Bob Cowles
SLAC National Accelerator Laboratory
HEPiX Spring Meeting, Prague
April 26, 2012

CYBER SECURITY RETROSPECTIVE AND FUTURE DIRECTIONS

Work supported by U. S. Department of Energy contract DE-AC02-76-SFO0515

BC History (1998-1999)

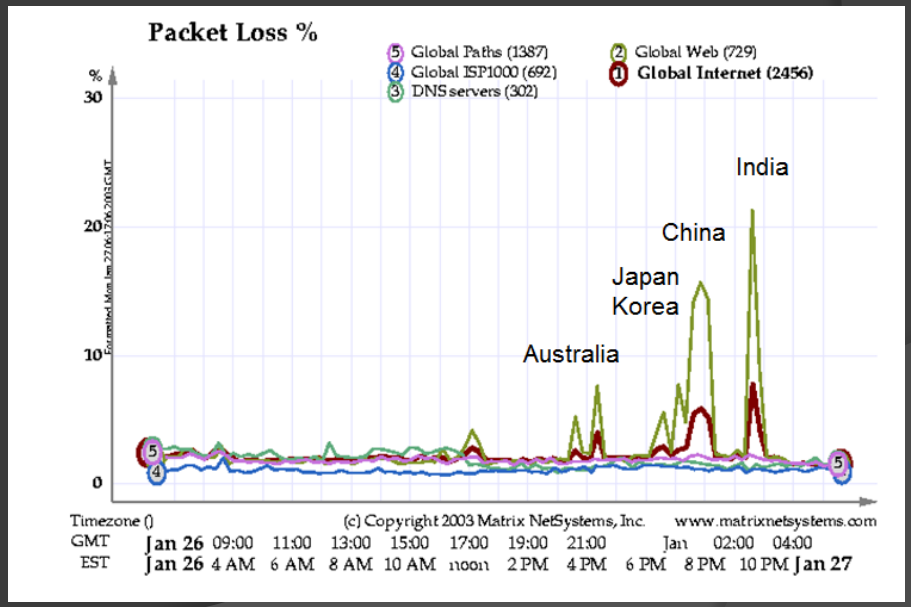
- 1998 – CERN (HEPNT)
- 1999 – SLAC (HEPiX/HEPNT)
- Status reports on changes following significant intrusion in June, 1998
  - Network architecture (partition business systems)
  - Deploy WTS/Citrix as portal to business systems
  - Removal of clear-text passwords (e. g. telnet)
  - Tightening client machine (WINNT) configurations

BC History (2000)

- 2000 – Braunschweig; JLab
- Importance of Business Impact Assessment
  - Senior management involvement is crucial
  - What needs protection?
  - Given security is not absolute
    - What losses are acceptable? .. .What costs are acceptable?
  - Everyone must be informed
  - Be sure to have emergency procedures documented
    - Catastrophe
    - Partial failure modes
  - Leverage security concerns to gain control of OS configurations
  - Limit visibility of complex protocols
    - Block if possible, otherwise allow only “well maintained” servers
    - HTTP and XML are going to have many more security issues

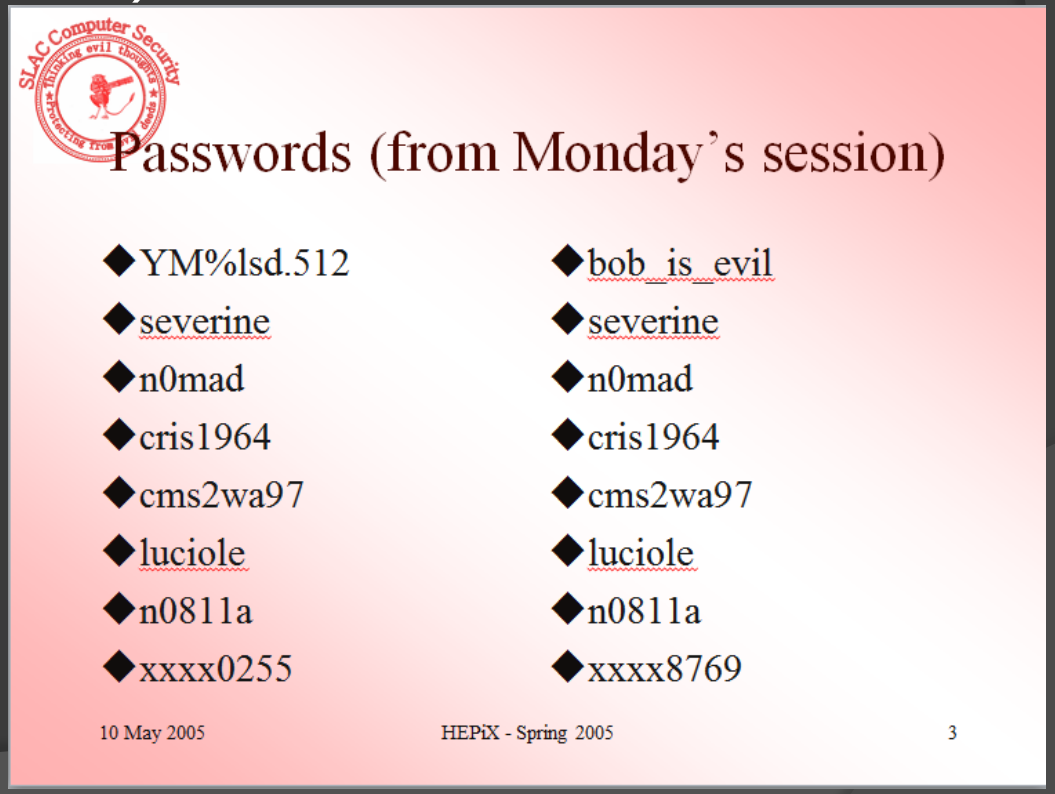
BC History (2001-2003)

- 2001 – NERSC (LBNL)
- 2002 – Fermi
- 2003 – TRIUMF
  - Poor system administration is ***still*** a major problem
  - Firewalls cannot substitute for applying patches
  - Multiple levels of virus/worm protection are necessary
  - No easy solutions



BC History (2004-2006)

- 2004 – Edinburgh, Brookhaven
- 2005 – Karlsruhe, SLAC
- 2006 – CASPUR (Rome)



BC History (2004-2006)

- Attacks coming faster; attackers getting smarter
- Complex attacks using multiple vulnerabilities
- No simple solution works
  - Patching helps
  - Firewalls help
  - AV & attachment removal help
  - Encrypted passwords/tunnels help
- You can't be "secure"; only "more secure"
- We must share information better

BC History (Recent)

- Password capture was turned over to Romain after 2006
- 2011 – TRIUMF
  - IPv6 Insecurities – but we have to do it anyway
- 2012 – Prague
  - You're listening to it

Old Technologies and Issues

- Password authentication, clear text, too many passwords, & password re-use https://xkcd.com/936/

- OS, server, & application/browser vulnerabilities
- Mis-configured webservers, networks, clients
- Wireless hijacking (2006; 2012 issue also) https://www.immunityinc.com/infiltratemovies/movies/markwuergler_Secretsinyourpocketanalysisofwirelessdata.mp4
- DDOS vulnerability – moved from network bandwidth to Server/Application bandwidth https://www.immunityinc.com/downloads/Effective_DoS_Attacks_against_web_application_platforms_INFILTRATE_2012.pdf
- Buffer overflows, Use-after-free – C lives on https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices
- Viruses, Trojans, Bots, Worms, Keyloggers
- Users – the Level 8 vulnerability https://www.websense.com/assets/reports/report-2012-threat-report-en.pdf

× Click to close

CYBERATTACKS TIMELINE

MAJOR COMPANIES/AGENCIES RECENTLY TARGETED *(Date of attacks only indicate when they were first discovered or publicised)*

2010 Dec — Hacker group claiming attack
Mastercard.com, Paypal, Visa.com, PostFinance
Anonymous launches orchestrated attacks in support of Wikileaks founder Julian Assange

2011 Mar. — (unidentified)
RSA
Hackers steal data related to RSA secure tokens

20 Apr or earlier
Sony Playstation Network
Hackers steal personal information from millions of users in first of a series of attacks on Sony

22 Apr*
Fox Networks
Lulzsec stole personal information of 70,000 X Factor contestants, database and passwords from employees

May
Citigroup Inc.
Hackers take 200,000 customers' data

21 May
Lockheed Martin
Hacked but managed to stop attack before any critical data was stolen

30 May
PBS.org *Lulzsec defaced its website, posted a fake article and stole its database*

1 Jun
Google *Email system hacked, attack suspected to originate from China*

2 Jun
Sonybmg.nl, Sonybmg.be
3 Jun
Nintendo.com
Infragard-Atlanta (FBI)

10 Jun
Turkish government websites
Anonymous takes down several government sites in protest to Internet censorhip

11 Jun
International Monetary Fund
Hack suspected to originate from a "foreign government"

Spanish National Police
Anonymous hacks website in response to arrests of alleged group members

13 Jun
Bethesda Game Studio
U.S. Senate *(www.senate.gov)*
Lulzsec hacked and released internal data from its servers

15 Jun
Malaysian government websites
Hacked after an attack warning from Anonymous in response for censoring Wikileaks

Central Intelligence Agency
Lulzsec hacked the CIA's public website, www.cia.gov, making it temporarily inaccessible

19 Jun
SEGA
Hackers compromise accounts of some 1.3 million customers

3 Jul
Apple
Anonymous hacks into one of Apple's servers, publishes internal usernames and passwords

21 Jul
NATO
Anonymous and Lulzsec hack NATO servers, obtain 1GB of restricted data

HACKER GROUPS ASSOCIATED IN RECENT ATTACKS

Insignias

Anonymous
Describes themselves as an online community who promotes internet freedom and freedom of speech. Participated in international hacktivism and protests since 2008

Insignia

Lulzsec
Believed to be a splinter group of Anonymous, they often post taunting or mocking messages to corporations and agencies they have compromised

Source: Lulz Security, Anonews.org, news reports *Actual date

REUTERS

https://www.networkworld.com/news/2011/120111-security-snafus-253649.html

New Technologies (outline)

- New devices on the network
  - Smartphones, tablets, electric meters, etc.
  - Device controllers (PLCs never meant to be on net)
- IPv6
- Cloud computing and SDN
- Distributed ID management

New Issues (Mobile Devices)

- Have gone from thin client to thick client
  - Unknown applications have significant access
  - Enterprise data stored on mobile device
- Non-enterprise owned devices so no control
  - How to verify configuration and patch level
- Travel from network to network
  - No network perimeter
- Security fixes difficult to roll out (e. g. Android)
  - Google-> Manufacturer -> Service Provider -> User

New Issues (PLC Controllers)

- Were never designed to be on the Internet
- Companies claim they are not; pen testers always find them
- Back doors, default passwords, vuln applications
- Difficult/impossible to update software
  - No test capability
  - Too important to fail due to an update
  - No upgrade process
  - https://www.networkworld.com/news/2012/041612-embedded-system-security-much-more-258318.html

New Issues (IPv6)

- Incomplete specification
  - Implementation mismatches
  - Device authentication not implemented
  - Implementations incomplete (= doesn't crash)
- Learning curve (developers and engineers)
- Dual stack with IPv4
  - Increased complexity
  - Tunneling eases IDS/Firewall bypass
- http://gcn.com/articles/2012/02/29/rsa-12-ipv6-security.aspx

New Issues (Cloud and SDN)

- New models of cyber security http://www.rationalsurvivability.com/blog/2012/03/security-as-a-service-the-cloud-why-its-a-net-security-win/
- Software Defined/Self Defended Networks (SDN) http://www.rationalsurvivability.com/blog/2011/10/the-killer-app-for-openflow-and-sdn-security/
- Hard to audit vendors' security vulnerabilities http://www.contextis.com/research/white-papers/assessing-cloud-node-security/

New Issues (ID Management)

- Allows password AND id reuse between sites offering many levels of service – vastly simplifies targeted attacks on your site
- Insecure passwords and PINs still common so lateral movement is eased
- Decreased trust in id management services
- Users are asked to make security decisions beyond their capability/training to judge risks

Are Things Really That Bad?

- Richard Bejtlich, chief security officer at Mandiant, a computer-security company, … 94% of the targeted companies didn't realize they had been breached until someone else told them. The median number of days between the start of an intrusion and its detection was 416, or more than a year ….
- Shawn Henry, former top cyber cop for the FBI said, "I don't see how we ever come out of this without changes in technology or changes in behavior, because with the status quo, it's an unsustainable model. Unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security,"
- http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html

What to Do?

- Can't continue & expect a different outcome
  - Rethink IT services based on enterprise priority
  - Rethink cyber security policies
  - Rethink network architecture
  - Rethink service provisioning and virtualization
  - Rethink ID management and authentication
  - Train employees
    - Data sensitivity
    - Safe computing

The Old Stuff

- Still have to manage and patch vulnerabilities
- https://www.zdnet.com/blog/security/kaspersky-mac-market-share-means-more-malware/11642
- Change default passwords
- Follow configuration best practices
  - Eliminate or block unneeded services
  - Limit ability for lateral movement by attacker
  - Strictly limit sudo/root and admin privileges
  - Good anti-virus software with frequent updates
- Follow application secure coding practices https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

1 - Inventory

- Perform Business Impact Assessment
  - Not a new requirement but few have done it
- What IT services are required to support the Enterprise services?
- Don’t forget external services
- Prioritize – but don’t make it too fine-grained (3-5 categories)

2 – Cyber Policies

- Ensure the important things are protected to a consistent level – Confidentiality, Integrity, Availability
- Develop policies, procedures, and both a sanction process and an exception process so people know what is expected and can appeal in exceptional cases – based on risk assessment with controls tailored to the service requirements
- Make the policies clear but flexible enough to adapt to new circumstances and technologies

3 – Network Architecture

- Track the current best practice suggestions for IPv6 implementation http://www.si6networks.com/presentations/HES2012/fgont-hes2012-recent-advances-in-ipv6-security.pdf
- The new perimeter is around the servers and associated infrastructure
- Access privileges are granted based on all of:
  - Who (and strength of authentication)
  - Where (is network you are on)
  - How (much do we know about the device)
- Assume: user device is compromised http://blog.ismaelvalenzuela.com/2011/09/16/when-prevention-fails-extending-ir-and-digital-forensics-to-the-corporate-network-slides-from-sans-boston-2011/
  - Highly limit direct access – require multifactor authentication
  - Use gateways, proxies, portals and VDI
  - Intensive logging and log correlation software is critical
  - Full packet capture should be architected for all but the highest speed data transfer paths

4 – Service Delivery

- Increased use of virtualization
  - Simplicity and complexity tradeoffs
  - Virtual servers – create on demand from a known, secure configuration
  - VDI (e. g. NX) isolates from untrusted systems
- If possible, provide a private cloud service
  - Keeps critical services in-house
  - Decreased complexity of additional external providers
  - Amazon is trying to make this difficult to justify

5 – Id Management

- Accept a variety of authentication methods https://cdsweb.cern.ch/record/1442597
- Assign Level of Assurance to different methods of authentication, e. g.
  - Google or Facebook – visitor wireless access
  - Locally registered userid/password – internal web
  - Multifactor from registered, maintained device on enterprise network – sensitive information
- Track developing LoA standards
- Carefully track roles and responsibilities – also require periodic privilege authorization

6 – Training

- Develop clear data classification policies and handling procedures; and make sure everyone knows and can easily find them
- Users are the first line of defense (and attack). They need to know what actions put the enterprise at risk
  - Poor passwords an password reuse across multiple sites
  - Social engineering
    - Clicking links in emails; Social networking scams
    - http://blog.trendmicro.com/bogus-olympics-2012-email-warning-blindside-users-with-malware/
    - Phone calls from "the help desk" or from "Microsoft" http://blog.eset.com/2012/04/18/how-to-recognize-a-pc-support-scam
    - Fake anti-virus alerts
  - Poorly configured or unpatched systems; public kiosks
  - Flash drives
  - Browsing unsafe websites

Human v 1.1

Hotfix patch

- dislodged eyelashes will no longer enter eyeball area and become inaccessible

- random cheek and tongue biting issue during food consumption fixed

- memory leak patched, should fix the "enter room and forget why" and item misplacement issues

- fixed a bug where the motivation module would randomly fail to load

http://www.edugeek.net/forums/jokes-interweb-things/72521-human-v-1-1-hotfix-patch.html

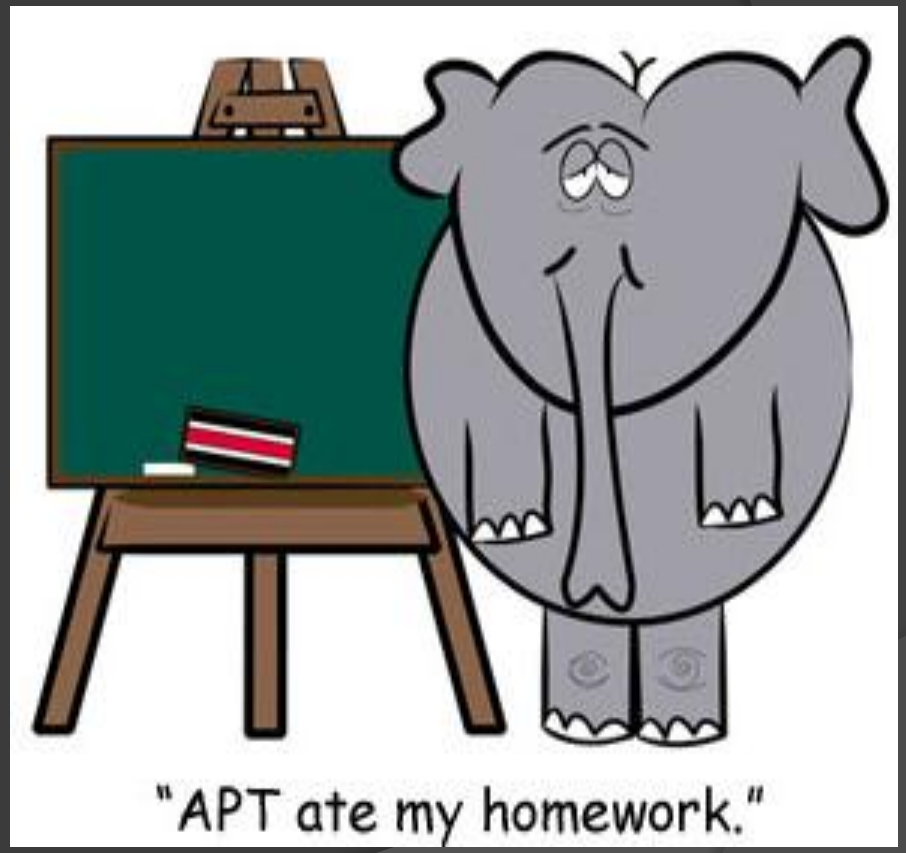
http://www.google.cz/imgres?imgurl=http://rlv.zcache.com/we_need_a_patch_for_human_stupidity_magnet-p147591607888353917z8x0x_400.jpg&imgrefurl=http://www.zazzle.com/we_need_a_patch_for_human_stupidity_magnet-147591607888353917&usg=__Rqm5tzoX8Dcbp1cxPrUym1YUjp8=&h=400&w=400&sz=33&hl=en&start=2&zoom=1&tbnid=sKeVC1BuZn4SvM:&tbnh=124&tbnw=124&ei=lkiVT-y2IMjjtQby6ZSMBA&um=1&itbs=1

Cyber Defense Against Cyberwar

- "While there is no entity that can bail out the Internet, there is no meaningful country that is not today researching ways to disrupt the Internet use of its potential adversaries. The most a country can hope to do is to preserve the Internet interior to itself."
  - Dan Geer speaking at 2012 SOURCE Boston
- maintaining redundancy – backup systems and manual processes – is necessary to not only secure the nation's critical infrastructure, but also to provide the necessary fallback mechanisms for the country to run properly in the event of a catastrophic Internet disruption.
- **On Sunday 22APR2012, Iran unplugged oil export facility from the Internet due to a cyberattack** http://abcnews.go.com/Technology/wireStory/report-iran-unplugs-oil-facilities-internet-16194653

No One Wants Our Science Data

- Bzzzzzt! Yes, they do!
- Three US DOE research labs hacked last year; had to drop off the Internet several weeks
- Attackers were attempting to exfiltrate unclassified but unpublished research data
- Initial entry via phishing or unpatched web app.
- Present a month before noticed
- Can your institute operate w/o Internet access? What sequence of actions would you take to restore service?



Embedded Computers Everywhere

- Misconfiguration provides attacker entry
  - Pen testers commonly use printers to gain access
  - PLCs are often insecure (and difficult *to* secure)
- Losing control of personal and enterprise data
  - Need to protect hard drives in copiers, printers, fax machines (repairs, too)
  - Mobile phones and tablets contain a volumes of data – email, attachments, photos, call records, location records, Wi-Fi access points
  - Many more devices with flash memory coming soon

Hacktivism

- Will increase and lead to more DDOS and credential leakage
- Prepare in advance for DDOS response – may affect a single server or impact the ISP http://www.secureworks.com/assets/pdf-store/articles/Understanding_and_Combating_DDoS_Attacks.pdf
- Millions of credentials leaked – service can alert individuals and companies http://pwnedlist.com
- Password manager software and multifactor authentication also help

Turn the Tables

- Remember – attacker needs only one mistake to penetrate your defenses
  - Impossible to be perfect
  - An adversary targeting you will always win
  - Nissan is the latest to admit they have been hacked http://bits.blogs.nytimes.com/2012/04/24/nissan-is-latest-company-to-get-hacked/
- Alter rules of the game
  - Log correlation software is crucial – as are human log reviewers
  - Find the attacker when they make their mistake and reveal their presence
  - Use tools like Hone (released 11APR2012) from PNNL http://gcn.com/articles/2012/05/07/feature-1-tool-spots-net-breach-sidebar.aspx google "hone pnnl" – 6th result
  - http://splunk-base.splunk.com/apps/45784/security-onion

Summary 2012 ++

- Business Impact and risk management is required to contain the costs
- Change the game on the attackers! Don't just wait to be attacked … defenders should model their organization's threats, gather intelligence and correlate the data to pinpoint possible threats. …employ… tactics, such as network canaries … to better understand attackers. http://www.sourceconference.com/publications/bos12pubs/Jackson%20-Incident%20Detection%20MacGyver%20Style%20SOURCEBoston%202012.ppt
- Assume you are pwned – now find them

  Enterprises need to be hunting inside the network perimeter. Information sharing of events and key indicators is critical

Questions?

Recent security conference – SOURCE Boston 2012

http://www.sourceconference.com/boston/speakers_2012.asp