SecureWorks University

Engineering Lessons Applied to IT Security

Vern Williams

Engineering Lessons Applied to IT Security

Vern Williams

SecureWorks University

Presenter

Vern Williams, MSIS

Director of External Security Education, Dell Secureworks University

CISSP, CSSLP, ISSEP, CBCP, ISAM

ISSA Distinguished Fellow

IEEE Senior Member

512.297.8798

VWilliams@SecureWorks.com

- 20 years driving nuclear subs for U.S. Navy
- Over 20 years in information security

Agenda

SecureWorks University

- Introduction
- Engineering failure and lessons learned
  - USS Thresher
  - Galloping Gurtie
  - Challenger
- Application to our world
- Basic tenets of security
  - People
  - Process
  - Products
- Building blocks
  - Identity management
  - Defense in depth
  - Change management

Engineering Failures

SecureWorks University

- **USS Thresher**

  April 10, 1963, loss of the USS Thresher with all hands during sea trials following a shipyard maintenance period

- **Galloping Gurtie**

  November 7, 1940, failure of the Tacoma Narrows Bridge after being in service for only four months

- **Challenger**

  January 28, 1986, the space shuttle Challenger was destroyed 73 seconds after liftoff when rocket booster seal failed, leading to a subsequent fireball and the deaths of all seven astronauts aboard

USS Thresher (SSN-593)

SecureWorks University

- The submarine sank on April 10, 1963, about 220 miles east of Boston. All aboard were lost: 16 officers, 96 enlisted men and 21 civilians
- Scenario
  - Conducting deep dive after after overhaul
  - Flooding in engine room from failed braze sprays electrical equipment
  - Reactor is shut down and steam stops shut by procedure
  - Emergency blow initiated and moisture in air flasks freezes and blow stops
  - With no propulsion or buoyancy, ship sinks below crush depth and implodes
- Loss
  - Ship with all hands and shipyard personnel
  - All engineers on passive ranging system

All photos in public domain

USS Thresher : Lessons Learned

SecureWorks University

- Engineering, design, and construction defects in both nuclear and non-nuclear systems can affect the safety or integrity of the entire system
- Standards selected for a task should not be overridden by the lack of time and resources. Selecting the easy standard to save time and money increased the probability of a failed weld.
- Communication of near-miss events by management helps to resolve weaknesses or flaws that, in future events, could prove tragic
- Procurement of equipment and components must be checked upon receipt as well as tested under operating conditions to verify suitability
- SUBSAFE program implemented
- Operating procedures need to be written with the “big picture” in mind
- Key assets need to be protected from a single casualty eliminating them

Applied to IT Security

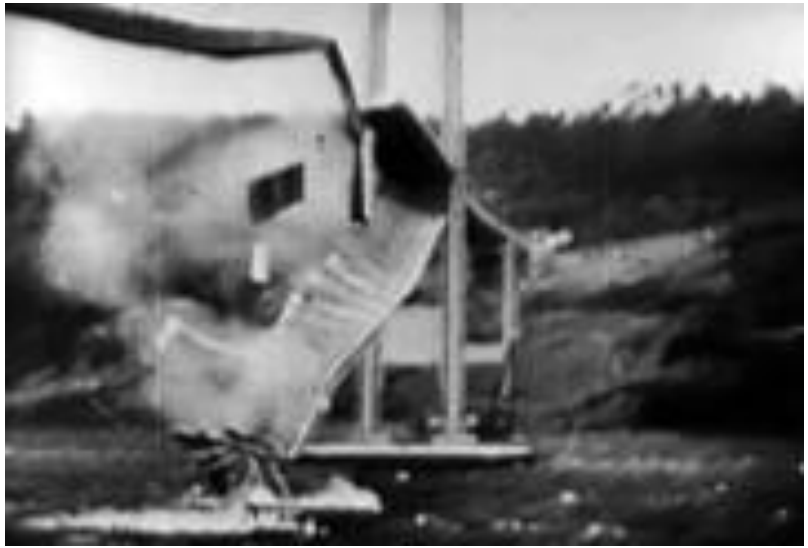
SecureWorks University

- A single vulnerability can compromise your system (weak link theory)
- Testing is essential for getting the correct outcome.
  - Start early
  - Do not short change it when schedules are tight
- Experience gained from close calls for one project or organization can help avoid failures for others
- Good supply chain management helps ensure that you get the "real" product whether hardware or software
- A company can recover from loss of a computer or even its datacenter if it has planned ahead (disaster recovery planning), but a plane crash with all of your "key players" may well be fatal for a company

Tacoma Narrows Bridge

SecureWorks University

- Stiffening the bridge with only eight-foot deep plate girders, instead of the 25-foot deep trusses proposed by the Dept. of Highways weakened the structure to save approximately $3 million to $4 million
- New designs and methods should be introduced incrementally, especially when safety-of-life issues are at stake
  - Ratio of width to length broke new ground
- Wind tunnel testing of new designs or new technology needs to be thorough
- Listen to the one engineer who sees the problem. Group think is dangerous.



All photos in public domain

Architects Learned from the Mistakes

"... the Tacoma Narrows bridge failure has given us invaluable information ... It has shown [that] every new structure which projects into new fields of magnitude involves new problems for the solution of which neither theory nor practical experience furnish an adequate guide. It is then that we must rely largely on judgment and if, as a result, errors or failures occur, we must accept them as a price for human progress."

- Othmar H. Ammann, Theodore von Kármán and Glenn B. Woodruff. The Failure of the Tacoma Narrows Bridge, a report to the administrator. Report of the Federal Works Agency, Washington, 1941

"The entire engineering community learned about issues related to poor aerodynamic performance," says Manuel Rondón, Bechtel's project manager for the Tacoma Narrows project. "Designing for wind loads is something we take for granted today." What is the potential cost of failure to mitigate risk?

Professionalism in IT Security

SecureWorks University

- How do we ensure "lessons learned" from security failures are passed to IA Practitioners?
  - Issues change much quicker than in "Architecture"
  - No source degree program for IA, but do we want one?
  - Accreditation is a complex problem with no easy solution
- Who sets the standards of practice for the security profession?
  - Where do we go for a "Standard"?
    - ISO, NIST, NERC, ISA, PCI?
  - Credentialing? by whom? Feds? States? CPAs?

Space Shuttle Challenger

SecureWorks University

- Several engineers — most notably Roger Boisjoly, who had voiced similar concerns previously — expressed their concern about the effect of the temperature on the resilience of the rubber O-rings that sealed the joints of the solid rocket boosters
- Thiokol engineers argued that if the O-rings were colder than 53° F (12° C), they did not have enough data to determine whether the joint would seal properly
- The O-rings failed and, as a result, the Space Shuttle Challenger was torn apart

Challenger Lessons Learned

SecureWorks University

"...failures in communication... resulted in a decision to launch 51-L based on incomplete and sometimes misleading information, a conflict between engineering data and management judgments, and a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers."

- Report of the Presidential Commission on the Space Shuttle *Challenger* Accident

Application to the Security Domain

SecureWorks University

- Enterprise-wide view coupled with attention to detail are critical in securing the enterprise data and systems
- Supply chain management is essential if you are to rely on a component
- Change management is the only way to keep your environment securable or manageable
- To have accountability, you have to be able to trace actions to identities
- Before you can rely on it, you have to test it
- Lessons learned need to be applied throughout the security profession

How Can We Get There?

SecureWorks University

- Develop a culture of causality, configuration management, and compliance
- Identity management and least privilege
- Change management and white listing authorized software
- Consistent OS and applications baseline
- Intentionally designed infrastructure
- Do not let “new stuff” break what works

The Three *P*s

SecureWorks University

- **People**
  - Hire carefully
  - Train appropriately for assignment
  - Protect against loss of critical staff
  - Hold accountable
- **Process**
  - Establish good policy and procedures
  - Use baselines and change management
  - Use good engineering to implement effective controls
  - Audit to ensure compliance
- **Products**
  - New technology needs to be carefully evaluated
  - Ensure good supply chain management
  - Update processes integral to implementing new products

Building Blocks of Compliance

SecureWorks University

- Do the most important 4 things first
- Identity management
- Defense-in-depth
- Change management

The 4 Things to do FIRST!

SecureWorks University

- **Australian DSD listed 35 Strategies to Mitigate Targeted Cyber Intrusions**
- **Four are identified as stopping 85% of the intrusions**
  - Patch 3rd party applications
  - Patch operating systems

    (< 48 hrs after release for high risk vulnerabilities and update to current versions)
  - Minimize users with domain or local admin rights
  - Application whitelisting

Identity Management

SecureWorks University

- **Rigorous identity proofing**
  - Check and validate identification
  - Validate references, degrees and employers
- **Converged identity management**
  - Use Multi-Factor authentication
  - Issue credentials with manger approval and defined rights
  - Physical and logical access based on assigned roles
  - Linkage between location and access
  - Single point of revocation
- **Separation of duties**
  - Business decision
  - Implement in policy, manual systems, IT systems and disaster recovery planning
  - Use role-based access control (RBAC) to allocate rights

Defense-in-Depth

SecureWorks University

- Physical prevention and detection controls
- Perimeter cyber defenses
- Effective end-point protections
- Protect up to and including the application layer
- Intrusion detection
- Segment networks
- Protected enclaves
- Encryption of sensitive material at rest and in motion
- Effective response to intrusions

Change Control Axiom

SecureWorks University

- We do not have the time or money to do it right, but we do have the time and money to be hacked, recover from the damage, troubleshoot the original problem that we created when we misconfigured the device, and then do it right.

- So, how do we improve our chances of getting it right the first time?

Lessons from Rickover's Navy

SecureWorks University

- Paraphrase: If people care enough, they can do things perfectly. No one forgets to cash their paycheck, so they can do things related to nuclear reactors correctly.
- Even when your life is on the line, people make mistakes.
- If it is really important, train people on how to do it right, have someone who knows how to do it right watch you, and be accountable for indicating you did it right. Then, review the paperwork and evidence that it was done right. Submarine Quality Assurance program is an example.
- Keeping the water out of the people tank and the hackers out of your data are both important.

Change Control

SecureWorks University

- Change control has a significant impact on both security and IT management.
- Capability Maturity Model Integration (CMMI®) Level 2 enforces change management in the software development arena.
- What about the rest of the infrastructure?
- It is a difficult task to both improve control and not decrease responsiveness, but the best IT organizations get it done.
- Structure compliance from a strategic point of view, not a checklist
  - Use compliance to effect positive change in culture and practices
- Build security in (and early) to
  - Change management process
  - Software development projects
  - Acquisition, especially of new technologies

System Change Management

SecureWorks University

- Start with a stable systems configuration or baseline
- Maintains effectiveness of using tested operating system images (how else can you meet a 48 hour patch goal)
  - Helps deploy software updates or new software
- Virtualization is a double edged "sword"
  - Improves recovery of servers if compromised or destroyed
  - Especially important for Internet-facing servers on your firewall demilitarized zone (DMZ)
  - It is another layer of obfuscation and a layer to protect
- Controls on software installs help to protect against Malware (white list)

Culture of Causality

SecureWorks University

- "Things" happen for a reason; there is a cause
- Root cause analysis tells you what happened and is a start to preventing recurrence
- Holding people accountable requires:
  - Enforceable policies with penalties signed by the CEO or equivalent
  - Training and awareness to ensure that employees know what is required and how to accomplish it
  - Signed acknowledgment by employees is essential
  - Enforce penalties, especially for senior employees
- Accountability for actions requires traceability and non-repudiation for actions

Resources

SecureWorks University

- US-CERT Control Systems Security Program
  - http://www.us-cert.gov/control_systems/
- Top 35 Mitigation Strategies, Australia DSD
  - http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- "From Bridges and Rockets, Lessons for Software Systems", C. Michael Holloway; NASA Langley Research Center; Hampton, Virginia, Proceedings of the 17th International System Safety Conference, August 1999, pp. 598-607,
  - http://shemesh.larc.nasa.gov/people/cmh/ISSC99/cmh-issc-lessons.pdf
- National Security Agency (NSA) and Department of Defense (DoD) Security Technical Implementation Guides (STIGS)
  - http://iase.disa.mil/stigs/stig/index.html
- "Visible Ops Security"
  - www.itpi.org
- Center for Internet Security
  - www.cisecurity.com
- Security-Related Associations: SANS, ISSA, ASIS, ISACA, ISC2 and ACP
  - www.sans.org, www.issa.org, www.asisonline.org, www.isaca.org, www.isc2.org, www.drii.org

Questions?

SecureWorks University

Vern Williams, MSIS

Director of External Security Education, Dell Secureworks University

CISSP, ISSEP, CBCP, CSSLP, ISAM

Distinguished Fellow, ISSA (Information Systems Security Association, International)
Senior Member, IEEE (Institute of Electrical and Electronics Engineers)
ISSA International Honor Roll, 2007
ISSA Security Practitioner of the Year, 2005

512.297.8798 (mobile)

VWilliams@SecureWorks.com

DELL SecureWorks