SAND2015-0526PE

Exceptional service in the national interest

Sandia National Laboratories

Security in the Connected World

Chris Jenkins

R&D S&E Cybersecurity

Senior Member of Technical Staff

February 10, 2015

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Executive Summary

- Goal #1: Provide a clear, concise of security related challenges and problems. This presentation does not represent an exhaustive list, but it does provide insight on cybersecurity.

- Goal #2: Motivate students to consider pursuing the cybersecurity field and understand where computer architecture fits into the larger picture.

Agenda

Part One

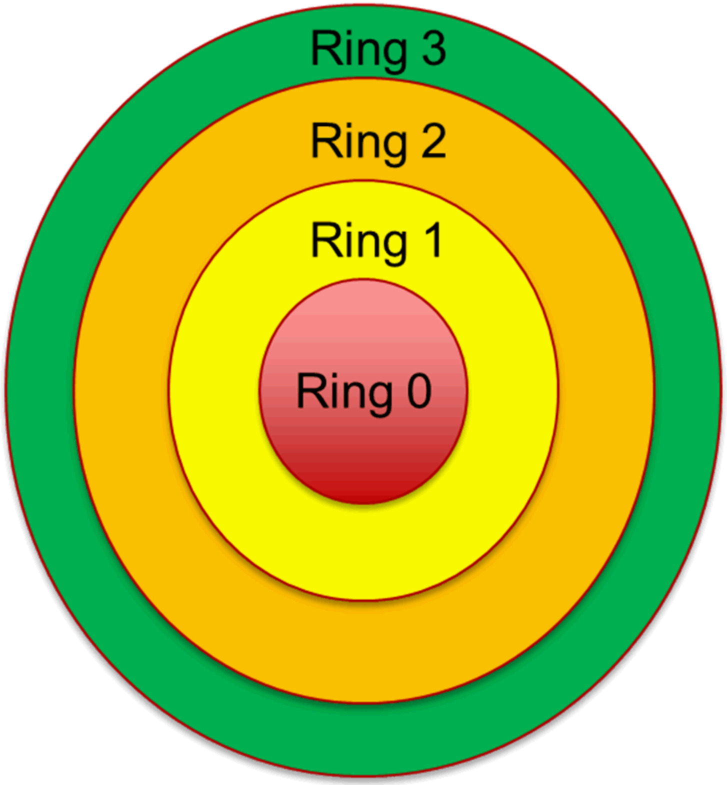
- Background
  - Modern CPUs
  - Operating Systems
  - Hypervisors
  - Trusted Computing
- Problems and Challenges
  - Consumer / Enterprise
  - Industrial / IoT

Part Two

- Examples
  - Consumer Router
  - Stuxnet
- Solutions
  - Host-based
  - Network-based
  - Processes
- Conclusion

Background - Modern CPU Rings

Rings

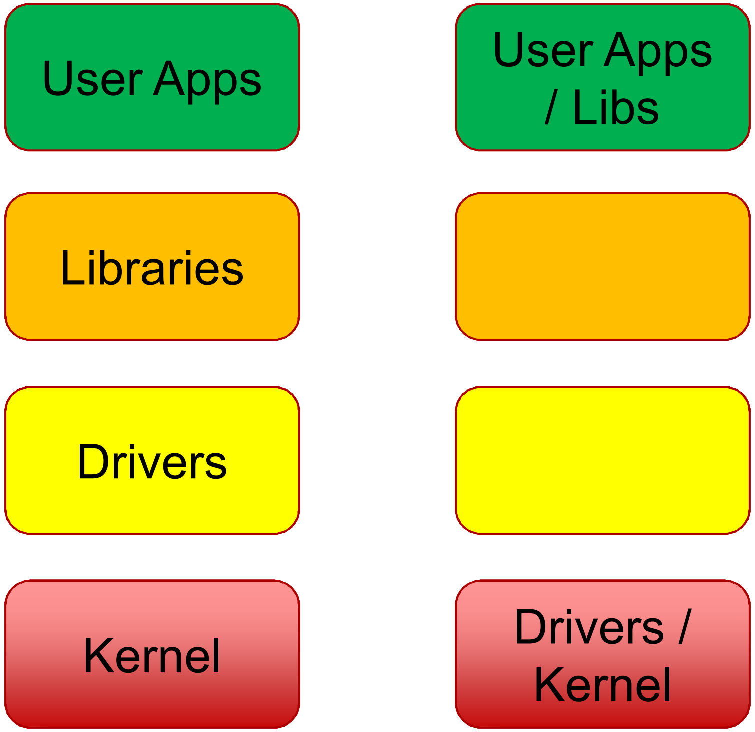


Concept

- Lower number = higher privilege
- Higher privilege means:
  - More instructions
  - Set memory access perms
  - Access system level registers
- How to design a system?

Background - Computer Design

Rings and Code

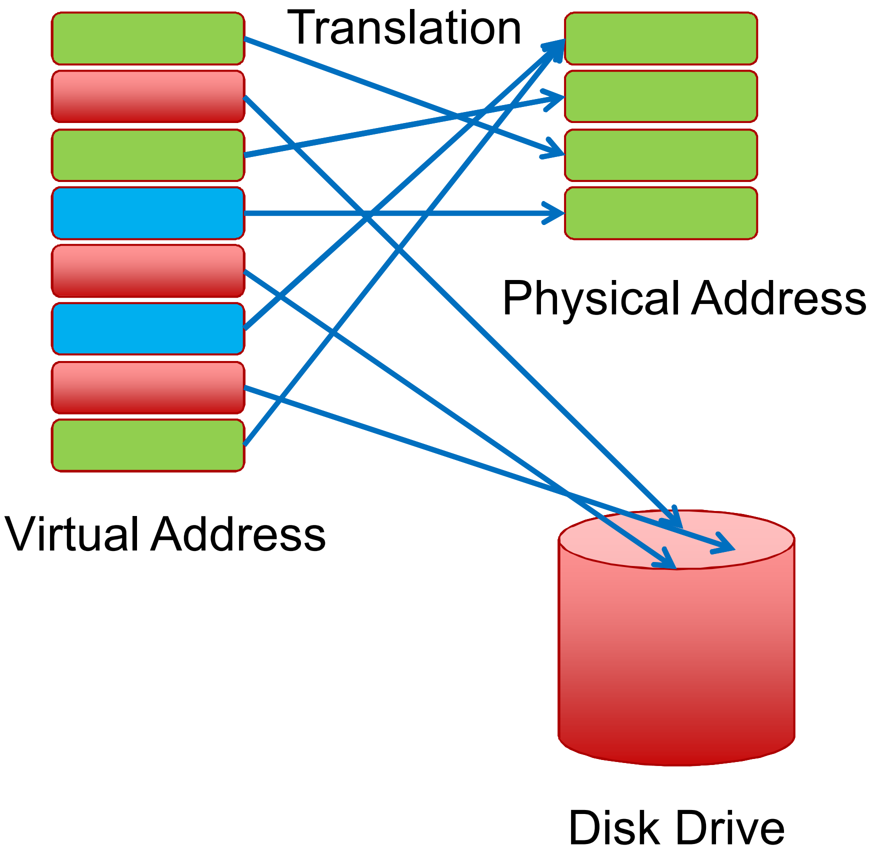


Concept

- Divide code into two levels
- Portable across architectures
- Userspace
  - Application
  - OS libraries
  - Issues system calls
- Operating System
  - Handles system calls
  - Devices / Peripherals
  - Memory management

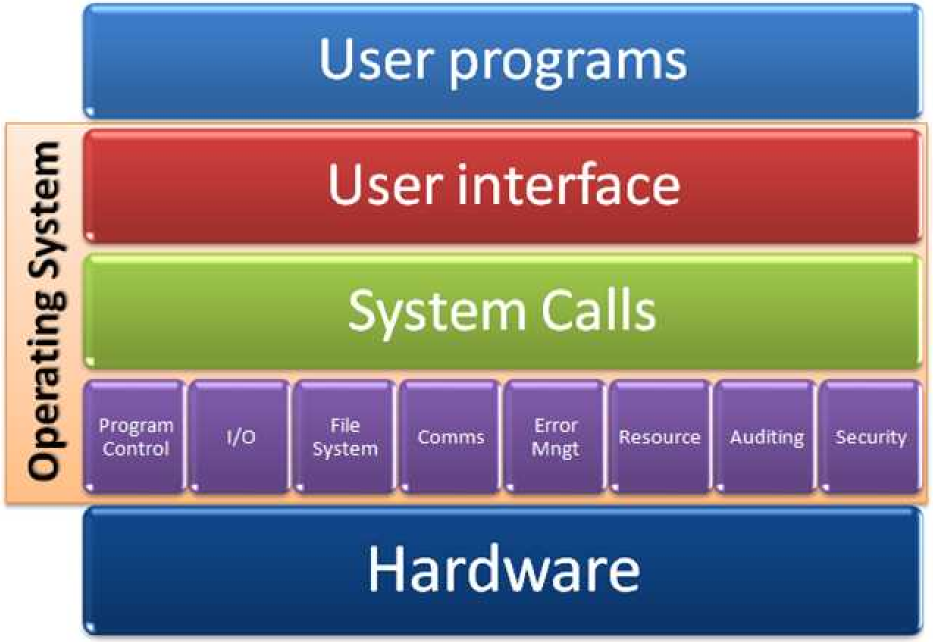
Background - Virtual Memory

- CPU address is not real
- Page table translates to “real” memory address
- TLB stores recent translations
- Privilege is needed to write page table / TLB
- Page out to disk if not enough “real” memory



Background – Operating Systems

- User programs use API
- Generic interfaces
- Separates programs into address spaces
- Implements system calls
- Manages underlying system resources

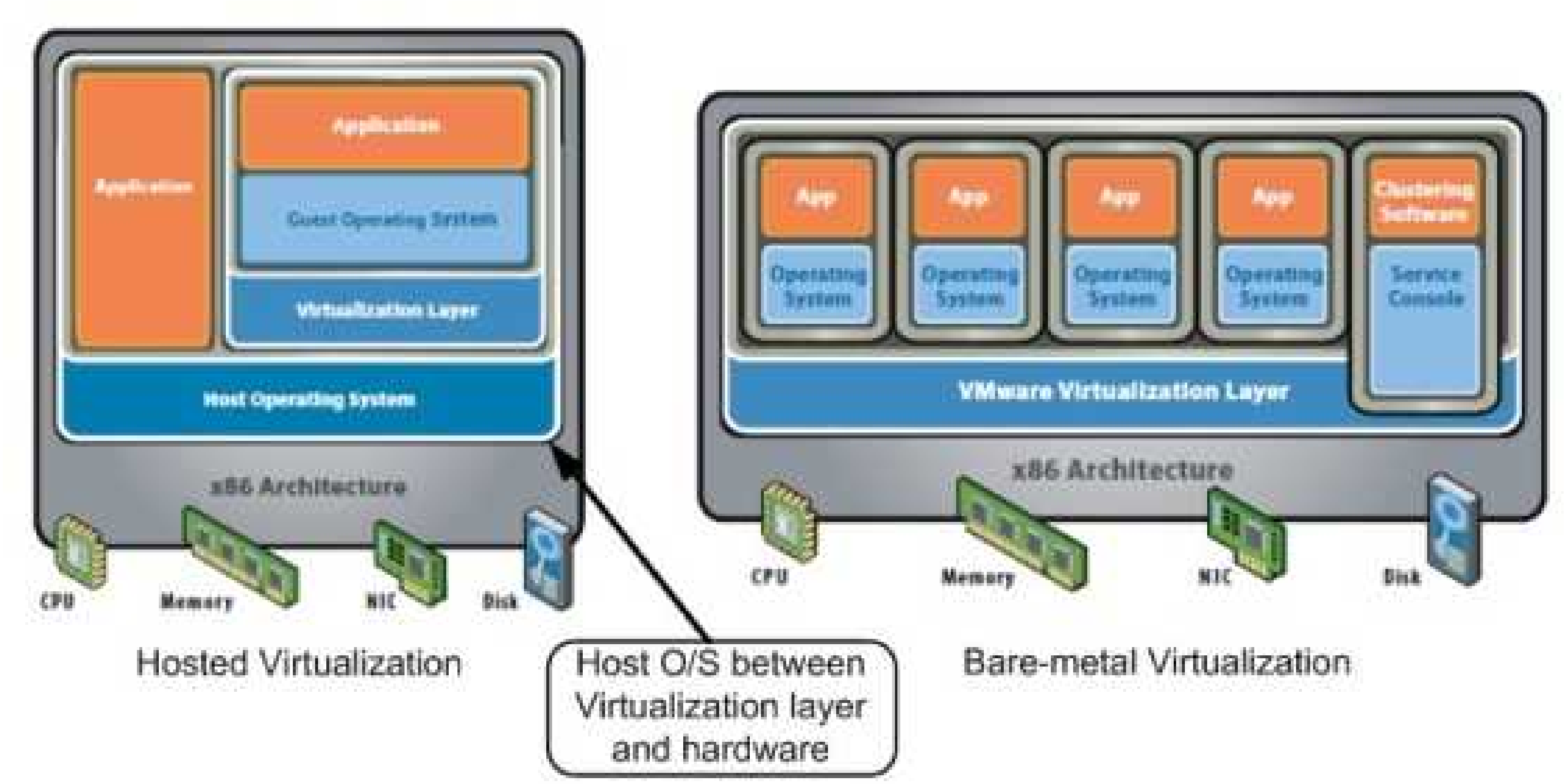


http://i.stack.imgur.com/swJir.png

Background – Hypervisors

Type 2

Type 1



Hosted Virtualization

Bare-metal Virtualization

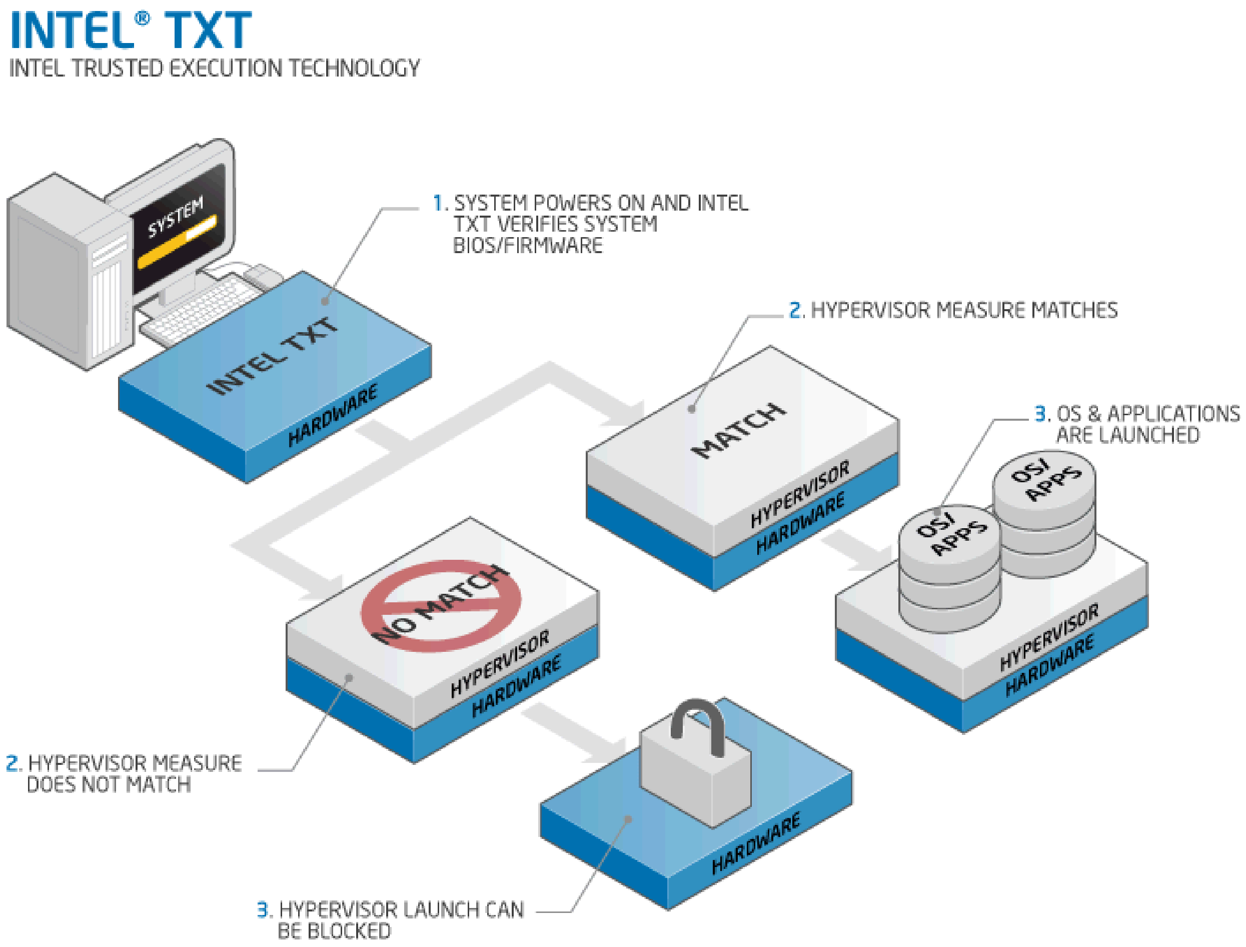
Host O/S between Virtualization layer and hardware

http://cdn.ttgtmedia.com/ITKE/uploads/blogs.dir/28/files/2009/10/whatisvirt12.jpg

Background – Trusted Computing

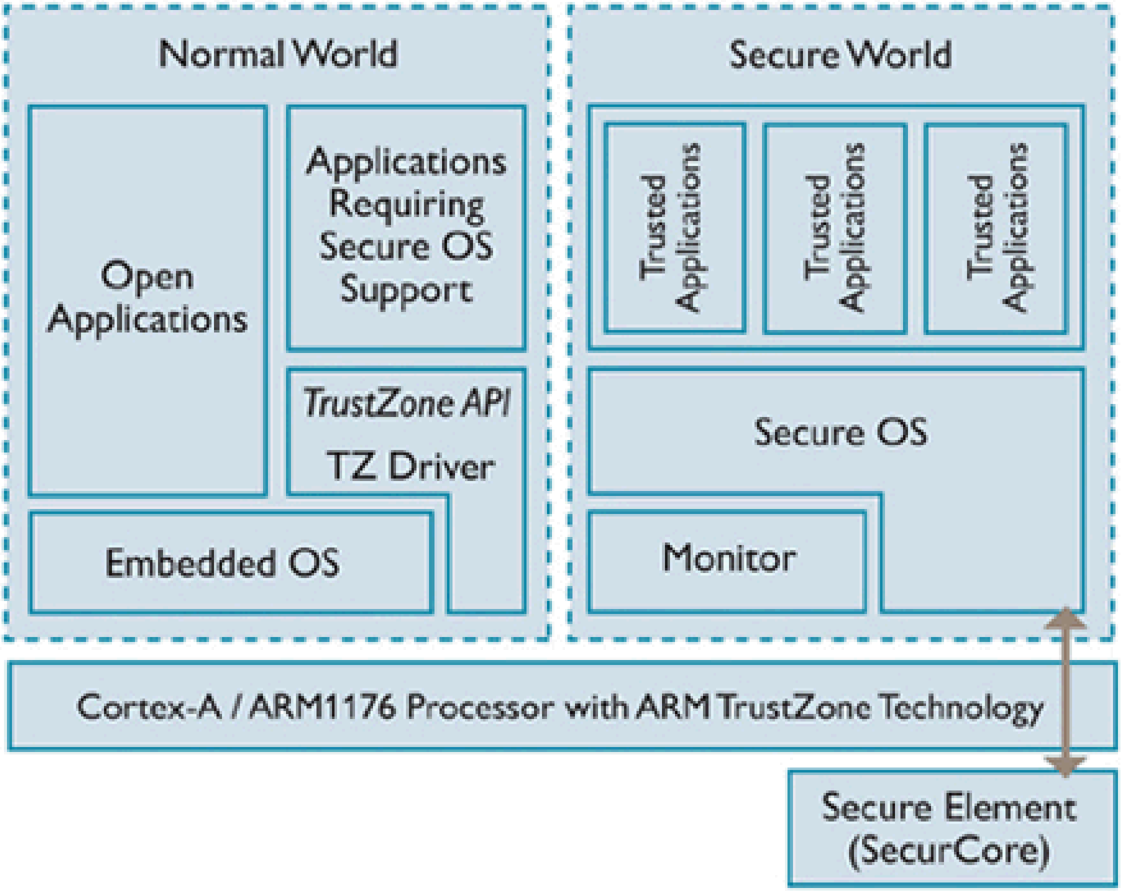
- Behave in expected ways
- Enforced by a combination of software and hardware
- Trusted computing components
  - Secure boot
  - Trusted boot
  - Linux IMA
  - TPM
  - Etc.
- Today
  - Intel TXT
  - ARM Trustzone
  - Freescale QorIQ

Background – Intel TXT


INTEL® TXT
INTEL TRUSTED EXECUTION TECHNOLOGY
SYSTEM
INTEL TXT
HARDWARE
1. SYSTEM POWERS ON AND INTEL TXT VERIFIES SYSTEM BIOS/FIRMWARE
2. HYPERVISOR MEASURE MATCHES
MATCH
HYPERVISOR
HARDWARE
3. OS & APPLICATIONS ARE LAUNCHED
OS/ APPS
OS/ APPS
HYPERVISOR
HARDWARE
NO MATCH
HYPERVISOR
HARDWARE
2. HYPERVISOR MEASURE DOES NOT MATCH
HARDWARE
3. HYPERVISOR LAUNCH CAN BE BLOCKED

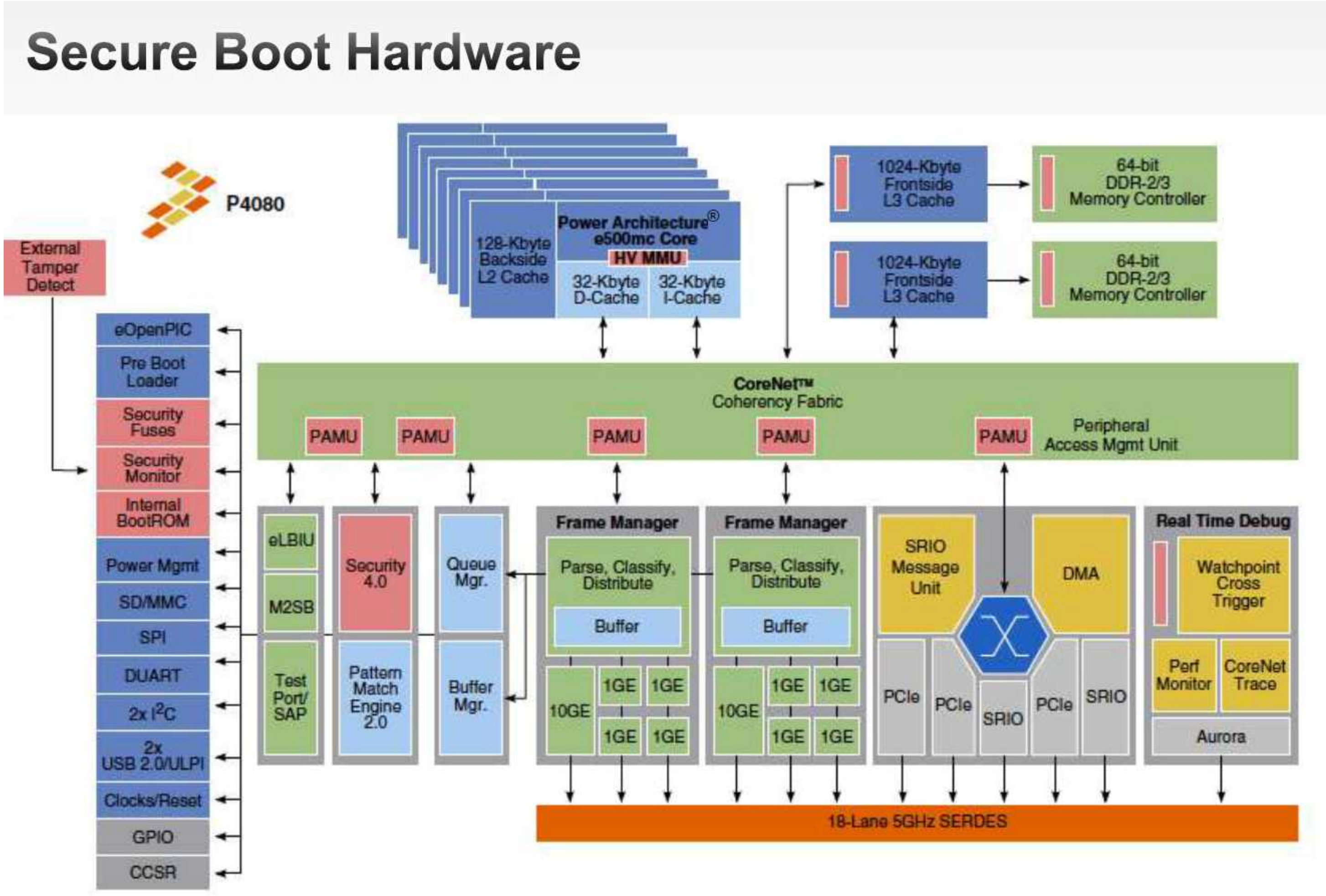
https://communities.intel.com/servlet/JiveServlet/showImage/38-17503-239158/txt-image.gif

Background – ARM Trustzone



http://www.arm.com/images/TrustZone_Software_Architecture.jpg

Background – Freescale QorIQ



Secure Boot on QorIQ P4080. Freescale, June 2012.

Consumer / Enterprise

Consumer

- Desktop
- Laptop
- Tablet
- Phone
- Store personal data
  - Credit cards
  - Passwords
  - Photos
  - Social Media

Enterprise

- Cloud Computing
- Data Center
- Stores IP
  - Financial
  - Trade Secrets
  - Implementations
  - Weaknesses
  - Financial Records
  - Services

Industrial Internet / IoT

Industrial Internet

- Coined by GE
- Integration of
  - Complex machinery
  - Networked sensors
  - Machine learning
  - Big data
  - IoT
  - M2M Communication
- Injest, analyze, adjust

Internet of Things

- Smart Thermostat
- Wi-Fi washer/dryer
- Heart monitoring implants
- Biochip transponders on farm animals
- Automobiles with built-in sensors
- Field operation devices that assist fire-fighters in S&R

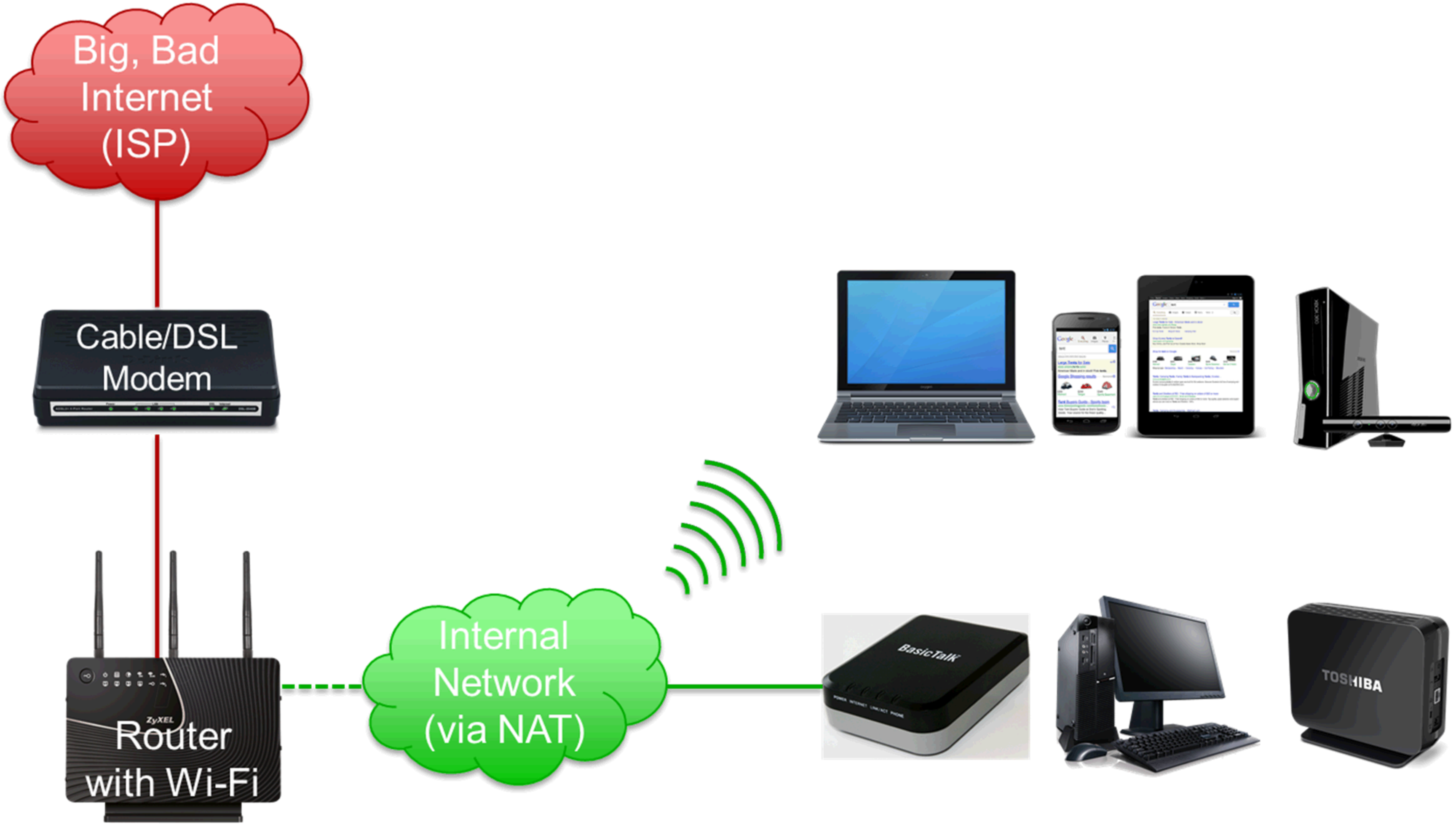
Interfaces

- Software
  - BIOS
  - UEFI
  - ACPI
  - SMM
  - OS
  - Application
- Hardware
  - CPU / GPU
  - DSP / FPGs
  - APIC / BMC / AMT
  - Hard drives / memory / network card / graphics / peripherals

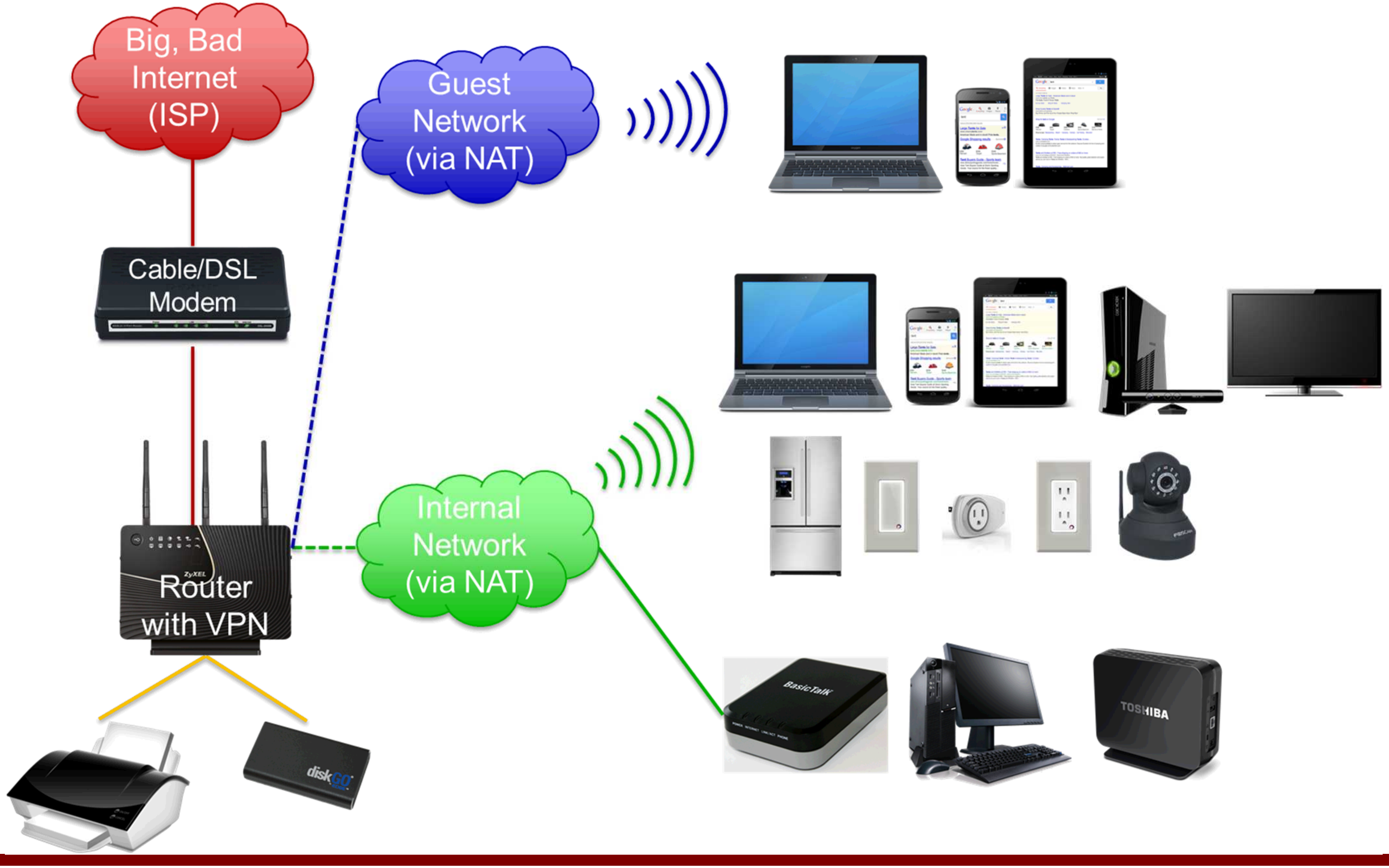
Applicability Discussion

- How many of you have consumer-grade
  - Cable/DSL modems, whether you rent or own?
  - Wi-Fi routers?
  - IP cameras?
  - NASes?
- Knowingly or otherwise, do you trust these devices?
- Do you rely on your Wi-Fi router to firewall you from the Internet?
- How often do you update the firmware on your devices?

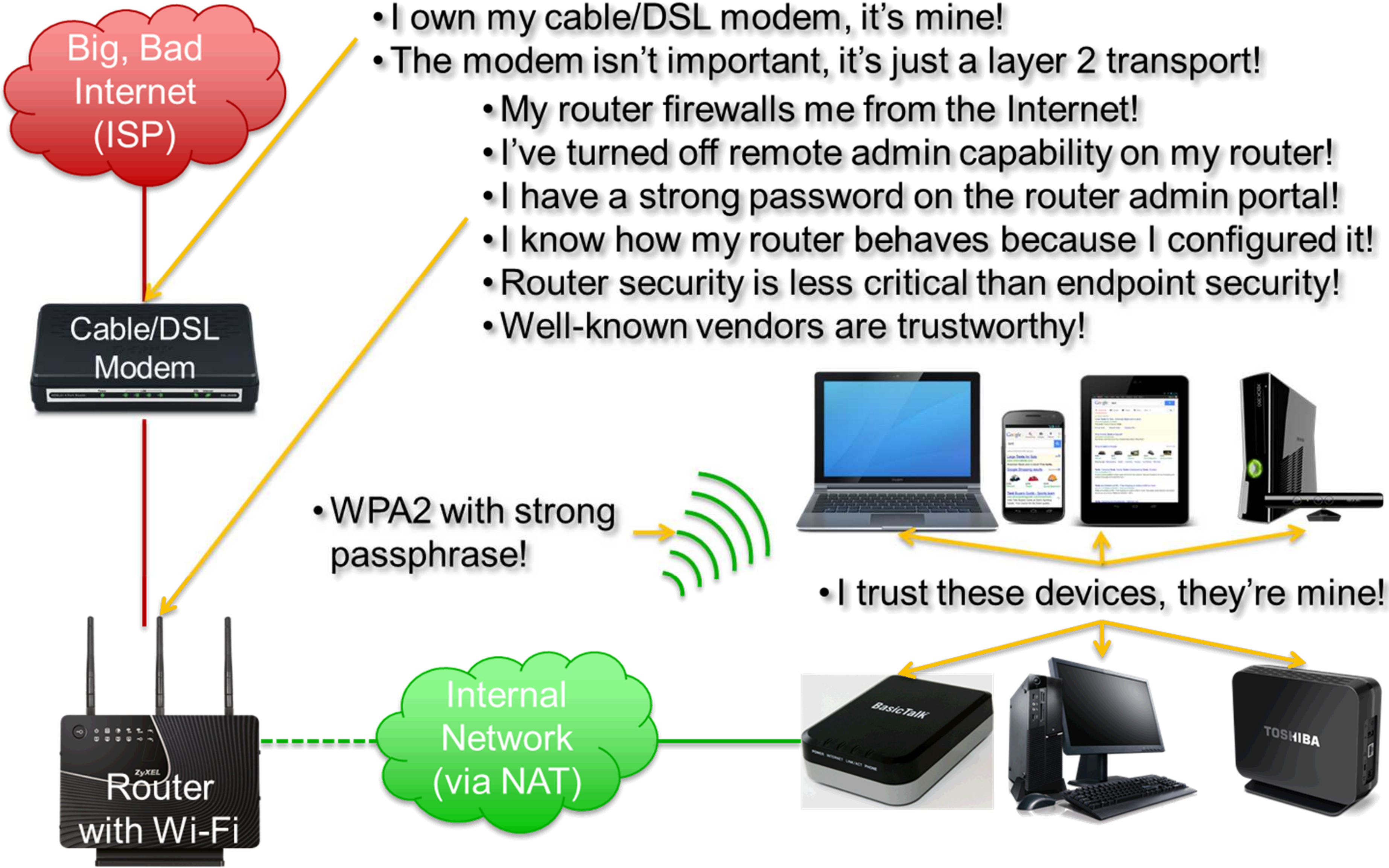
The Typical Consumer Setup



An Advanced Consumer Setup

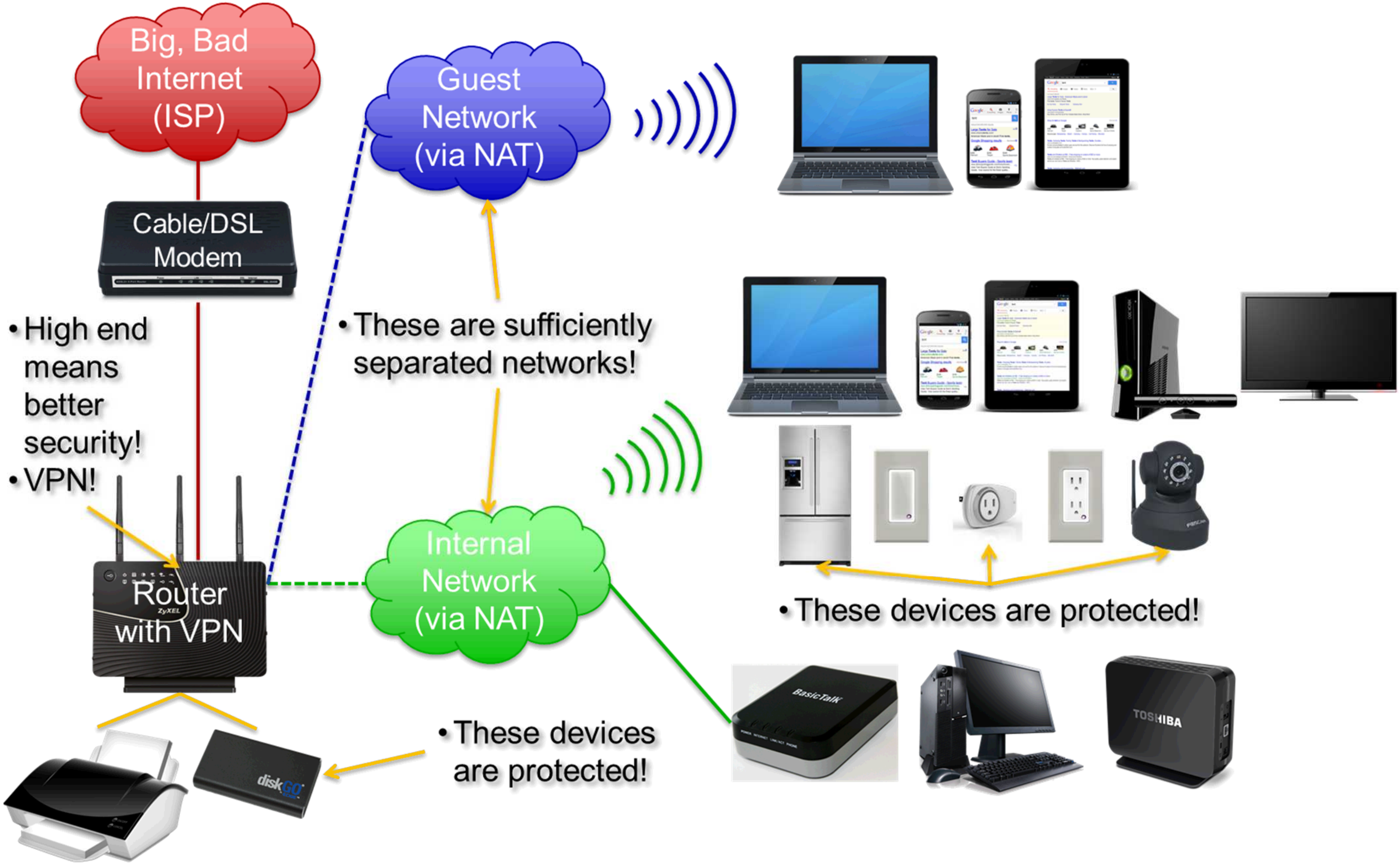


The Security Mirage



- I own my cable/DSL modem, it's mine!
- The modem isn't important, it's just a layer 2 transport!
  - My router firewalls me from the Internet!
  - I've turned off remote admin capability on my router!
  - I have a strong password on the router admin portal!
  - I know how my router behaves because I configured it!
  - Router security is less critical than endpoint security!
  - Well-known vendors are trustworthy!
- WPA2 with strong passphrase!
- I trust these devices, they're mine!

The Security Mirage



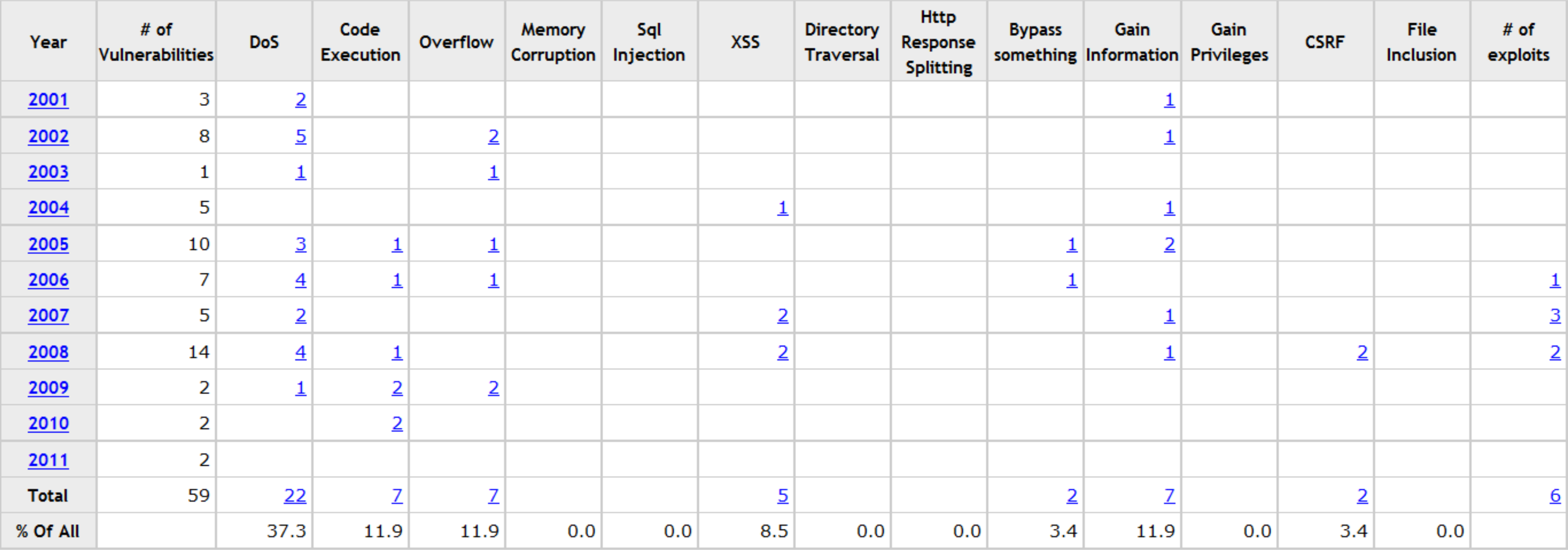
- High end means better security!
- VPN!

- These are sufficiently separated networks!

- These devices are protected!

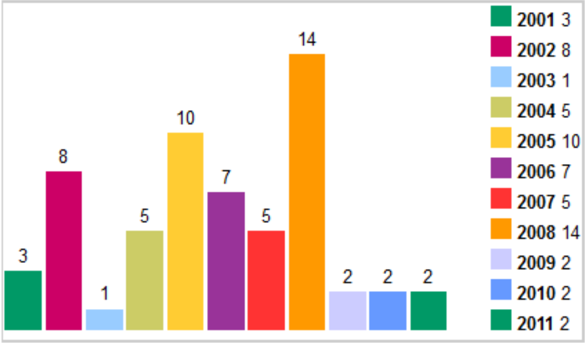
- These devices are protected!

(In)Security, In General

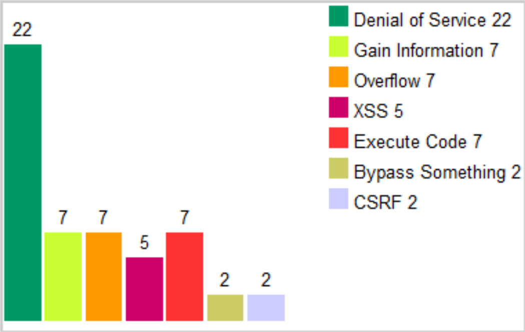


Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	3	2									1				
2002	8	5		2							1				
2003	1	1		1											
2004	5						1				1				
2005	10	3	1	1						1	2				
2006	7	4	1	1						1					1
2007	5	2					2				1				3
2008	14	4	1				2				1		2		2
2009	2	1	2	2											
2010	2		2												
2011	2														
Total	59	22	7	7			5			2	7		2		6
% Of All		37.3	11.9	11.9	0.0	0.0	8.5	0.0	0.0	3.4	11.9	0.0	3.4	0.0	

Vulnerabilities By Year



Vulnerabilities By Type



CVE Details for Linksys

As of July 2014

http://www.cvedetails.com/vendor/833/Linksys.html

Some Specific Security Issues

- DHCP on Linksys BEFSR11, BEFSR41, BEFSR81, and BEFSRU31 Cable/DSL Routers, firmware version 1.45.7, does not properly clear previously used buffer contents in a BOOTP reply packet, which allows remote attackers to obtain sensitive information.
- *This is analogous to the Heartbleed vulnerability, except it leaks kernel memory, not process memory.*

Some Specific Security Issues

- SNMP service in Atmel 802.11b VNET-B Access Point 1.3 and earlier, as used in Netgear ME102 and Linksys WAP11, accepts arbitrary community strings with requested MIB modifications, which allows remote attackers to obtain sensitive information such as WEP keys, cause a denial of service, or gain access to the network.
- *This is like accepting any password, not just a valid one.*

Some Specific Security Issues

- Linksys EtherFast BEFSR41 Cable/DSL routers running firmware before 1.39.3 Beta allows a remote attacker to view administration and user passwords by connecting to the router and viewing the HTML source for (1) index.htm and (2) Password.htm.
- *This is like giving the password to an attacker, then asking them for it to login.*

Some Specific Security Issues

- VPN Server module in Linksys EtherFast BEFVP41 Cable/DSL VPN Router before 1.40.1 reduces the key lengths for keys that are supplied via manual key entry, which makes it easier for attackers to crack the keys.
- *This is like accepting a 20 character password, but only checking the first 8 characters at login.*

Some Specific Security Issues

- `$ strings GS105PE_V1.2.0.5.bin | grep -i passw`
- `$ strings GS105PE_V1.2.0.5.bin | grep -i debug`
- In the Netgear ProSafe GS105PE firmware v1.2.0.5 and earlier, there is a built-in debug username ("ntgruser") and password ("debugpassword"); turns out it cannot be disabled.

Insecurity, By Design

- Wi-Fi Protected Setup (WPS)
  - An 8- to 63-character WPA/WPA2 passphrase is reduced to an 8-digit number
  - The 8-digit number is actually reduced down to two 4-digit numbers
  - The second 4-digit number is reduced to a 3-digit number, due to a checksum digit.
  - Any passphrase falls in 12 hours or less
  - Most routers won’t let you turn WPS off, even if they claim they do
- Home Network Administration Protocol (HNAP)
  - SOAP-based
  - Common HTTP/web service problems haunt HNAP in about the same way as they do HTTP-based admin portals
- Universal Plug and Play (UPnP)
  - Unauthenticated
  - Multicast
  - Sometimes listens on the Internet-side of the router
  - Most routers lie about or don’t allow turning UPnP off

Some Root Causes

- Why all these problems?
  - The bar is set low: security stinks, in general
  - With embedded systems, security smells particularly foul
  - There is little incentive to fix identified problems
  - You get what you pay for: low-cost mean low(er) quality
  - There is little investment in engineering and development
  - Vendors tend to just hastily glue together third-party hardware and software to build “their” consumer-grade products
  - Vendors don’t assign their “A game” to developing these products
  - There has not been, and likely never will be, consumer outcry

Introduction

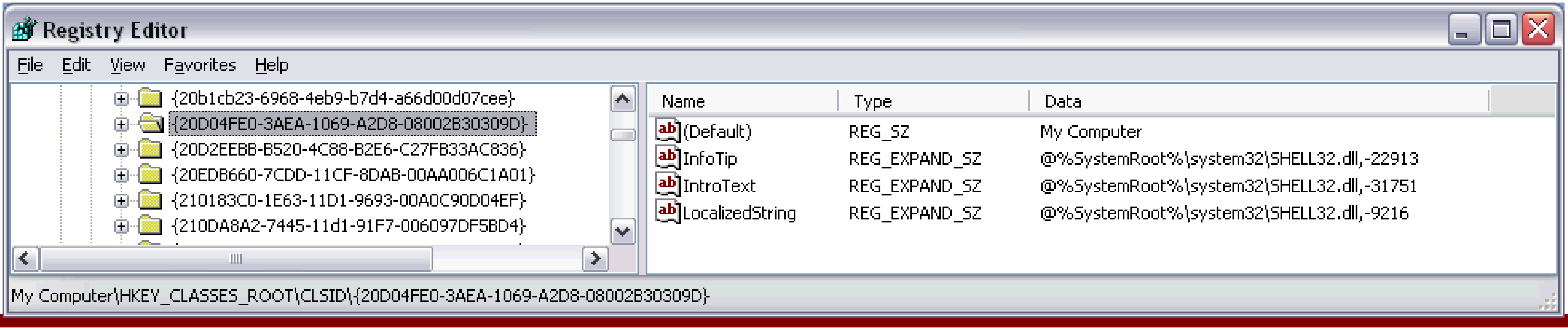
- What is Stuxnet?
  - Malware that targets Siemens Control Systems
- Why is it getting so much attention?
  - Media frenzy over possible nuclear connection
  - Targets control systems (SCADA)
  - Drivers signed with stolen certificates
  - Targeted attack, but operates as a worm
  - Multiple 0-day exploits
  - All in one malware
- Infection Statistics
  - Over 100,000 computers
  - Over 40,000 organizations
  - ~15 of these are SCADA related

Why is it interesting (technical perspective)?

- The total attack required multiple skillsets
  - In-depth Siemens control system knowledge (i.e., experienced engineer)
  - Process Control expert that understands the target process
  - Skilled Windows malware author
    - Quality control
    - Multiple zero-days
    - Knowledge of how to exploit them
- It burned multiple “magic beans/golden tickets” all at once
  - 2 certificates – not trivial to obtain
  - Essentially 4 zero-days - one alone is the basis for a successful attack
    - Why give up four future attacks for this one?
- It is large
- It is self-limiting
  - Only 3 infections per thumb-drive
  - Only propagates the malware if “local” infection is less than 21 days old

LNK Vulnerability

- Stuxnet exploits a feature of Windows “link” files that allows icons to be displayed
  - Poorly designed feature
  - Link file requests system to run any dll
  - Should have been limited to “display-control-panel” dlls
- Only requires that the icon is rendered by Explorer
  - If the icon is visible on the screen, infection has begun
  - No clicking is required
- Points to My Computer -> Control Panel -> Runs DLL
  - Real purpose was for the DLL to return images to display as Control Panel icons
  - Uses CLSID found in registry:



{20b1cb23-6968-4eb9-b7d4-a66d00d07cee}
{20D04FE0-3AEA-1069-A2D8-08002B30309D}
{20D2EEBB-B520-4C88-B2E6-C27FB33AC836}
{20EDB660-7CDD-11CF-8DAB-00AA006C1A01}
{210183C0-1E63-11D1-9693-00A0C90D04EF}
{210DA8A2-7445-11d1-91F7-006097DF5BD4}

Name	Type	Data
(Default)	REG_SZ	My Computer
InfoTip	REG_EXPAND_SZ	@%SystemRoot%\system32\SHELL32.dll,-22913
IntroText	REG_EXPAND_SZ	@%SystemRoot%\system32\SHELL32.dll,-31751
LocalizedString	REG_EXPAND_SZ	@%SystemRoot%\system32\SHELL32.dll,-9216

My Computer\HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}

Other Infection Vectors

- Print Spooler
  - Allows for guests or more privileged users to “print” files onto other computers
  - Schedules that file to run– infects target computer
- MS10-073 – Keyboard Layout, Win32k.sys
  - Elevation of privileges by loading a specific keyboard layout, used against XP
- N/A EoP – Task Scheduler
  - Elevation of privileges by a crc32 collision on a writable file, used against newer Windows versions
- MS08-067 – Server Service
  - Same vulnerability used by Conficker
  - Schedules that file to run– infects target computer
- WinCC Database
  - Use of hard coded password allows access
  - Allows for infection of database server
- Step 7 Project Files
  - Stores a malicious DLL, which appears to get loaded by Siemens' software

Communication

- Command and Control Server Communication
  - Over HTTP
    - www.mypremierfutbol.com, www.todaysfutbol.com
  - XOR encoded
  - Sends:
    - OS version, service pack version, products installed, name, domain name
  - Does not seem to be the main focus
  - Can survive without it
  - Does not appear to exfiltrate proprietary information
- P2P with other infected hosts
  - RPC – Remote Procedure Calls
  - Can update to newest version
  - Allows for update w/o direct internet connection to C&C Server

Control Systems Information

- Typically older Operating Systems
  - Turn around on applying Microsoft patches can be very slow
    - Or not at all
  - Fastest vendor response is two weeks, uncommon
- May or may not be internet connected
  - Which is why Stuxnet needed so many infection vectors
- Utilize PLCs
  - Programmable Logic Controllers
  - Typically programmed from Windows stations
- In relation to Stuxnet
  - Targeted Siemens' software/PLCs

PLC Information

- What is a PLC?
  - A Programmable Logic Controller is used to have some autonomous behavior in a controlled process.
- Sections:
  - Data Blocks (DB) - for program specific data
  - System Data Blocks (SDB) - for configuration data
  - Organization Blocks (OB) - for entry points of programs, executed automatically by the CPU of the PLC
  - Function Blocks (FC) - are standard code blocks

Control System Interaction

- Assumed end goal
  - Malicious modification to PLC code
- Hooks Siemens Control Software
  - Hide its modifications to PLC code
  - Prevent operator from overwriting modifications to PLC code
  - Being called “PLC Rootkit” in media
    - Not technically correct
- Target PLCs
  - 6ES7-417 – appears to be unused
  - 6ES7-315-2

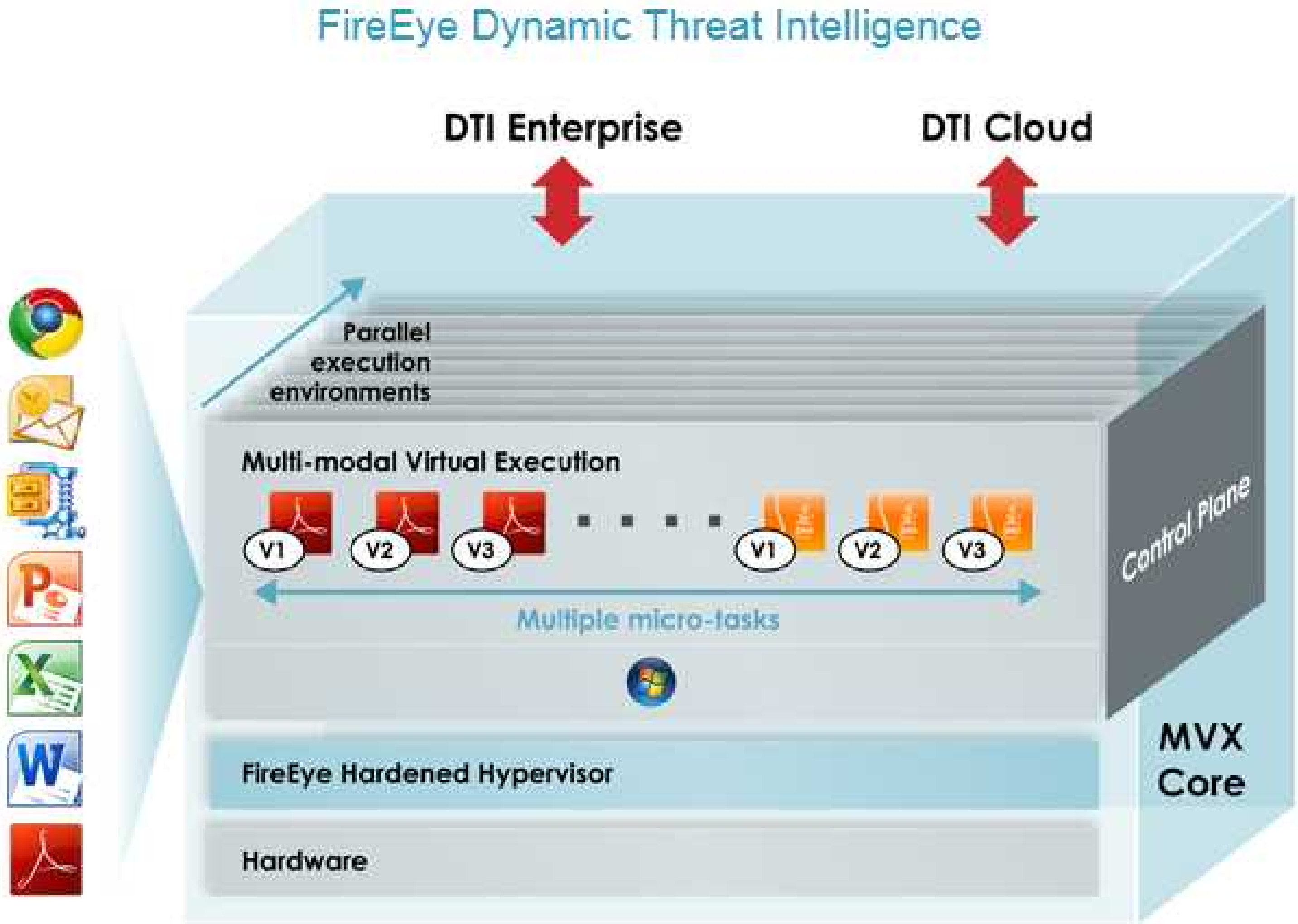
How could Stuxnet be avoided?

- Protect process information
- Rootkit Protection \ Detection
- Real Air-Gaps (sneaker-net is still connectivity)
- Trip-Wire like protection for both PC and PLC
- A deep-freeze like reverting tool could prevent changes
- Develop a forensics process for Control Systems
- Network Intrusion Detection System could have seen some of the network traffic. Combined with a decent forensics capability this could have warned at some stage.
- More Ideas?

"Next – Generation" Solutions

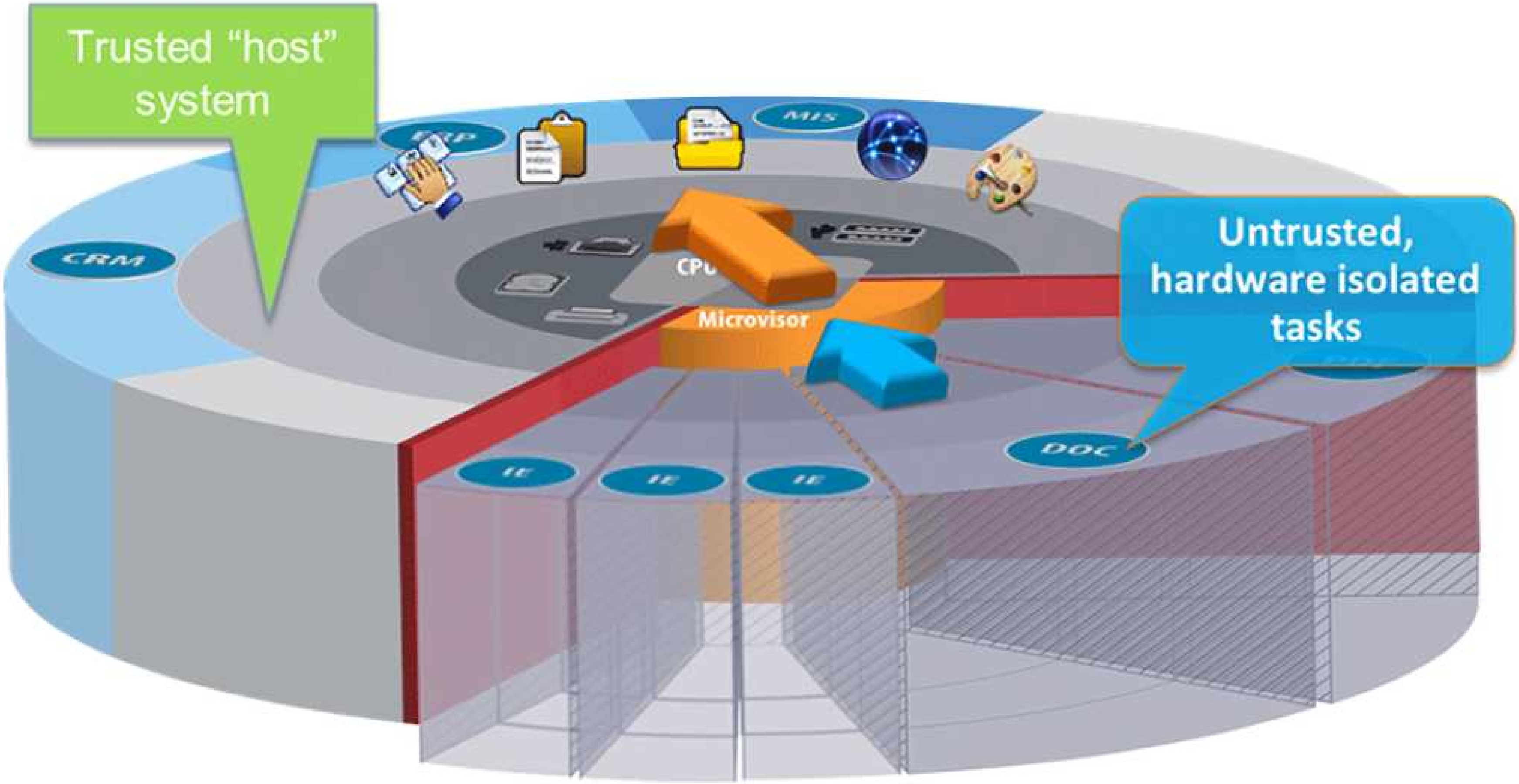
- Architecture
  - Signature-less
  - Still can use signatures
- Monitor Point
  - Network
  - Host (Virtualization)
  - Cloud Analytics (Big Data)
  - Hybrid
- Target
  - Zero days
  - Advance persistence threats
- Examples
  - Fireeye
  - Bromium

NG Solutions – Fireeye


FireEye Dynamic Threat Intelligence
DTI Enterprise
DTI Cloud
Parallel execution environments
Multi-modal Virtual Execution
V1
V2
V3
V1
V2
V3
Multiple micro-tasks
Control Plane
FireEye Hardened Hypervisor
Hardware
MVX Core

Source: http://www.fireeye.com/products-and-solutions/virtual-execution-engine.html

NG Solutions - Bromium



Security Audits

Security Audits

- Access is given to assessors by the owner/operator
- Clearly defined standards and metrics exist
- Assessor assures that common protection criteria are met
  - Actual security is not tested
  - Compliance with established security procedures is verified

Possible Assessor Activities

- Check for rogue equipment and unauthorized use
- Verify and validate security settings are compliant with laws and regulations
- Measure against established best practices

Vulnerability Assessments

Sandia National Laboratories

Vulnerability Assessments

- Access is given to assessors by the owner/operator
- Should not be performed by the designers/developers
- Scope is negotiable
  - Clearly defined standards and metrics likely do not exist
  - Depth and breadth appropriate to system function and team skill
- Assessors look for vulnerabilities in system design and implementation

Possible Assessor Activities

- Examine hardware and software components for known flaws (e.g., buffer overflows)
- Verify proper integrity, confidentiality, and availability mechanisms
- Locate weaknesses in physical and logical equipment placement

Penetration Tests

Penetration Tests

- Authorization to attack, but no access, is given to assessors by the owner/operator
- Should be performed by trained and reputable professionals
- Scope is negotiable
  - Components in/out of bounds
  - “Rules of engagement”
  - Overt/covert
- Validates or refutes assumptions made about system security
  - Vulnerabilities are not always exploitable
  - Demonstrate how actual security posture holds up to various attacks

Possible Assessor Activities

- Attempt to insert rogue equipment and bypass security controls
- Enumerate and attempt to exploit hardware and software component flaws
- Exploit weaknesses in integrity, confidentiality, and availability mechanisms
- Penetrate deeper into system through multi-homed components
- …

Red Team Assessments

Red Team Assessments

- Authorization to attack (and possibly some access), is given to assessors by the owner/operator
- Should be performed by trained and reputable professionals
- Scope is negotiable
  - Adversaries of concern shape the depth and breadth of the assessment
  - “Rules of engagement”
  - Overt/covert
- Determine how the system both defeats and is susceptible to adversaries of concern
  - Not all vulnerabilities are exploitable by or of interest to adversaries of concern
  - Demonstrate how actual security posture holds up to various attacks subject to adversarial constraints (commitments and resources)

Possible Assessor Activities

- Those activities enumerated for penetration tests
- Attempt theft and/or cloning of authorized equipment
- Determine criticality of wireless systems to target missions
- Assume the assistance of a malicious insider
  - Attack from the “wired side” to affect integrity, availability, and confidentiality of the “wireless side”
  - Intentionally weaken security controls

Attestation / IMA

Attestation

- Detect changes to computer configuration
- Measurement of software
- TPM / Secure Core
- 3rd party
- Cryptography
- May not measure all software
    - SMM
    - AML
    - AMT

IMA

- Measures code before execution
- Access control and policies
- Collect
- Store
- Attest
- Appraise
- Protect

The Foreseeable Future

- It will get worse
  - Vendors are under increased pressure to rush to market
  - “Smart”-ness is becoming more prolific: “The Internet of Things”
  - There is increased motivation for attackers to do what they do
  - Advanced features being added will open up more local and remote attack opportunities
  - The consequences of exploitation will worsen: think cars
  - Tighter integration will mean vulnerabilities in one product will facilitate access to another

Questions?

Source: http://www.danajarvis.org/virtualteams/?tag=trust

Center for Cyber Defenders

- http://www.sandia.gov/careers/students_postdocs/internships/institutes/cyber_defenders.html
- http://www.sandia.gov/titans/
- Create Profile, otherwise you can’t be hired

Some History

1990s

- Internet access becomes available to the general public.
- Because most consumer Internet access is dial-up based, there is little need to share Internet access.
- The Wi-Fi Alliance is formed in 1999.
- 802.11 technology ships with WEP, despite known flaws.

2001

- Linksys ships its 1 millionth cable/DSL router.
- UPnP Forum Steering Committee approves the Internet Gateway Device (IGD) standard.

2002

- The Linksys WRT54G router is first released.

2003

- Draft 802.11i (WPA) becomes available for use.

Some History

2004

- Consumer Internet access is roughly split evenly between dial-up and broadband.
- Full 802.11i (WPA2) is standardized.

2005

2006

- The ability to access the Internet over cellular networks becomes commonly available.
- Wi-Fi Protected Setup (WPS) is introduced.

2007

Some History

2008

2009

2010

- Over 90% of consumer Internet access is broadband based.
- The Wi-Fi Alliance consists of between 350 and 400 companies.
- The UPnP Forum Steering Committee approves IGDv2 standard.

2011

- Fundamental design flaw in WPS is publicly revealed, along with a tool for brute-force exploitation.

Some History

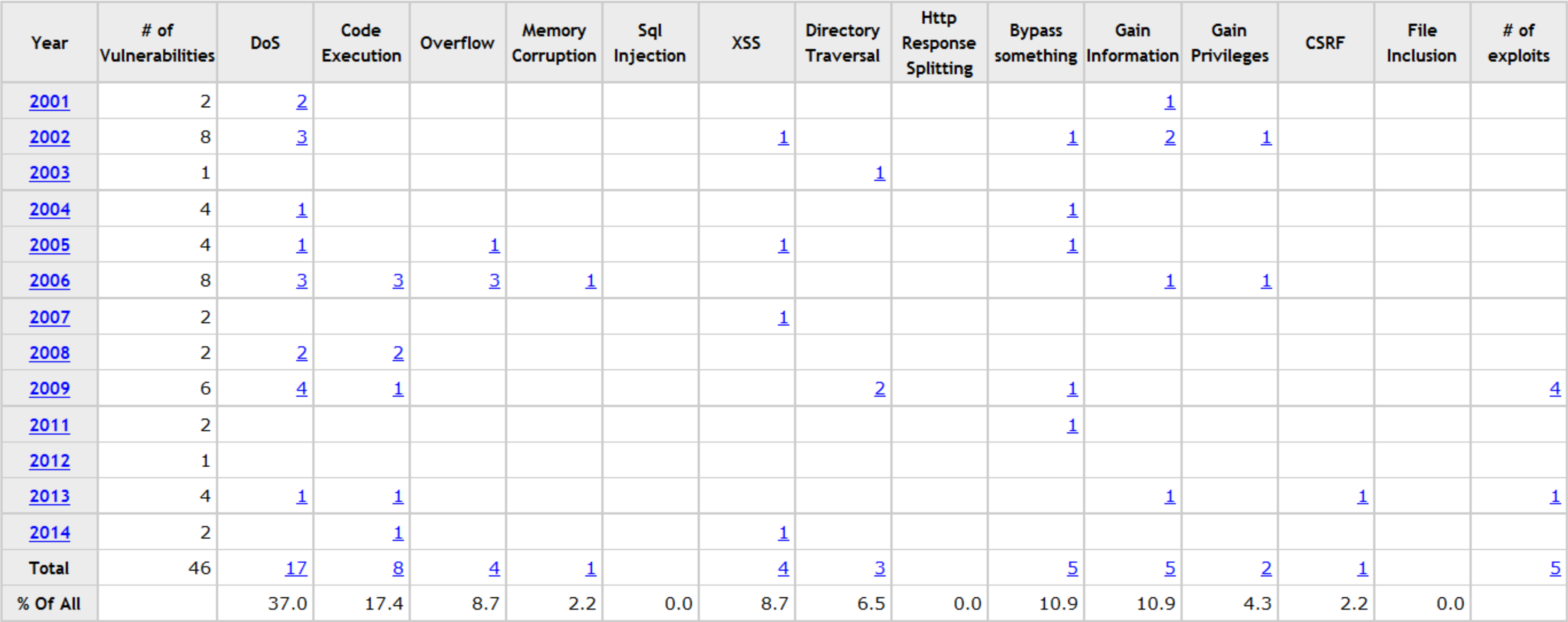
2012

2013

2014

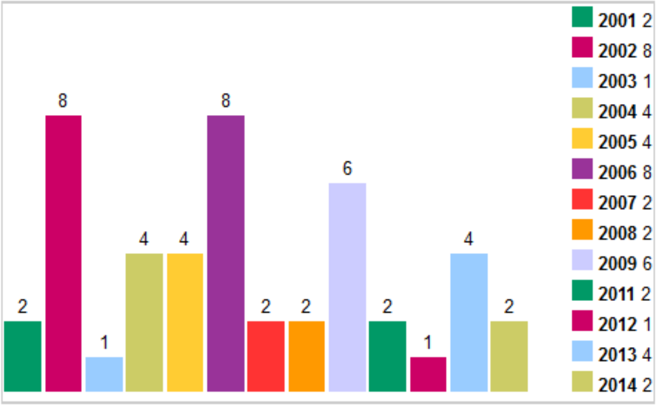
- Linksys announces it will no longer updates for equipment models no longer in production.

(In)Security, In General

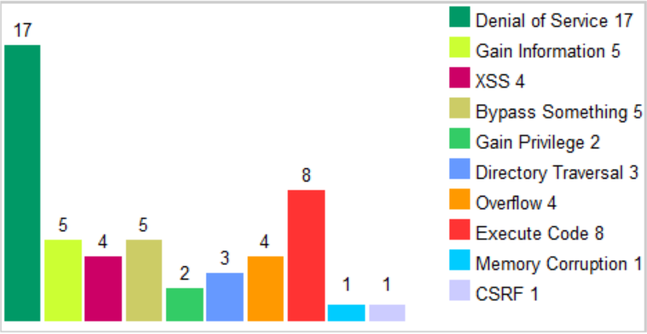


Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	2	2									1				
2002	8	3					1			1	2	1			
2003	1							1							
2004	4	1								1					
2005	4	1		1			1			1					
2006	8	3	3	3	1						1	1			
2007	2						1								
2008	2	2	2												
2009	6	4	1					2		1					4
2011	2									1					
2012	1														
2013	4	1	1								1		1		1
2014	2		1				1								
Total	46	17	8	4	1		4	3		5	5	2	1		5
% Of All		37.0	17.4	8.7	2.2	0.0	8.7	6.5	0.0	10.9	10.9	4.3	2.2	0.0	

Vulnerabilities By Year



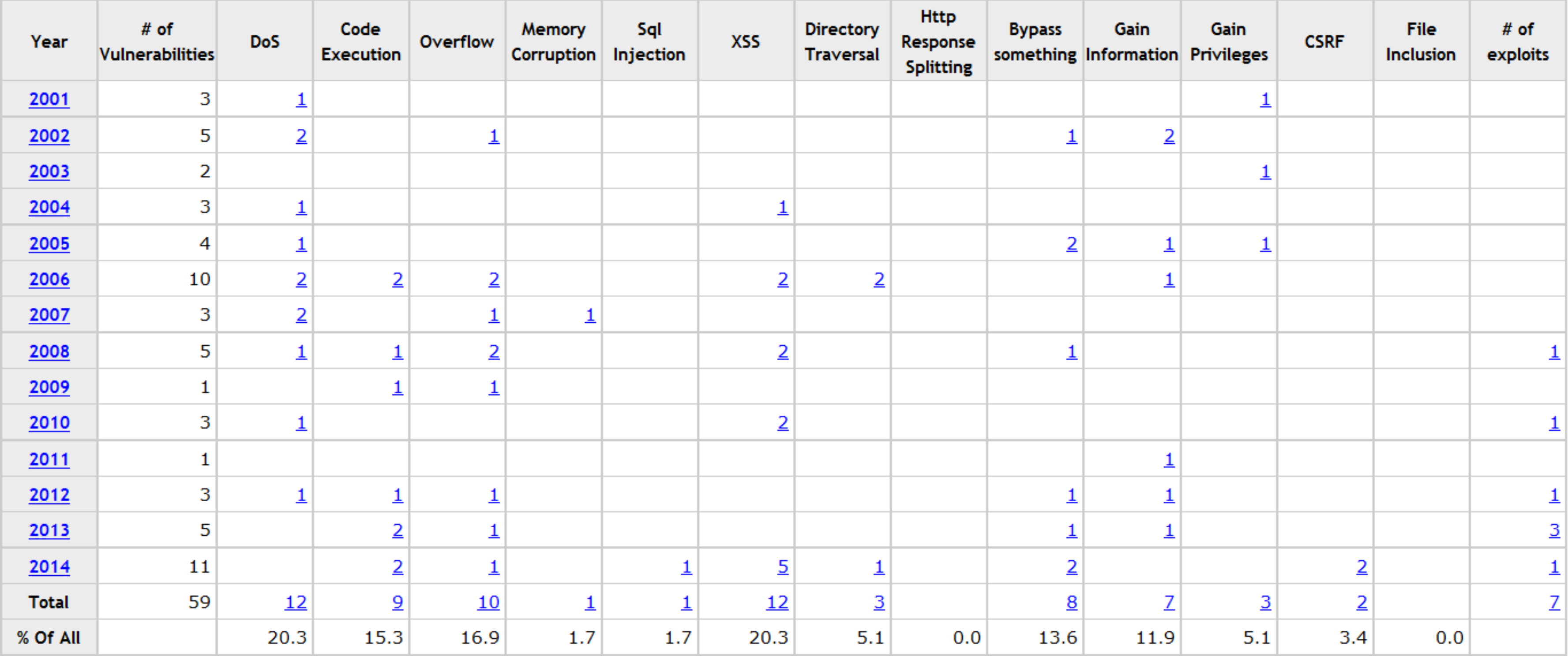
Vulnerabilities By Type



CVE Details
for Netgear

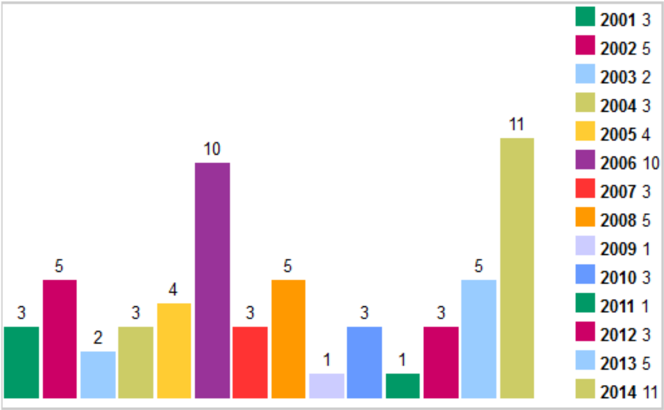
As of July 2014
http://www.cvedetails.com/vendor/834/Netgear.html

(In)Security, In General

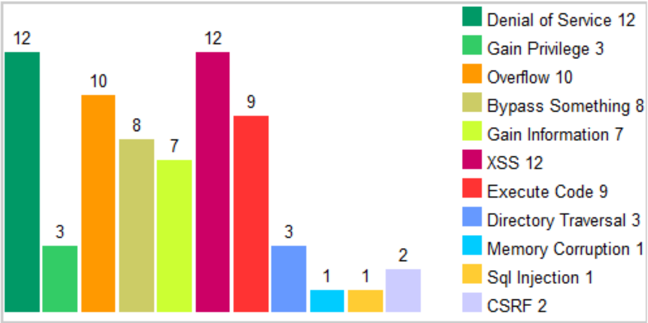


Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	3	1										1			
2002	5	2		1						1	2				
2003	2											1			
2004	3	1					1								
2005	4	1								2	1	1			
2006	10	2	2	2			2	2			1				
2007	3	2		1	1										
2008	5	1	1	2			2			1					1
2009	1		1	1											
2010	3	1					2								1
2011	1										1				
2012	3	1	1	1						1	1				1
2013	5		2	1						1	1				3
2014	11		2	1		1	5	1		2			2		1
Total	59	12	9	10	1	1	12	3		8	7	3	2		7
% Of All		20.3	15.3	16.9	1.7	1.7	20.3	5.1	0.0	13.6	11.9	5.1	3.4	0.0	

Vulnerabilities By Year



Vulnerabilities By Type



CVE Details
for D-Link

As of July 2014
http://www.cvedetails.com/vendor/899/D-link.html

Some Specific Security Issues

- GlobalSunTech Wireless Access Points (1) WISECOM GL2422AP-0T, and possibly OEM products such as (2) D-Link DWL-900AP+ B1 2.1 and 2.2, (3) ALLOY GL-2422AP-S, (4) EUSSO GL2422-AP, and (5) LINKSYS WAP11-V2.2, allow remote attackers to obtain sensitive information like WEP keys, the administrator password, and the MAC filter via a "getsearch" request to UDP port 27155.
- *This is a backdoor, plain and simple.*

Some Specific Security Issues

- Linksys EtherFast Cable/DSL BEFSR11, BEFSR41 and BEFSRU31 with the firmware 1.42.7 upgrade installed opens TCP port 5678 for remote administration even when the "Block WAN" and "Remote Admin" options are disabled, which allows remote attackers to gain access.
- *This means your router ignores your configuration settings.*

Some Specific Security Issues

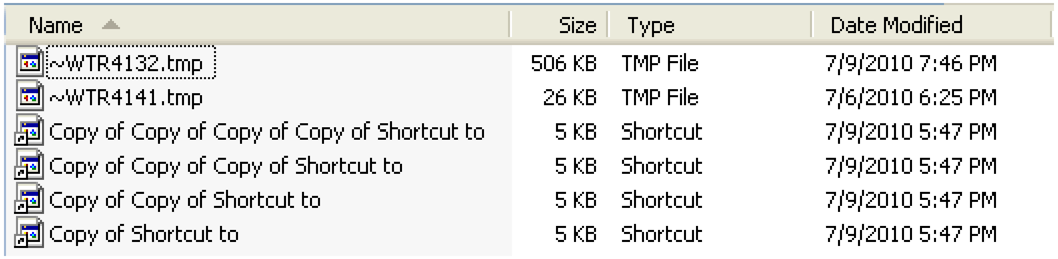
- A cross-site scripting bug was found on the router’s apply.cgi that works regardless of authentication and would allow an attacker to access the device, change settings or upload modified firmware.
- *This means the admin HTTP server carries all the common web application problems.*

Timeline – The Basics

- January 2009
  - Earliest assumed work on Stuxnet begins
- June 2010
  - VirusBlokAda finds current Stuxnet variant in the wild
- July 2010
  - Microsoft uses the name Stuxnet publicly
- July 17, 2010
  - VeriSign revokes Realtek certificate used in Stuxnet
- July 20, 2010
  - VeriSign revokes JMicron certificate used in Stuxnet
- August 2, 2010
  - Microsoft releases security bulletin about LNK vulnerability
- September 14, 2010
  - Microsoft releases security bulletin about print spooler vulnerability
- October 12, 2010
  - Microsoft releases security bulletin about Win32k.sys vulnerability

Stuxnet Contains:

- LNK files
  - "Copy of Shortcut to.lnk"
  - "Copy of Copy of Shortcut to.lnk"
  - "Copy of Copy of Copy of Shortcut to.lnk"
  - "Copy of Copy of Copy of Copy of Shortcut to.lnk"
- Infection DLLs
  - ~WTR4141.tmp
  - ~WTR4132.tmp
  - Stuxnet.dll
  - S7otbxdx.dll
- Rootkit Drivers
  - MRXCLS.sys
  - MRXNET.sys
- Other
  - Backup files
  - Configuration files
  - Alternate infection files



Name	Size	Type	Date Modified
~WTR4132.tmp	506 KB	TMP File	7/9/2010 7:46 PM
~WTR4141.tmp	26 KB	TMP File	7/6/2010 6:25 PM
Copy of Copy of Copy of Copy of Shortcut to	5 KB	Shortcut	7/9/2010 5:47 PM
Copy of Copy of Copy of Shortcut to	5 KB	Shortcut	7/9/2010 5:47 PM
Copy of Copy of Shortcut to	5 KB	Shortcut	7/9/2010 5:47 PM
Copy of Shortcut to	5 KB	Shortcut	7/9/2010 5:47 PM

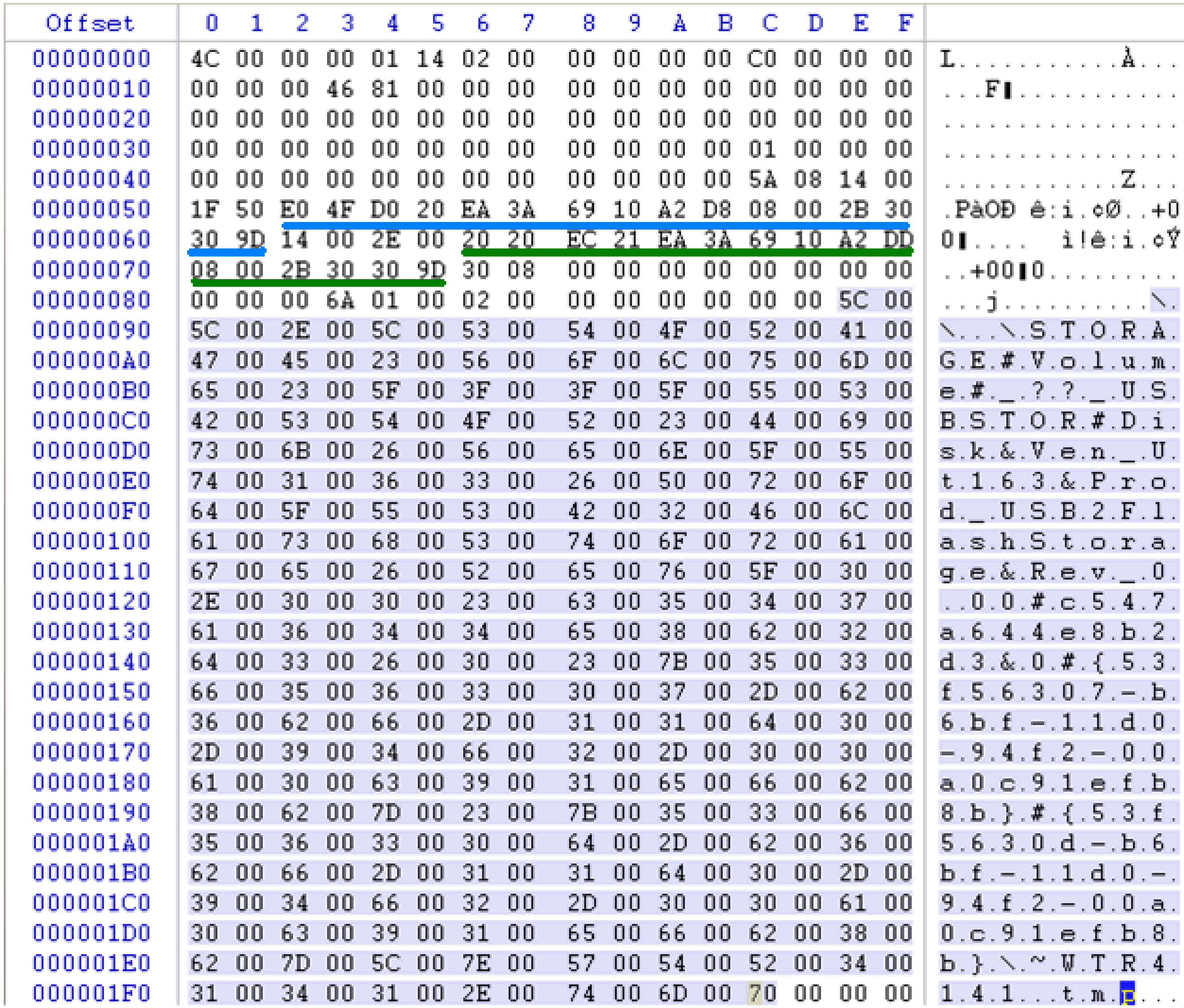
Infection Vectors

Vulnerability Name	0-day?	Type of vulnerability
MS10-046	No*	LNK – remote code execution when a special link file is viewed with Explorer
MS10-061	No*	Print Spooler – remote code execution through a special print request over RPC
MS10-073	Yes	Elevation of privilege in XP through Win32k.sys
N/A	Yes	Elevation of privilege in Vista & Win7
MS08-067	No	Server Service – remote code execution through RPC

* Unnoticed by Microsoft until Stuxnet

LNK Vulnerability

- Blue – CLSID for My Computer
- Green – CLSID for Control Panel
- Highlight – Target DLL



```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  4C 00 00 00 01 14 02 00  00 00 00 00 C0 00 00 00  L...........À...
00000010  00 00 00 46 81 00 00 00  00 00 00 00 00 00 00 00  ...F▮...........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 5A 08 14 00  ............Z...
00000050  1F 50 E0 4F D0 20 EA 3A  69 10 A2 D8 08 00 2B 30  .PàOÐ ê:i.¢Ø..+0
00000060  30 9D 14 00 2E 00 20 20  EC 21 EA 3A 69 10 A2 DD  0▮....  ì!ê:i.¢Ý
00000070  08 00 2B 30 30 9D 30 08  00 00 00 00 00 00 00 00  ..+00▮0.........
00000080  00 00 00 6A 01 00 02 00  00 00 00 00 00 00 5C 00  ...j..........\.
00000090  5C 00 2E 00 5C 00 53 00  54 00 4F 00 52 00 41 00  \...\.S.T.O.R.A.
000000A0  47 00 45 00 23 00 56 00  6F 00 6C 00 75 00 6D 00  G.E.#.V.o.l.u.m.
000000B0  65 00 23 00 5F 00 3F 00  3F 00 5F 00 55 00 53 00  e.#._.?.?._.U.S.
000000C0  42 00 53 00 54 00 4F 00  52 00 23 00 44 00 69 00  B.S.T.O.R.#.D.i.
000000D0  73 00 6B 00 26 00 56 00  65 00 6E 00 5F 00 55 00  s.k.&.V.e.n._.U.
000000E0  74 00 31 00 36 00 33 00  26 00 50 00 72 00 6F 00  t.1.6.3.&.P.r.o.
000000F0  64 00 5F 00 55 00 53 00  42 00 32 00 46 00 6C 00  d._.U.S.B.2.F.l.
00000100  61 00 73 00 68 00 53 00  74 00 6F 00 72 00 61 00  a.s.h.S.t.o.r.a.
00000110  67 00 65 00 26 00 52 00  65 00 76 00 5F 00 30 00  g.e.&.R.e.v._.0.
00000120  2E 00 30 00 30 00 23 00  63 00 35 00 34 00 37 00  ..0.0.#.c.5.4.7.
00000130  61 00 36 00 34 00 34 00  65 00 38 00 62 00 32 00  a.6.4.4.e.8.b.2.
00000140  64 00 33 00 26 00 30 00  23 00 7B 00 35 00 33 00  d.3.&.0.#.{.5.3.
00000150  66 00 35 00 36 00 33 00  30 00 37 00 2D 00 62 00  f.5.6.3.0.7.-.b.
00000160  36 00 62 00 66 00 2D 00  31 00 31 00 64 00 30 00  6.b.f.-.1.1.d.0.
00000170  2D 00 39 00 34 00 66 00  32 00 2D 00 30 00 30 00  -.9.4.f.2.-.0.0.
00000180  61 00 30 00 63 00 39 00  31 00 65 00 66 00 62 00  a.0.c.9.1.e.f.b.
00000190  38 00 62 00 7D 00 23 00  7B 00 35 00 33 00 66 00  8.b.}.#.{.5.3.f.
000001A0  35 00 36 00 33 00 30 00  64 00 2D 00 62 00 36 00  5.6.3.0.d.-.b.6.
000001B0  62 00 66 00 2D 00 31 00  31 00 64 00 30 00 2D 00  b.f.-.1.1.d.0.-.
000001C0  39 00 34 00 66 00 32 00  2D 00 30 00 30 00 61 00  9.4.f.2.-.0.0.a.
000001D0  30 00 63 00 39 00 31 00  65 00 66 00 62 00 38 00  0.c.9.1.e.f.b.8.
000001E0  62 00 7D 00 5C 00 7E 00  57 00 54 00 52 00 34 00  b.}.\.~.W.T.R.4.
000001F0  31 00 34 00 31 00 2E 00  74 00 6D 00 70 00 00 00  1.4.1...t.m.p...
```

PLC Impact

- Three different variations of STL code are loaded into different PLCs. Symantec refers to them as A, B, and C.
  - A: Manipulates network communication. Targets 6ES7-315-2.
  - B: Functionally equivalent to A.
  - C: I/O manipulation. – appears to be incomplete. Targets 6ES7-417.
- OB1 is moved and replaced (pre-pended) to allow new behavior and original behavior
- OB35 is a “watchdog” that can suspend operation of the OB1 called code under some conditions (where the condition is passed as a memory value)

PLC Known Malicious Code

`UC FC1874` – unconditional call in OB35, called every 100ms (`FC 1865` for OB1)
`POP`
`L DW#16#DEADF007` – if return from FC 1874 or FC 1865 is DEADF007, original code on PLC is skipped
`==D`
`BEC` – block end conditional
`L DW#16#0` – if return code did not match, accumulator is cleared
`L DW#16#0`

- DEADF007
  - Dead Foot – aircraft lingo
  - Dead Fool
  - May or may not have significance