Application Security: A Summary and Some Thoughts about Costs

NIST Forum

April 12, 2011

Discussion Questions (what did we learn?)

- What is an application?
- What does application security mean?
- What does it cost to write software?
- What does it cost to test software?
- What does it cost to write/test secure software?
- What does it cost to “bolt it on” vs “bake it in”?
- What does it cost to recover from compromised software?

What is an Application?

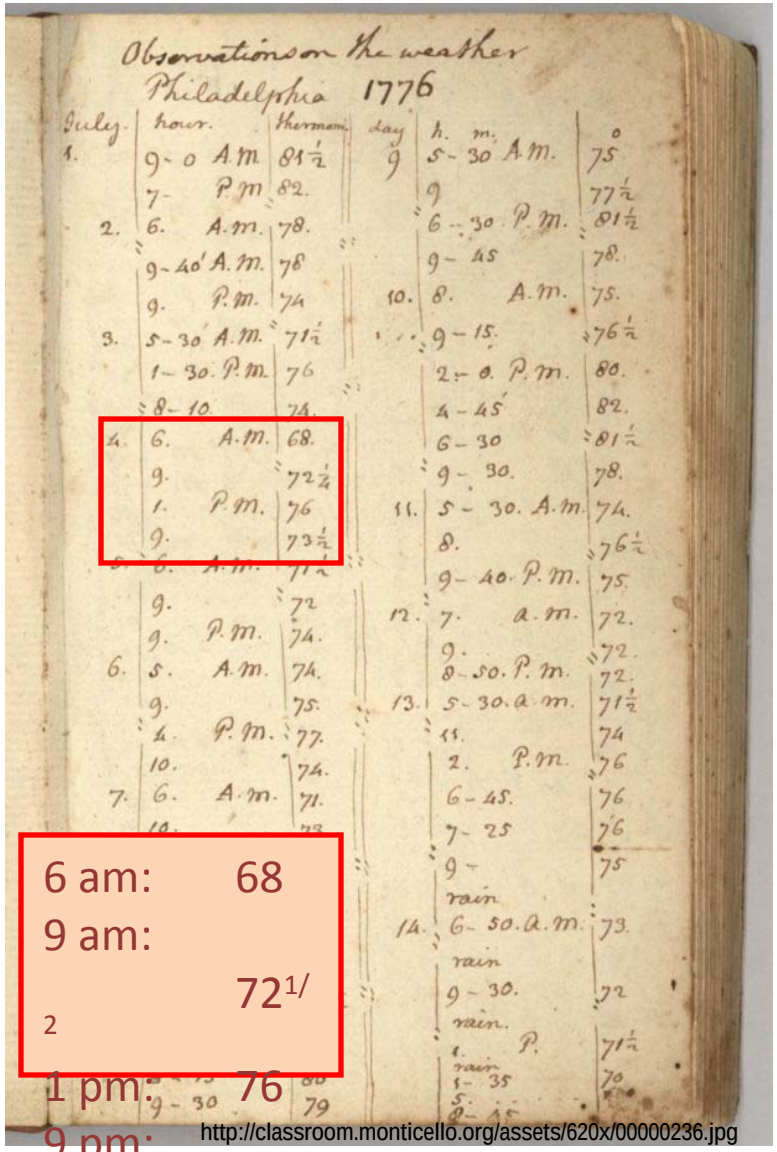
- Application
  - Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An Application runs on one or more Servers or Clients. (ITIL® V3 Glossary, v01, 30 May 2007)
  - OSI Model: The Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. (Wikipedia)
    - This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model.
    - Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.
    - When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit.
    - When determining resource availability, the application layer must decide whether sufficient network or the requested communication exist.
    - In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.
  - Is OSI model still current/relevant?

What is an Application?

- NIST guidance: The terms “Application” and “Software” are not defined in current NIST publications, yet both are used extensively throughout all NIST publications
- NIST guidance provides ready access to the statutory definitions for:
- Information Technology [40 U.S.C., Sec. 1401]:
  - Any equipment or interconnected system or subsystem of equipment that is used in the **automatic** acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
  - For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
  - The term information technology includes computers, ancillary equipment, **software**, firmware, and similar procedures, services (including support services), and related resources.
- Information System [44 U.S.C., Sec. 3502]:
  - A discrete set of information resources organized for the **collection, processing, maintenance, use, sharing, dissemination, or disposition** of information.
  - [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

What is an Application?

- Go back to ITIL: “Software that provides Functions”
  - Different from the Operating System software that enables the server or router to Operate, that is, “to perform as expected.” (ITIL)
- Working definition: An application is software that defines/performs the function of the information system
  - Example: NOAA Environmental Satellite Processing System (ESPC): ingest, process, distribute satellite data ,and products derived from that data, from other information systems, to other information systems and end users.
    - We operate Linux and Windows servers to process satellite data using commercial and custom-developed applications.
    - Same Linux/Windows servers could process financial or human resources data, with different applications software
- Without the application, we cannot perform our business functions (in an automated way…)



http://classroom.monticello.org/assets/620x/00000236.jpg

What does Application Security mean?

- Adequate Security
  - Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
- Application Security
  - Encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application. (Wikipedia, courtesy of David Fletcher)
  - “Design and implementation assurance addresses whether the features of a system, application, or component meets security requirements and specifications and whether they are well designed and well built. “ (NIST SP 800-12, October 1995)
- Measures taken to ensure the function(s) of the information system continue without, or survive through, the loss, misuse, or unauthorized access to or modification of information.
  - Can it be broken?
  - Can it survive the breaking?
  - Can we recover/repair/replace the information and/or the components?
- Applications & Operating Systems are different, yet have similar needs
  - Patching/maintenance cycles, documentation, interactions with other components

Who does Application Security? (NIST SP 800-37)

- Software applications depend on the resources provided by the **hosting information system** and as such, can take advantage of (i.e., leverage) the security controls provided by the system to help provide a foundational level of protection for the hosted applications, when this type of inheritance is applicable.
- Additional application-level security controls are provided by the **respective software applications**, as needed.
- **Organizations** ensure that all security controls, including application-level controls employed in separate software applications, are managed and tracked on an ongoing basis.
- **Application owners** coordinate with information system owners to ensure that information security and risk management activities are carried out as seamlessly as possible among applications and hosting systems.

Who does Application Security? (NIST SP 800-64)

- The **[Software] developer** is responsible for programmatic coding regarding applications, software, and Internet/intranet sites, including “secure coding,” as well as coordinating and working with the Configuration Management (CM) manager to identify, resolve, and implement controls and other CM issues.
- Primary responsibility for application security, during early phases, lies in the hands of the **development team** who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. They are the first level of defense and opportunity to build in security. It is important that their role not be assumed or diminished.
- Providing application security training to the development and testing teams will increase understanding of the issues and techniques and should enable the development of more secure systems. If developers are aware of what to look for and what to test during the development phase, the number of security defects developed and released to quality assurance (QA) should be reduced.
- In addition, if the **QA test team** is well educated in the area of application security, they are more likely to identify a security issue before the product is moved on to the next phase of testing. Such training should result in greater confidence in the overall security of the production system. Providing training in application security will also emphasize the importance of application security to the team.
- **(Who provides the training?)**

What does Application Security cost?

- What does it cost to write software?
- What does it cost to test software?
- What does it cost to write/test secure software?
- What does it cost to “bolt it on” vs “bake it in”?
- People, process, technology costs
  - Project teams, training, meetings & documentation, code reviews, tools, component refresh …
- Can we answer these questions?

What does incomplete Application Security cost?

- What does it cost to recover from compromised software?
  - PII system with 1K records, 10K, 100K?
  - Sensitive information loss to a competitor?
  - Complete loss of system availability?
- Ponemon/Symantec "2010 Annual Study: U.S. Cost of a Data Breach"*
  - Benchmark study of 51 companies; 1000 – 100K records; primarily PII
  - Considers several factors, including criminal activity, negligence, system failures;
- Ponemon: In 2010, companies more vigilant about preventing systems failures
  - The number of breaches caused by systems failures dropped 9 points in 2010 to 27 percent.
  - Breaches from systems failures averaged **$210**, up $44 (27 percent).
  - The noticeable drop in breaches from systems failures may point to organizations becoming more conscientious in ensuring their systems can help prevent and mitigate breaches (through new security technologies and/or compliance with security policies and regulations)

PII system failure costs		
# of Records	Cost	What could I buy?
1,000	$210,000.00	
10,000	$2,100,000.00	
100,000	$21,000,000.00	

* http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

What does incomplete Application Security cost?

- Prius 2005 recall
  - A software problem is causing some Toyota Prius gas-electric hybrid cars to stall or shut down while driving at highway speeds, according to a published report.
  - 23,900 cars affected; 1-hour software update required to correct
  - Working Approximate Guess: $100/hr at the dealer = $2,390,000.00
  - **Automobile as Industrial Control System (ICS)**
- Prius 2010 recall
  - "Toyota has acknowledged previously that the event data recorders are not accurate," said Takeshi Uchiyamada, executive vice president in charge of research and development. "We have been able to determine that there is no defect in the event data recorders."
  - But, "we have found that there was a software bug in the event data recorder readers that download data. The bug had to do with data that indicated speed," he said. The issue was discovered this past spring and has since been corrected.
  - Estimates between $2 billion and $5 billion
- "I hope I'm not writing a blog five years hence about a 2015 Toyota Prius bug!" (Toyota owner blog)

http://money.cnn.com/2005/05/16/Autos/prius_computer/index.htm?cnn=yes
http://www.cadence.com/Community/blogs/ii/archive/2010/02/12/toyota-prius-2005-an-early-warning-about-verification.aspx
http://www.autoweek.com/article/20100914/CARNEWS/100919945#ixzz1JHXYin8Q
http://www.msnbc.msn.com/id/35893905/ns/business-autos/

What does incomplete Application Security cost?

- Intelsat's Galaxy 15 telecommunications satellite
  - rendered unable to take commands by an electrostatic discharge that fouled its onboard software
  - remained electrically active while adrift in orbit for more than eight months; interference (availability) threat to other satellites
  - recovered when it lost attitude control and reset, allowing controllers to restore commanding functions
- Intelsat and Orbital designed three software "patches" to prevent recurrence of the problem on Galaxy 15 or any other Orbital-built satellite that uses the same platform
  - software uploads mainly designed to ensure satellite will respond to commands even if a similar electrostatic discharge occurs
  - communications payload will automatically shut down if it has not received specific ground commands within a 21-day period.
- "satellites like Galaxy 15 today cost $250 million to build, launch and insure, but the satellite probably cost less when it was launched in 2005."
- 8 months of lost revenue for Intelsat = ???
- Orbital Satellites – estimated loss of $3+ million; separate $7 million payment (insured)
- Satellite also supported FAA Wide Area Augmentation System (WAAS)

http://www.msnbc.msn.com/id/41065770/ns/technology_and_science-space/#
http://www.satnews.com/cgi-bin/story.cgi?number=1534047477
http://www.msnbc.msn.com/id/37086846/ns/technology_and_science-space/
http://www.nsr.com/index.php?option=com_content&view=article&id=355:does-the-imminent-galaxy-15-failure-cast-doubt-on-the-hosted-payload-proposition&catid=94:industry-updates-2010&Itemid=153
http://www.spacenews.com/satellite_telecom/100722-orbitals-revenue-rises-earnings-fall.html