An Industry Perspective on Cybersecurity

Steven B. Lipner
Senior Director of Security Engineering Strategy
Trustworthy Computing
Microsoft Corporation
Redmond, WA
slipner@microsoft.com

Historical Perspective on Cybersecurity

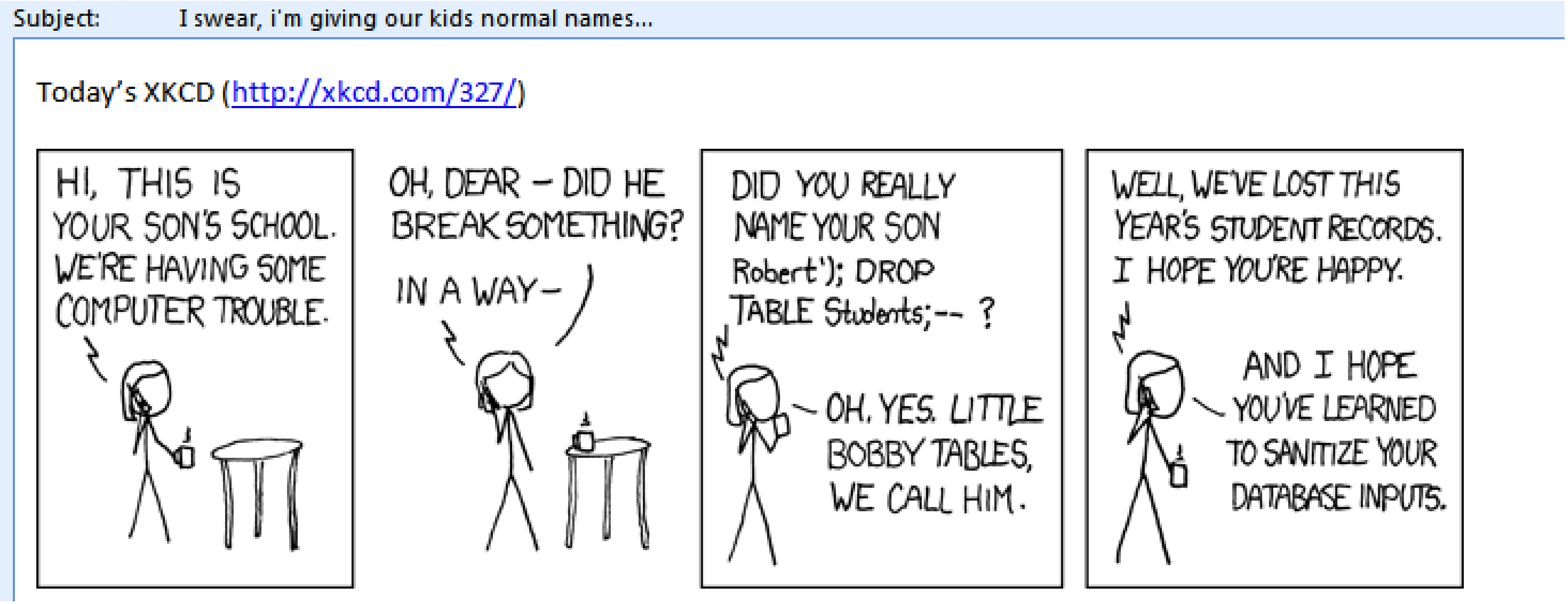
- We’ll build a system, prove it’s secure and we’ll be done… (1975)
- We’ll have the government evaluate our products (1985)
- We’ll build a secure firewall, run antivirus, lock down our systems, and our systems will be protected (1993)
- We’ll issue patches and protect our users (1999)
- We’ll integrate security into our development process (2002)
- We’ll integrate security into our development process, issue patches, build a secure firewall, run antivirus, lock down our systems, have the government evaluate our products, and devise new tools and techniques (2009)…

…and we’ll never be “finished”

Today's Landscape

- (Many) vendors put significant effort into building products that can resist attack
- In the Internet environment there is a significant amount of well-engineered malicious software
- The underlying problem is that software is not perfect – and the attacker must search for ***a*** vulnerability while the defender must find ***every*** vulnerability
- Vulnerability refers to design and coding errors
  - Buffer overruns in C/C++ programs
  - SQL injection errors in web applications
  - And many others

SQL Injection



Subject: I swear, i'm giving our kids normal names...

Today's XKCD (http://xkcd.com/327/)

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Realities of Cybersecurity

- Security, unlike other aspects of science and engineering, is about attack and defense (or attackers and defenders)
  - We identify specific problems (vulnerabilities) and (try to) remove them
  - Attacker’s job is to identify and exploit a new vulnerability that we didn’t think of – or didn’t remove
- Security is “in the weeds”
  - Principles and models can help
  - If the details aren’t correct, the defender loses
- Invention of new classes of attack is fairly common

Approaches to Building More Secure Systems

- Secure by design – enumerate the points where someone might attack and ensure that there are countermeasures
  - Exposed network communication -> encrypted protocols
  - Software that takes external input -> robust input validation, use of code analysis and testing tools
- Secure by default
  - Least privilege – run components so the effects of failures are isolated or bounded
  - Frustrate attacks – non-executable memory, address space randomization
- Secure in deployment
  - Ship systems in "locked down" configurations

NIST and Cybersecurity

- NIST efforts in cybersecurity date to at least 1972
- NIST focus on security for unclassified/civil government always collaborative with industry
  - DES
  - Risk Management guidance
- Computer Security Act formalized NIST role – and fragmented the government's approach to cybersecurity
- Sometimes contentious relationship with national security/classified world
- Always valued by vendors and private sector
- Frequent owner of tasks from OMB and Congress

The Security Research Community

- Players on the cybersecurity “research” stage
  - Academics and theoreticians
  - Developers of secure products, security products, tools
  - End user organizations (government and commercial)
  - Vulnerability finders
- NIST widely respected by the community
  - Theoretical research programs
  - Security development processes, concepts, metrics
  - Guidance programs
  - National Vulnerability Database

NIST Contributions

- Too numerous to list…
- Unclassified/commercial encryption standards
  - From DES to FIPS-140 to AES to SHA-3
- Security management guidance
  - FISMA standards and guidelines (but see below)
- National Vulnerability Database
- Identity standards for strong user identification and authentication (PIV card/FIPS-201)
- Configuration standards (FDCC)

Perspectives on NIST and Cybersecurity

- Computer security efforts at NIST are healthiest in my experience (1972-2009)
  - Best management
  - No longer (badly) underfunded
  - Collaborating across government
  - Bringing real-world perspective to problems
  - Integrating outside expertise
- Cybersecurity extends across IT Lab
  - Secure networking
  - Secure development
- Still more to do – important to maintain focus and resourcing

Recommendations

- Integrate attacker perspective
  - Initial FISMA guidance lost sight of this principle
  - Updated version better
- Tackle important hard problems
  - Measuring security
    - Project is under way –may be impossible, but worth trying
  - Cloud security
  - Electronic medical records
  - Smart grid
  - Operational security management – build on success of FDCC
  - Trusted User Experience
  - Building a more authenticated/accountable Internet

Recommendations

- Maintain robust links to the security community
  - Recognize diversity of stakeholders
  - Seek inputs on plans, programs, products
- Seek real-world perspective and balance
  - Supply chain security
  - Security assurance case
- Speak up where your voice is needed
  - Common Criteria for security evaluation needs active NIST participation