When CSOs Attack

Implementing a mandatory audit policy

BSides San Francisco 2011

HD Moore

RAPID7
Chief Security Officer

metasploit
Founder & Chief Architect

Agenda

1. The accumulation of crufty systems
2. The acquisition of new technology
3. The case for mandatory audits
4. The quicklist for hardware
5. The quicklist for software
6. The quicklist for services
7. Real-life case studies

Accumulation

Accumulation

- How often do you decommission old systems?
- How do you manage the risk of these systems?
- What do you do with obsolete hardware?
- How fast are your networks growing?
- What about those 3rd party services?

Accumulation

- Networks will continue to grow
- Legacy systems never die
- You are still responsible

Accumulation

- SNMP survey of 3.1b IPs = 2M results
- Build date exposed in 250k of those
- Identified over 60,000 Cisco routers
- Cisco releases ~43 advisories/year (1999)
- Over 50% of Cisco routers are exploitable
  - 37,000 of 60,000 were 2007 or earlier
  - Only counts devices with open SNMP

Accumulation

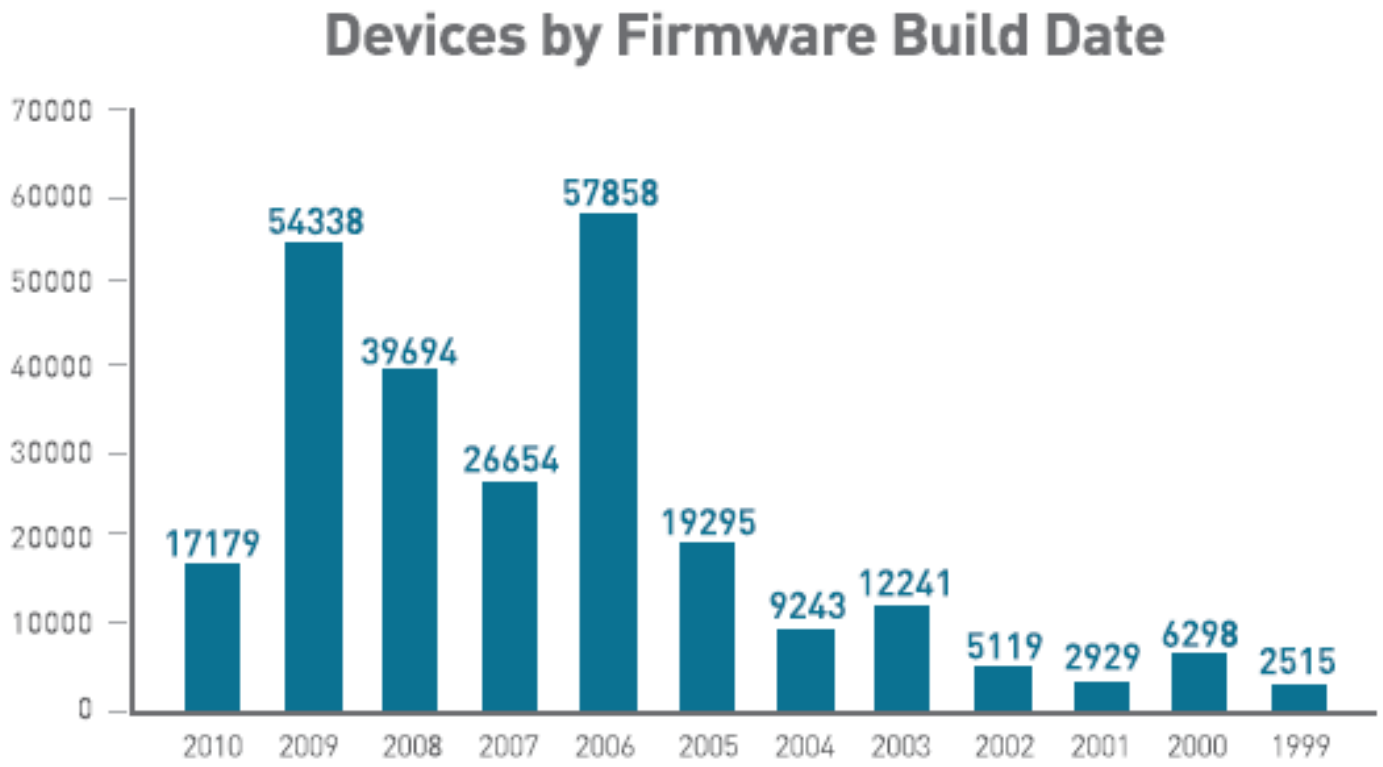

Figure 1 | Breakdown of 205,742 devices by firmware build date

Accumulation

- We are burying ourselves in obsolete systems
- This is a real problem with a mix of solutions
  - Vulnerability management
  - Risk management
  - Mitigations
  - Controls
- We are limited in options with legacy assets
- We can improve the situation going forward

Acquisition

Acquisition

- We buy tons of software, hardware, services
- We want to solve a real business need
- We want to solve as fast we can
- We want to deploy it securely
- We want to keep it secure

Acquisition

- We receive pressure from all sides
  - From the user who wants to actually use the product
  - From the stakeholders waiting on the result
  - From accounting to use the budget
  - From the vendor's sales team

- The timing can be critical
  - Window of actual usefulness
  - Limited time sales offers

Acquisition

- The acquisition process is an opportunity
  - Our best shot at reducing long-term risk
  - Our best chance to allocate resources
  - Our best leverage with the vendor

- This only works if you can move fast
  - Stakeholders don’t want to wait
  - Vendors certainly want to close
  - Prep your team in advance

Auditing

Auditing

- Common reasons for NOT auditing
  - Lack of qualified staff to perform the test
  - Lack of resources to conduct the review
  - Lack of access to the proposed solution
  - Lack of executive support for your role

Auditing

- Building a qualified audit team
  - Allow your existing folks to learn as they go
  - Supplement with consultants/experts to start
  - Involve the IT folks when time permits
  - Motivation is the #1 requirement
  - Anything is better than nothing

Auditing

- Finding and allocating resources
  - Nearly everything can be virtualized these days
  - Prepare base OS images for common platforms
  - Identify audit resources in the project plan
  - Make it clear these resources are required

Auditing

- Getting access to the proposed solution
  - Vendors love to cut out the security folks
  - Make it clear that the audit is required
  - Make it clear that you want it to pass
  - Describe the setup you need
  - Bug them until you get it

Auditing

- Getting executive support for audits
  - Prepare a case study of a prior IT security failure
  - Describe how a pre-sales audit would help
  - Justify the resources and time with examples
    - Existing workarounds for production systems
    - The full cost of a rip and replacement
    - The full cost of a data breach

Hardware

Hardware

1. Obtain the raw disk image whenever possible
2. Obtain a virtual machine whenever possible
3. Review everything, not just the “application”
   - Versions of package, libraries, and kernels
   - Crack stored password databases (shadow)
   - Support package configurations
   - Firewall rules and restrictions
4. Focus on the vendor applications last*
   - Vendors are much worse at OS maintenance
   - Often easier to fix an application flaw

Hardware

- Routers and switches
  - Grab the CF-IDE card when possible
  - Grab the OS image via TFTP
  - Grab the OS image from the vendor

- Virtual Appliances
  - Ignore the appliance and grab the VMDK image
  - Mount this and audit it independently first
  - Avoids boot passwords and console logins

Software

Software

1. Create a virtualized clone of the real environment
   - The same OS, SP, IPs, network ranges
   - Make heavy use of virtual machine snapshots
2. Always review the dependencies
   - Check the configuration and version numbers
3. Capture and analyze the network traffic
4. Quickly review binaries via IDA Pro
5. Examine all crypto certificates in detail
6. What is their SLA for reported vulnerabilities?

Services

Services

1. Obtain the last 3 SAS-70s and look for patterns
2. Obtain the results of their last security audit
   - Make sure the scope matches your own use case
3. Review the complete solution architecture
4. Determine how customer resources are mixed
5. Ask for audit access to the hosted environment
6. Ask for backup access to the binaries and logs
7. Ask for a right to audit as a contract addendum
8. Ask for a SLA for fixed reported vulnerabilities

Case Studies

#1. Web Portal "A"

- Business need
  - A web portal to interact with the community
  - Maintain an online knowledge base
  - Spark community discussions

- Audit process
  - Standard due diligence and SAS-70 reviews
  - Manual web application assessment
  - PASSED

#1. Web Portal "A"

- Moved forward with implementation
  - Vendor bait-and-switched to a different application
  - Demo platform was ASP.NET
  - Production was classic ASP

- Triggered a second audit
  - Manual web application assessment
  - FAILED: SQLI, XSS, CSRF, etc

#2. Web Portal "B"

- Business need
  - A web portal to interact with the community
  - Maintain an online knowledge base
  - Spark community discussions

- Audit process
  - Standard due diligence and SAS-70 reviews
  - Manual web application assessment
  - PASSED

#2. Web Portal "B"

- Moved forward with implementation
  - Vendor refused access to the hosted environment
  - Immediate red flag about shared resources

- Triggered a contract addendum
  - Statement regarding resource allocation
  - Remote access to online backups and logs
  - Configured a standby backup installation
  - PASSED

#3. QA Automation Framework

- Business need
  - Help QA automate and manage product tests

- Audit process (#1)
  - Consultants installed the product to a test server
  - Audit of the OS and base configuration
  - Audit of the web application itself
  - FAILED

#3. QA Automation Framework

- Reasons for audit failure
  - Default WAMPP installation with zero security
  - Multiple exposed web applications (phpMyAdmin)
  - Weak or missing passwords on all services
  - Web application encoded with IONCube
  - XSS in the login page

#3. QA Automation Framework

- Audit process (#2)
  - Reinstalled into a supported Linux configuration
  - Configured strong passwords on all services
  - Audit of the OS and base configuration
  - Audit of the web application itself
  - FAILED

#3. QA Automation Framework

- Reasons for audit failure
  - Passwords exposed via web interface four ways
  - IONCube loader exposes sensitive information
  - PHP cronjob scripts accessible via web
    - Resulted in exposed SQL dumps

#3. QA Automation Framework

- Moving forward
  - Created a massive .htaccess list to whitelist pages
  - Contract addendum to fix application flaws
  - PASSED

#4. Check Point Firewall

- Business need
  - Install a new firewall for a datacenter

- Audit process
  - Clone the configuration into a virtual environment
  - Audit every component of the installation
  - FAILED

#4. Check Point Firewall

- Reasons for audit failure
  - Endpoint Security Server exposed private data
  - All SSL private keys and package signing keys

- Moving forward
  - Excluded vulnerable components in production
  - Reported to the vendor and patch issued*
  - See Rapid7 advisory R7-0038 for more
    - http://www.rapid7.com/security-center/advisories/R7-0038.jsp
  - PASSED

#5. File Transfer Appliance "A"

- Business need
  - Securely share files with customers and partners

- Audit process
  - Configure a virtual appliance in a test environment
  - Audit the OS packages and configuration
  - Audit the backend processes and code
  - Audit the web application frontend
  - FAILED

#5. File Transfer Appliance "A"

- Reasons for audit failure
  - Remote root through spoofed, encrypted UDP
  - Static passwords for many system accounts
  - Ancient SSH keys in authorized_keys file
  - Misconfigured rsync and internal daemons
  - Admin console TTY check bypass
  - IONCube encoded web application
  - See Rapid7 advisory R7-0039 for more
    - http://www.rapid7.com/security-center/advisories/R7-0039.jsp

#6. File Transfer Appliance "B"

- Business need
  - Securely share files with customers and partners

- Audit process
  - Configure a virtual appliance in a test environment
  - Audit the OS packages and configuration
  - Audit the backend processes and code
  - Audit the web application frontend
  - FAILED

#6. File Transfer Appliance "B"

- Reasons for audit failure
  - Axis2 interface exposed with default user/pass
  - Outdated Java libraries for Tomcat (Spring)

- Moving forward
  - Verified that Axis2 is not exploitable
  - Verified that Spring use is not exploitable
  - PASSED

Summary

Summary

- Mandatory audits save time for everyone
- Stronger leverage with the solution vendor
- Improved awareness among all stakeholders
- Provides tangible data for security decisions
- Sets a security baseline for new purchases

Questions?