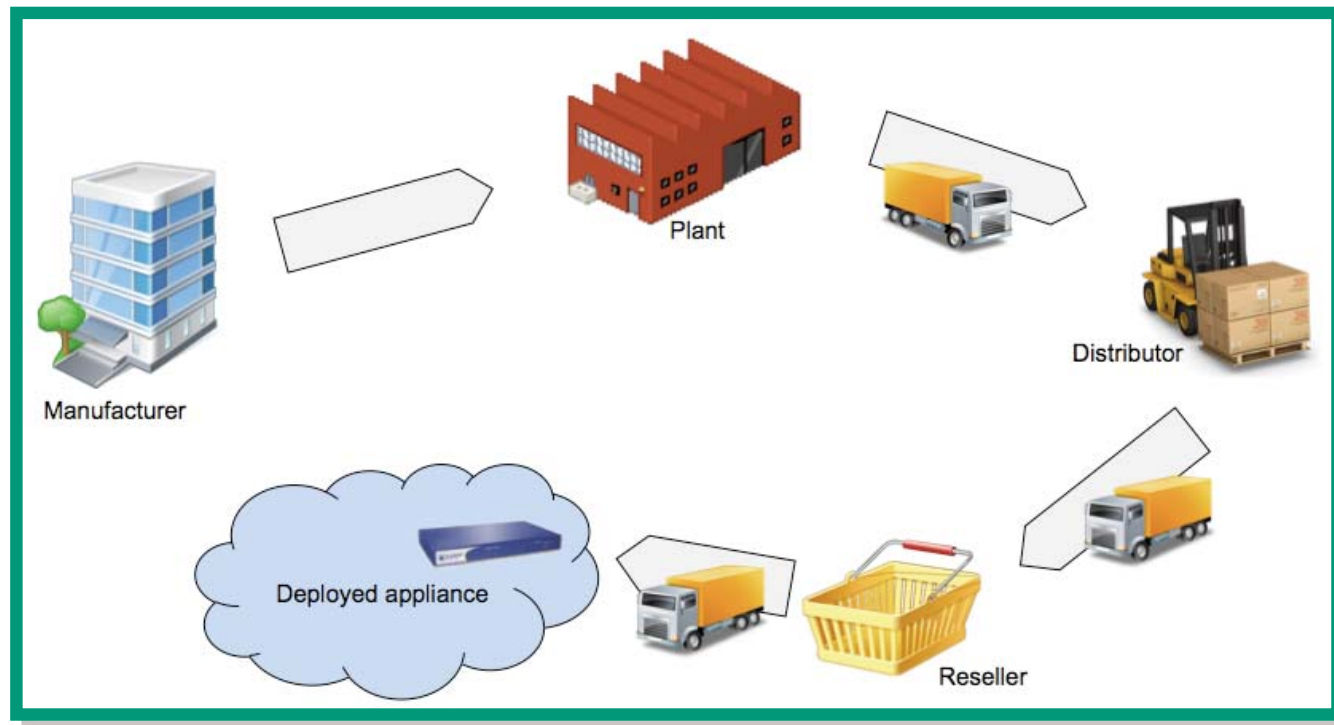
The U.K's Dedicated Cheque and Plastic Crime Unit (DCPU) have recently uncovered state of the art social engineering scheme, where once backdoored, chip and PIN terminals were installed at retailers

The U.K's Dedicated Cheque and Plastic Crime Unit (DCPU) have recently uncovered state of the art social engineering scheme, where once backdoored, chip and PIN terminals were installed at retailers and petrol stations in an attempt to steal the credit card details passing through. Originally, before online banking took place proportionally with the developments on the banker malware front, scammers used to take advantage of old-fashioned ATM skimming and fake keypad devices, which were installed at less popular locations due to the



So what does this mean?

- Potentially every party in this chain might be able to touch “sensitive parts” of the device.



And maybe not only authorized parties

MOVING FORWARD

LEARN MORE

ON NOVEMBER 2ND VOTE FOR COUNTYWIDE TRANSPORTATION

Pd. Pol. Adv. paid for by Moving Hillsborough Forward, 4300 West Cypress Street, Suite 250 Tampa, FL 33607

St. Petersburg Times

Most emailed

- ❑ Sports on TV/radio
- ❑ Caliente nudist resort to be scene of new TV reality show
- ❑ Royal Bank of Scotland seeks to foreclose on Tampa's 'Beer Can' tower
- ❑ Officials advise New Tampa residents to boil water while cloudiness examined
- ❑ Former Florida Gators quarterback Cameron Newton has blossomed into a Heisman Trophy candidate at Auburn

Public Safety: Crime

- ❑ Inmate tried to grab deputy's gun in escape attempt, ...

Thieves swipe thousands of laptops from Special Ops contractor in Hillsborough

By [Dong-Phuong Nguyen](#), Times Staff Writer
In Print: Tuesday, July 13, 2010

On March 6, as many as seven people broke into iGov Technologies at 9211 Palm River Road and stole 3,000 laptops and other electronics, according to a search warrant.



[STEPHEN J. CODDINGTON | Times]

TAMPA — The thieves hit on a weekend when no one was around.

The target: a military contractor for the super secret Special Operations

[Print](#) [Email](#) [Post](#) [Republish](#)

Story Tools

[Comment on this story](#) [Contact the editor](#)

Want more breaking news?

Sign Up For Breaking News

E-mail Newsletters

Subscribe to the Times



Click here for daily delivery of the St. Petersburg Times.

ADVERTISEMENT

Creamy Olive Dip



What do you mean by “sensitive parts”?

- **Bootloader**



- **Firmware / Image**



- **Configuration Files**



“At a device’s going-into-production, we replace those anyway”

- Are you sure?



- For the bootloader??

- Would you notice (and delete) a user “sysupdate” in the administrators group of \$SOME_SECURITY_APPLIANCE?

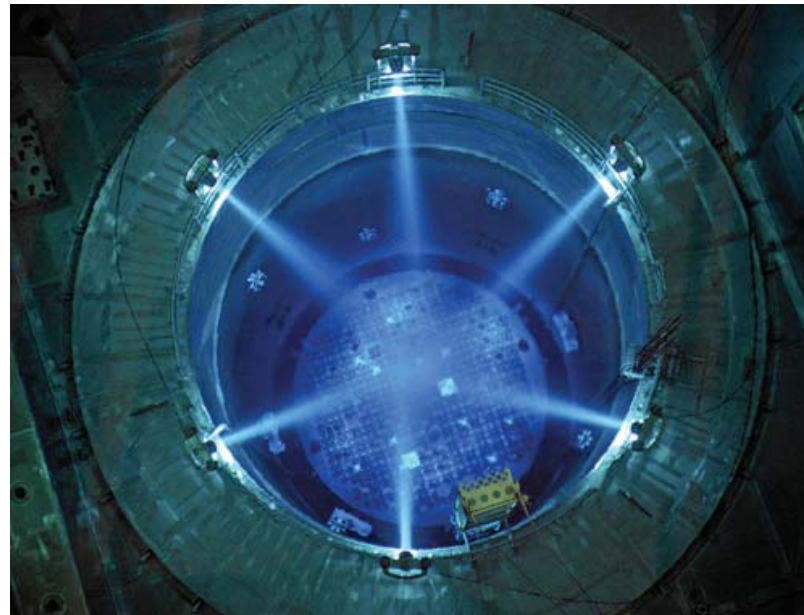
“Isn’t firmware protected against tampering anyway?”

- ... by cryptographic means (checksums, digital signatures etc.) ...
- Well, that’s what you might expect.
- Reality proves otherwise...



So why would somebody want to do that?

- **Blowing up something, some time**
- **Deployment of backdoors (to devices or your network)**



Blowing up something, some time

Siberian pipeline sabotage

From Wikipedia, the free encyclopedia

The **Siberian pipeline sabotage** refers to the alleged 1982 sabotage of the *Soviet Urengoy - Surgut - Chelyabinsk* pipeline, allegedly involving the theft of American technology.

Contents [hide]

- 1 Background
- 2 Hoax Theory
- 3 References
- 4 See also
- 5 External links

Background

The pipeline, as planned, would have utilized plans for a sophisticated computer program for sabotage purposes, even

The CIA was tipped off to the Soviet operation proceeded to deny the sabotage company was anticipated, and, in J

Data Acquisition (SCADA). The pipeline utilized a logic bomb in the program for sabotage purposes.



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

Backdoors

- [PAXSON00]:
- **“A backdoor is a mechanism surreptitiously introduced into a computer system to facilitate unauthorized access to the system.”**



More on this

- This brings up some interesting questions.



- **Is enabled SNMP with public/private a backdoor?**
 - Based on deliberate decision (= “surreptitiously”).
 - Means to provide access.
 - Well, yes, maybe not intended for *unauthorized* access.
 - But used for such in many cases...

Types of backdoors

- **Buffer Overflow vulnerabilities**
- **Hidden configuration options (“allowHiddenAccountLogin=YES”)**
- **Unsecure cryptographic properties**
 - Weak initialization vectors
 - Manipulated S-Boxes (e.g. in AES)
 - Deterministic PRNGs
- **Master password (“lkwppeter”)**
- **Hidden credentials (user/pass)**
- **Port knocking**
- **Data leakage/logging second channel (external system, ...)**
- **Additional access mechanism (SSH, telnet, ...) ← *most common rootkit behavior***



Typical vulnerabilities in supply chain security

- **Lack of standards**
 - ISO 28001 much lesser known than ISO 27001
- **Lack of visibility**
- **Lack of tools for verification**





Architecture details of some popular security appliances



Disclaimer



- **All this stuff is not too well documented. We did our best when assembling the information displayed in the following slides. Still, it might be inaccurate here + there.**

Helpful tools when analysing...

- Hex Editor
- IDA disassembler - supports many chipsets
- Programming manuals for different architectures
- Compression / decompression software
- Cryptography tools
- Universal Chip Reader
- Serial console cable

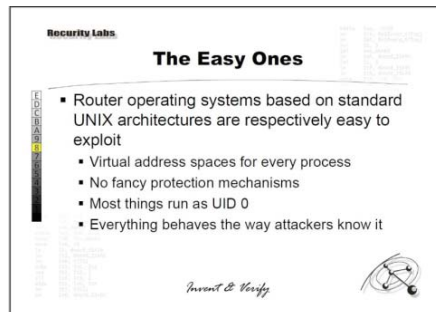
Cisco ASA

- Based on (mostly) standard PC hardware, x86 architecture
- Image is based on Linux kernel and can be extracted, see e.g.[1]
- Presumably the BIOS can be modified/replaced, although this voids the warranty ;-), see [2]
- “Verify” command for verifying the MD5 checksum present [3]
 - ... but does not inhibit firmware execution if checksum fails



Juniper routers

- Routing engine is commodity hardware with Intel CPU, harddrive, flashdrive etc.
- Parts can be exchanged easily
- JunOS based on FreeBSD kernel



- Usually new image released every 90 days
 - One can “predict new image” ;-)
- REs have CF card slot
 - Which, by default, is booted from first



Juniper Netscreen devices

- **ScreenOS proprietary RTOS on PowerPC**
- **Previous research “Netscreen of the Dead” Blackhat 2009**
See http://www.troopers.de/content/e728/e897/e938/TROOPERS10_Netscreen_of_the_Dead_Graeme_Neilson.pdf
- **Weakness in the firmware protection & verification**
- **Developed fully trojaned ScreenOS firmware image with**
 - backdoor
 - custom code execution
 - firmware update prevention



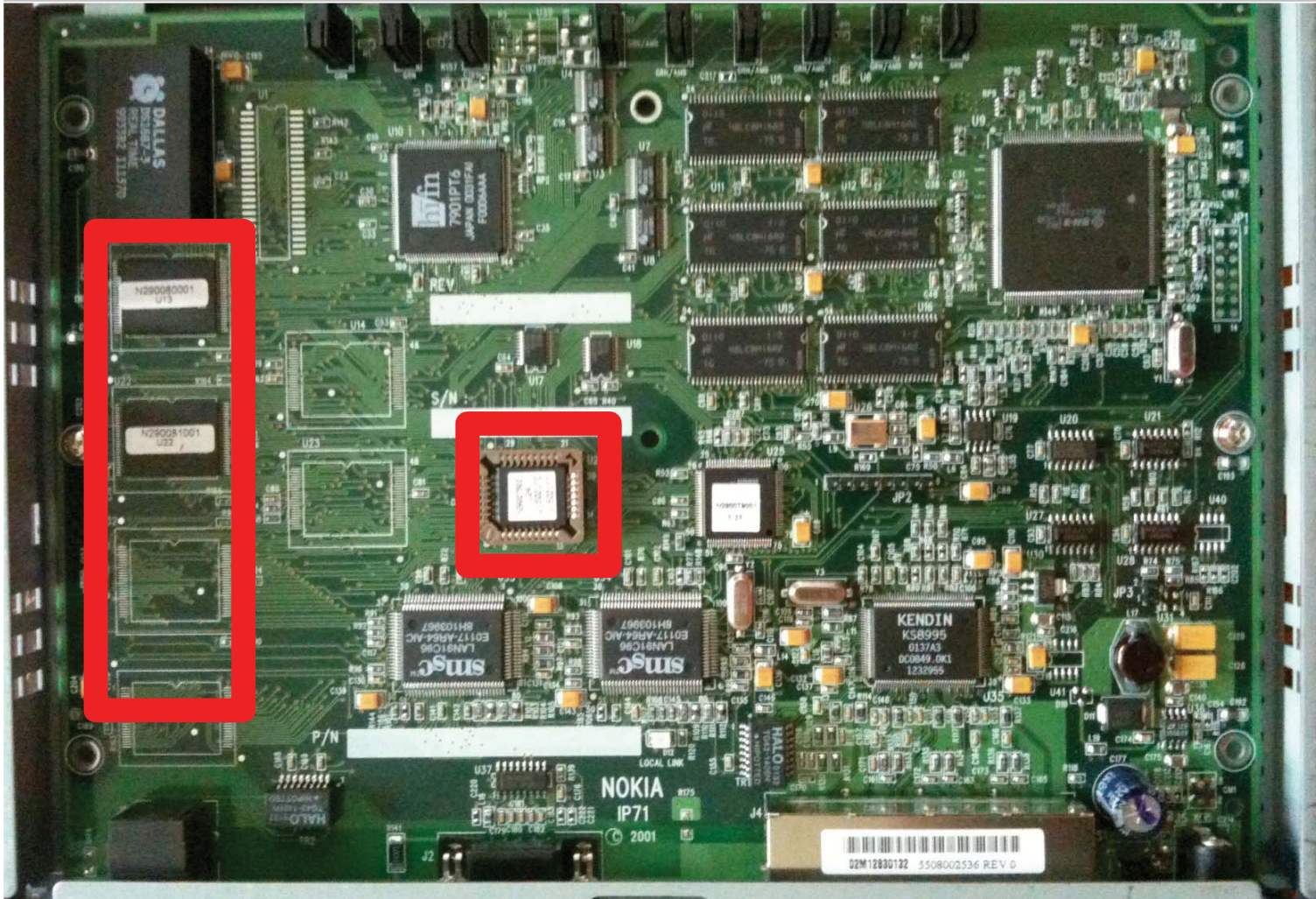
Nokia & Check Point

- Check Point supply Firewall-1/VPN-1 software which can run on top of other operating systems
- Appliances Linux/FreeBSD based

Example Appliance (admittedly an old one, newer behave differently)

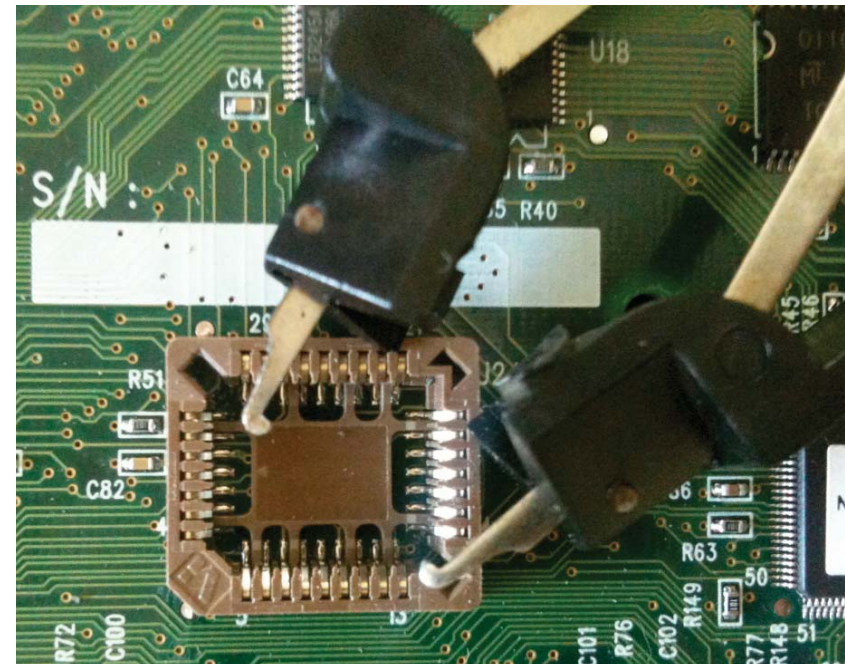
- Nokia IP71 series with SuperH RISC processor
- System is stored in on-board flash with no option to download flash :(
- Restricted shell with a custom menu console application running
- Attack vectors are:
 - break out of app and restricted shell
 - customise or overwrite BIOS to gain control of flash memory

Nokia IP71



Nokia (IP71) BIOS

- Removable BIOS chip running Nokia boot loader
- Remove chip, dump code, reverse engineer, modify, reflash chip
- BIOS rootkit or “BootKit”



Demo : ZomBIOS

- BIOS level control



Fortigate

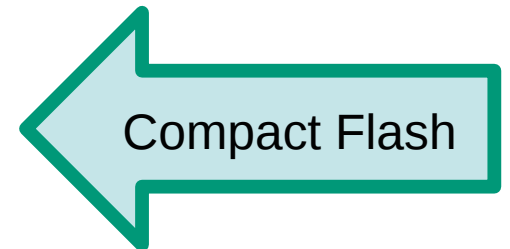
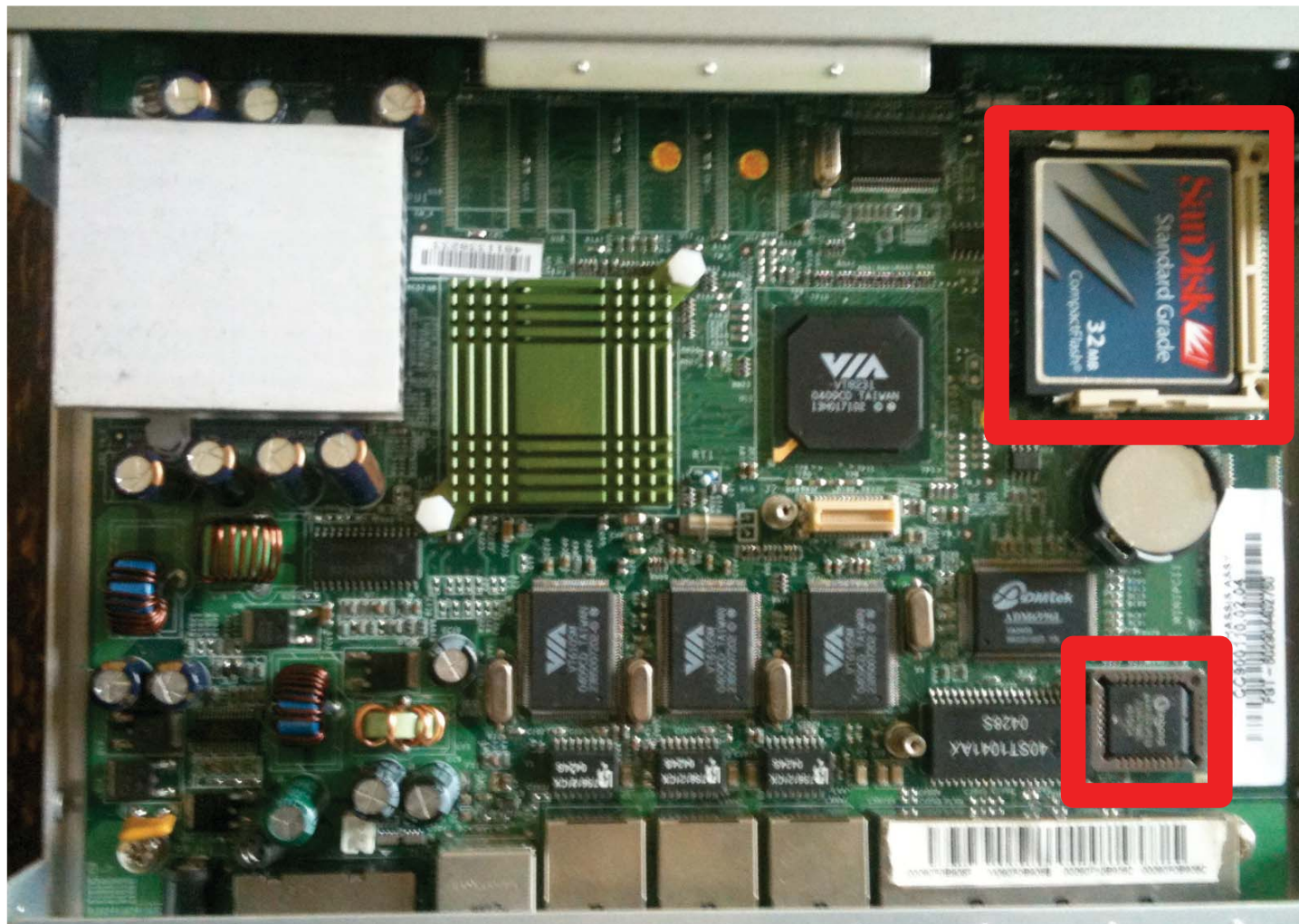
- Fortinet make Fortigate appliances (x86 platform).
- Runs FortiOS - based on Linux.
- Supplied as standard gzip file with certificate and hash appended.
- Decompress gives an encrypted blob of data.
- The encryption used has weaknesses:
 - Watermarks (patterns in the data) looks like a disk image.
 - Location of MBR, kernel, root file system can be seen.
 - This allows known plain text attacks



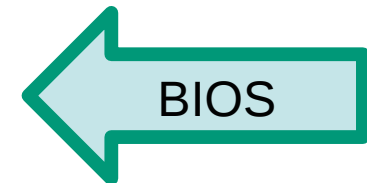
Watermarks

00001f9c	03 2A 64 2B 48 7A 1A 56 11 77 46 25 18 54 33 52 39	. *d+Hz.V.wF%.T3R9
00001fad	73 35 52 12 4A 0B 52 2D 73 09 52 27 73 3D 77 04 2D	s5R.J.R-s.R's=w.-
00001fbe	63 2C 4F 7D 1D 51 16 70 41 22 1F 53 34 55 3E 74 32	c,O}.Q.pA".S4U>t2
00001fcf	55 15 4D 0C 55 2A 74 0E 55 20 74 3A 70 03 2A 64 2B	U.M.U*t.U t:p.*d+
00001fe0	48 7A 1A 56 11 77 46 25 18 54 33 52 39 73 35 52 12	Hz.V.wF%.T3R9s5R.
00001ff1	4A 0B 52 2D 73 09 52 27 73 3D 77 04 2D 63 2C 9C AE	J.R-s.R's=w.-c,...
00002002	CE 82 C5 A3 92 F1 CC 80 E7 86 ED A7 E1 86 C6 9E DF	
00002013	86 F9 A7 DD 86 F3 A7 E9 A3 D0 F9 B7 F8 9B A9 C9 85	
00002024	C2 A4 95 F6 CB 87 E0 81 EA A0 E6 81 C1 99 D8 81 FE	
00002035	A0 DA 81 F4 A0 EE A4 D7 FE B0 FF 9C AE CE 82 C5 A3	
00002046	92 F1 CC 80 E7 86 ED A7 E1 86 C6 9E DF 86 F9 A7 DD	
00002057	86 F3 A7 E9 A3 D0 F9 B7 F8 9B A9 C9 85 C2 A4 95 F6	
00002068	CB 87 E0 81 EA A0 E6 81 C1 99 D8 81 FE A0 DA 81 F4	
00002079	A0 EE A4 D7 FE B0 FF 9C AE CE 82 C5 A3 92 F1 CC 80	
0000208a	E7 86 ED A7 E1 86 C6 9E DF 86 F9 A7 DD 86 F3 A7 E9	
0000209b	A3 D0 F9 B7 F8 9B A9 C9 85 C2 A4 95 F6 CB 87 E0 81	
000020ac	EA A0 E6 81 C1 99 D8 81 FE A0 DA 81 F4 A0 EE A4 D7	

Fortigate



Compact Flash



BIOS

Fortigate

- Fortigate will load firmware even if it has no certificate, no hash and is unencrypted.
- The verification is of filenames contained within the gzips
 - Start of MBR must contain a filename matching a device & version ID
 - Kernel must be called “fortikernel.out”

00000000	1F 8B 08 08 A1 7F 90 4B 00 03 46 47 54 2D 36 30 2D	K..FGT-60-
00000011	33 2E 30 2D 2D 62 75 69 6C 64 30 36 32 2D 30 38 30	3.0--build062-080
00000022	33 31 37 00 EC D8 3F 6C 94 65 00 C7 F1 E7 8A 2D 24	317...?l.e.....-\$
00000033	2A 88 C8 3F 15 DB 9D 1C 39 24 01 07 31 68 1A 1C 6A	*..?....9\$.!h..j
00000044	08 89 12 13 26 62 4C 94 84 95 BF 05 7A 85 45 E3 D2	&bL.....z.E..
00000055	C1 C1 C1 41 13 13 13 06 16 76 13 16 47 17 12 C1 AA	...A.....v..G....
00000066	28 0A 02 62 C1 C5 95 FA 7B EF DA B4 20 85 90 D8 BB	(..b.....{... ..
00000077	2A 9F 4F F2 BD F4 BD F7 B9 3E EF DD 7B CF 9B BC 57	*.O.....>..{...W
00000088	4A A5 D6 7A 9C 2C A7 76 6D 7F FD AD FA E6 46 7D D3	J..z.,.vm.....F}.
00000099	86 46 BD FE CE FE BD FB DE 6D 6C 7E B1 DE 78 A9 B1	.F.....ml~...x..
000000aa	69 E3 96 B2 F3 ED C1 AD 65 9E 55 47 D2 7C 65 BE 67	i.....e.UG. e.g
000000bb	F9 BF 68 A6 93 69 34 9F D8 B6 4F DB CF 55 DB 67 C7	..h..i4...O..U.g.
000000cc	67 B6 EF 67 D7 A9 F9 3B 36 00 00 00 00 00 00 00 00	g..g....;6.....
000000dd	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Fortigate

- Can modify existing system or replace kernel and file system.
- Automated firmware upgrade on reboot from USB stick is a feature.
- Boot into custom linux and dd memory
 - to Compact Flash data is encrypted
 - to serial console there is no encryption



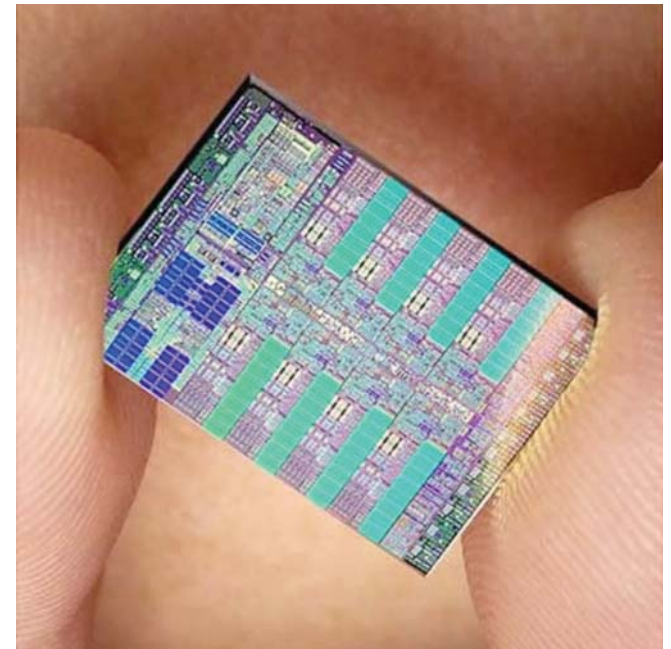
Demo : ZombiOS

- Operating system level control



As a point of comparison...

- **Playstation 3 NOT a firewall, NOT protecting your data, designed to protect Sony's intellectual property and investment in game development.**
- **IBM Cell architecture – chip designed with security at the hardware level**
 - Secure processing vault
 - Runtime secure boot
 - Hardware root of secrecy
- **Signed code necessary at multiple levels: boot time, hypervisor, gameOS, game.**



As a point of comparison...

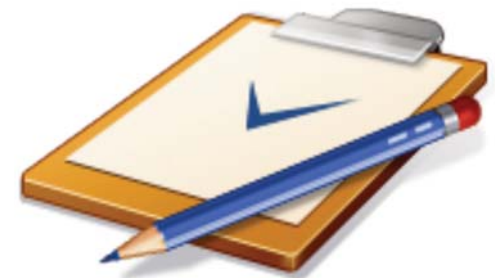
- Full hard disk encryption
 - Recently a flaw in the USB stack allows running unsigned code BUT this is not persistent across reboots because of the signed boot code and signed hypervisor.
- A gaming console is a more secure platform than most security appliances!



PlayStation 3 cluster

Some (kind-of-checklist) questions

- **What are the motivations/incentives of the involved parties?**
- **Do you think they're capable (of providing a secure supply chain)?**
- **What do you know about your organization's (security device) supply chain?**



Conclusions

- **(Most) security appliances are not designed to withstand “unauthorized physical access”.**
- **The supply chain may not be as secure as you expect.**
 - **This might lead to “interesting scenarios” ;-)**
- **Think about it!**



There's never enough time...

THANK YOU...

...for yours!



TROOPERS II, 03/28-04/01/2011 Heidelberg, Germany



Subscribe to the newsletter at www.troopers.de,
follow us on Twitter [@WEareTROOPERS](https://twitter.com/WEareTROOPERS)
and meet with experts from around the world at TROOPERS11 at Heidelberg, Germany.

References

■ Specific to Cisco ASA

- [1] “Simulation [of] Cisco ASA with QEMU and GNS3”:
<http://kizwan.blogspot.com/2010/01/simulatio-cisco-asa-with-qemu-and-gns3.html>
- [2] Cisco ASA 5580 Adaptive Security Appliance Hardware Installation Guide:
<http://www.cisco.com/en/US/docs/security/asa/hw/maintenance/5580guide/procedures.html>
- [3] Cisco ASA “verify” command
<http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/uz.html#wp1569565>

■ Specific to Cisco routers

- <http://www.cisco.com/web/about/security/intelligence/iosimage.html>

