Integrating Systems Engineering & Information Systems Security Engineering Processes

23 April 2007

Rosaly Lam

Agenda

- Greetings (Audience Introduction)
- Project Introduction
- Information Assurance Concept
- The Role of Systems Engineering in Information Security
- The Cost of separating SE from ISSE
- Integrating SE with ISSE during Information Systems Development
- Conclusion
- References

Project Introduction

- My Background & Work projects
- Project Introduction:
  - The next two charts illustrate the increasing trend of information security attacks
    - Internet users are vulnerable to attacks

Web Hacking Statistics

Web Hacking Statistics – Incidents per Year (Last Updated 18 April 2007)
(Reference: http://www.webappsec.org/projects/whid/statistics.shtml)

Year	Count
1999	1
2000	5
2001	6
2002	4
2003	9
2004	17
2005	60
2006	44
2007	14

Note:
The database tracks only media reported security incidents that can be associated with a web application security vulnerability.

SAN'S Top 20 Internet Security Attack Targets (2006)

Operating Systems
- W1. Internet Explorer
- W2. Windows Libraries
- W3. Microsoft Office
- W4. Windows Services
- W5. Windows Configuration Weaknesses
- M1. Mac OS X
- U1. UNIX Configuration Weaknesses

Cross-Platform Applications
- C1 Web Applications
- C2. Database Software
- C3. P2P File Sharing Applications
- C4 Instant Messaging
- C5. Media Players
- C6. DNS Servers
- C7. Backup Software
- C8. Security, Enterprise, and Directory Management Servers

Network Devices
- N1. VoIP Servers and Phones
- N2. Network and Other Devices Common Configuration Weaknesses

Security Policy and Personnel
- H1. Excessive User Rights and Unauthorized Devices
- H2. Users (Phishing/Spear Phishing)

Information Security Concept (1)

- **Definition:**
  - Information Security is the process to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of data access, and unauthorized disclosure of information.

Information Security Concept (2)

- **Information Security Triad (CIA):**
  - **Confidentiality**
    - Protection of information from unauthorized access, regardless of where the information resides or how it is stored
  - **Integrity**
    - Protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes
  - **Availability**
    - Assurance that the information and resources are accessible by authorized users as needed

IA and ISSE

- **Information Assurance (IA)**
  - Used mostly by the commercial industry to describe the process to build information security systems
- **Information Systems Security Engineering (ISSE)**
  - Used by government agencies, specifically, the Department of Defense (DoD) to describe the process of discovering and meting the user's information protection Needs
  - ISSE Processes close resemble SE processes

Elements of Information Assurance (1)

- **People**
  - Commitment from Senior-level management
  - Establishment of effective Information Security policies and procedures, assign roles and responsibilities
  - Commitment of resources, training of critical personnel and enforcement of personal accountability
- **Technology**
  - Establish effective policies and processes for technology acquisition
    - Include security policy
    - IA principles
    - System-level IA architectures and standards
    - Criteria for needed IA products

Elements of Information Assurance (2)

- **Operations**
  - Inspection
  - Protection
  - Detection
  - Reaction
    - Watch and Warn
    - Repair and Report
    - Pursue and Prosecute
  - Reflection

SE Role in Information System Development (1)

- **Requirement Analysis**
  - Translates the customer requirements into a set of product functions and performance requirements
  - Identifies the customer information requirements
- **Functional Analysis and Allocation**
  - Allocates identified needs to systems
  - Develops system context to identify the system environment and to show the allocation of system functions to that environment
  - Preliminary CONOPS

SE Role in Information System Development (2)

- **System Analysis**
  - Defines and refines user needs into technical requirements
  - Proves feasibility (or non-feasibility) of a specific approach given the current understanding of physical limitations
  - Evaluates the effect of decisions on cost, reliability, and performance
  - Provides progress measurement and assessment
  - Analyzes data obtained during verification activities
  - Analyzes design constraints and trade-offs, does detailed system design, and considers life-cycle support. The final detailed design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented
  - Performs trade-off analysis, benchmarks system throughput to ensure the system meets its requirements

SE Role in Information System Development (3)

- **System Integration**
  - Components are tested and evaluated
- **System Verification**
  - Examines how well the information system meets the needs of the mission

Disadvantages of Separating SE & ISSE (1)

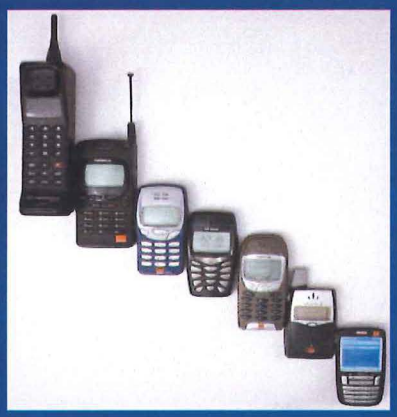
- **Cost of Implementing SE without ISSE**
  - SE are not experts in Information Security
  - Resulting system lacks sufficient built-in security measures
  - *Example: The Cellular Phone Evolution*

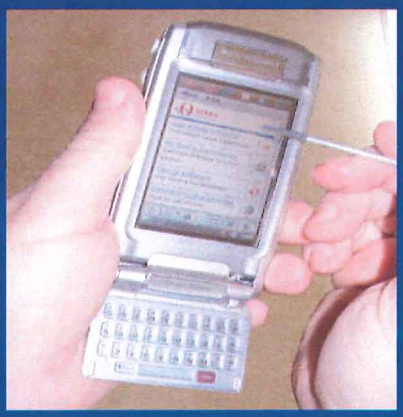
Disadvantages of Separating SE & ISSE (2)

- **Cost of implementing ISSE without SE**
  - Five steps of IA (Inspection, Protection, Detection, Reaction, and Reflection) are typically performed by the IT organization, without consulting the SE
  - Requires additional equipment purchases or replacements, system redesign, impacting the system performance and ultimately creates an imbalance between performance and security
  - Depending on the size and sensitivity of the system, the cost of implementing ISSE after the development cycle has been completed could top millions of dollars.

Disadvantages of Separating SE & ISSE Example (1 of 3)

- **The Cellular Phone Evolution:**





Disadvantages of Separating SE & ISSE Example (2 of 3)

Evolving Functionality of the Phone:

- Transmit and Receive voice Data
- Transmit and Receive Text Data
  - *Vulnerable to Worms and Viruses*
- Fax files
- Camera
- Transmit & Receive pictures
- Download & upload data from/to PC
- MP3
- Browse the Internet
  - *Infected by Skulls Virus*
- Bluetooth connectivity
  - *Hijacked by Cabir Virus*
- Download GPS information
- Mini computer (Smartphone)
  - *As susceptible to attacks as a PC*

Disadvantages of Separating SE & ISSE Example (3 of 3)

- All this time, the Systems Engineers & designers only concentrated on improving the capabilities of the phone, not its security features, hence these phones were not guarded from viruses
- Had the Information Systems Security Engineers been involved, there would not have been any other capabilities except to transmit and receive voice data
- After the attacks, the users had to reload their equipments – this would be the cheapest way. The other option would be for the manufacturers to upgrade the phones with the new security features including software and hardware, which would increase the cost of the phones.
- Imagine applying this process to a much larger, more expensive and security sensitive information system. The cost penalty would be enormous.

ISSE Process in IS Development (1)

1. Discover Information Protection Needs

- Information System Security Engineer works with the customer to determine the needs for information protection
  - Assigning metrics for Harm to Information (HTI) and Potentially Harmful Events (PHE) to each information domain
  - IS Security Engineer and the customer apply confidentiality, integrity, availability, access control, identification and authentication (I&A), non-repudiation, and security management services to each information threat.

- ***This activity should be performed in parallel with the SE's Discover Needs activity***

ISSE Process in IS Development (2)

2. Define System Security Requirements

- Information Systems Security Engineer considers one or more solution sets
- ISSE supports SE to define the system security requirements, system security modes of operation, and system security performance measures
- ISSE allocates security functions to target or external systems
- ISSE identifies data flow and protection needs associated with these flows
- ISSE ensures that the solution set meets the mission or business security needs
- ISSE coordinates the system boundaries and ensures security risks are acceptable

- ***This activity should be performed in parallel with the SE's Define System Requirements activity***

ISSE Process in IS Development (3)

3. Design System Security Architecture

- ISSE works with SE to ensure the security requirements flow properly to the architecture and that the architecture decisions do not impede security
- Allocates security requirements to target and external systems and ensures that the external systems identified can support what is allocated to them
- ISSE identifies high-level security mechanism (e.g. encryption, digital signature) so that dependencies such as key management for encryption can be addressed and allocated

- ***This activity should be performed in parallel with the SE's Design System Architecture activity***

ISSE Process in IS Development (4)

4. Develop Detailed Security Design

- ISSE ensures compliance with the security architecture
- Performs trade-off studies
- Defines system security design elements:
  - Allocating security mechanism to system security design elements
  - Identifies candidate commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) security products
  - Identifies custom security products
  - Qualifies element and system interfaces (internal and external)
  - Develops Common Criteria Protection Profiles

- ***This activity should be performed in parallel with the SE's Develop Detail Design activity***

ISSE Processes in IS Development (5)

5. Implement System Security

The ISSE provides:

- Verification that the system as implemented does protect against the threats identified in the original threat assessment
- Tracking of , or participation in, application of information protection assurance mechanisms related to system implementation and testing practices
- Inputs to and review of evolving system life cycle support plans, operational procedures, and maintenance training materials
- A formal information protection assessment in preparation for the final system effectiveness assessment
- Participation in the multidisciplinary examination of all system issues

This activity should be integrated with the SE activity to acquire, integrate, configure, test, document, and train the users. It concludes with the final system effectiveness assessment

ISSE Processes in IS Development (6)

6. Assess Information Protection Effectiveness

This activity spans the entire SE/ISSE process:

- During the Discover Information Protection Needs phase:
  - Present an overview of the process
  - Summarize the Information model
  - Describe threats to the mission or business through information attacks
  - Establish security services to counter those threats and identify their relative importance to the customer
  - Obtain customer agreement on the conclusions of this activity as a basis for determining system security effectiveness
- During the Define System Security Requirements phase:
  - Ensure that the selected solution set meets the mission or business security needs
  - Coordinate the system boundaries
  - Present security context, security CONOPS, and system security requirements to the customer and gain their concurrence
  - Ensure that the project security risks are acceptable to the customer

ISSE Processes in IS Development (7)

6. Assess Information Protection Effectiveness (cont.)

- During the Design System Security Architecture Phase:
  - Begin the formal risk analysis process to ensure the selected security mechanisms provide the required security services and to explain to the customer how the security architecture meets the security requirements
- During the Develop Detailed Security Design Phase:
  - Review how well the selected security services and mechanisms counter the threats by performing an interdependency analysis to compare designed to effective security service strengths
  - The risk assessment results, particularly any mitigation needs and residual risk, will be documented and shared with the customer to obtain their concurrence
- During the Implement System Security Phase:
  - The risk analysis is concluded and updated
  - Strategies are developed for the mitigation of identified risks
  - Possible mission impacts are identified and advised to customer

Conclusion

- Information is important for an organization as well as an individual. It needs to be safeguarded.
- Information Security is the process to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of data access, and unauthorized disclosure of information
- Information Security is built on three elements: People, Technology, and Operations
- When building an Information System, SE and ISSE should be brought together to achieve maximum security while balancing performance, cost, and schedule.
  - Building IS without ISSE results in data loss, financial loss, or even national security threats. The costs could be over hundreds of millions of dollars.
  - Grafting on ISSE after the Information System has been built without consulting the SE could impact system performance while raising the cost of development.

Questions

References

- Jan Killmeyer Tudor, Information Security Architecture, Auerbach Publications, 2001
- Defense-in-Depth Information Assurance Technical Framework (IATF) Release 3.1 – September 2002
- Donald L. Pipkin, Information Security - Protecting the Global Enterprise, Prentice Hall PTR, 2000
- SE Handbook - http://ipds.msd.ray.com/IPDS_V2.2.3/se/enablers/secure/se_hndbk/index.htm
- Source: Computer Security Institute – Dollar Amount of Losses by Type - 2001 http:www.sgrm.com/art15.htm, 7/24/2006.
- Mark S. Friedman and Kristin Bissinger, "InfoJacking@: Crimes on the Information Superhighway!"

References

- Michael Smith. Darknets: Security's Bright Future.
  http://www.infosectoday.com/Articles/Darknets.htm
- The Role and Nature of Anti-Tamper Techniques in US Defense Acquisition
  http://www.findarticles.com/p/articles/mi_m0JZX/is_4_6/ai_78177436
- Defense Acquisition Guidebook (DAG)
  http://akss.dau.mil/dag/DoD5000.asp?view=document
- Hacking Incident Reports
  http://www.webappsec.org/projects/whid/
- Mobile Phone Technology
  http://en.wikipedia.org/wiki/Mobile_phone_features
- SANS' Institute Top 20 Internet Security Attack Targets
  http://www.sans.org/top20/

Backup Charts

Incidents by Threat Classification

Class	Count
Cross-site Scripting	52
Unknown	29
Insufficient Authorization	17
SQL Injection	17
Credential/Session Prediction	15
Insufficient Authentication	13
OS Commanding	8
Other	6
Predictable Resource Location	6
Content Spoofing	4
Information Leakage	4
Weak Password Recovery Validation	4

The Needs for Information Security (1)

- **Government**
  - To protect national databases & security
- **Military**
  - To ensure soldiers have accurate intelligent data and have full control of the weapon system during battles

The Needs for Information Security (2)

- **Business Environment**
  - To protect from disgruntled employees, unethical business competition, corporate espionage, etc.
  - Employees who are not familiar or trained with new technologies can accidentally cause security risks
  - Companies find themselves needing to partner with a company one area, while that same company is a competitor in another area. This requires granting access to some while denying access to others in the same company
  - The amount of information created and collected by companies pose a great security challenge
- **Individual**
  - Personal data needs to be protected

Motives & Classes of Attack

- **Motives:**
  - Personal
  - Financial
  - Social
  - Political
- **Classes of Attack**
  - Passive
  - Active
  - Close-In
  - Insider
  - Distribution

IA Defense Strategy (1)

- IA approach should be based on risk analysis and keyed to the organization's operational objectives.
  - Objective should be to achieve protection against cost, performance, and operational impact

IA Defense Strategy (2)

- ISSE should be built on the three elements:
  - People
    - Support from high level management
    - Establish effective policies and procedures, assignment of roles and responsibilities
    - Enforce personal accountability
    - Support training for IT personnel
    - Make employees aware of the importance of Information Security
    - Provide adequate user training
  - Technology
    - Use COTS, GOTS
    - Use in-house SW development for items not otherwise available
    - Learn and apply emerging IA technologies, balancing enhanced capability with increased risks
    - Create and maintain firewalls
    - Use overlapping protection
  - Operations
    - Enforce Security Policy
    - Plan and follow a continuous migration approach to take advantage of the evolving information processing and network capabilities
    - Periodically evaluate IA postures for improvements
    - Monitor or IA breaches, provide quick detection, reaction, and system recovery

Dangerous Claims about The Smart Phone Security

1. It's just a phone with cool features
2. It's stable just like any other purpose built appliance
3. Communications are encrypted from end to end
4. The connection is secure unless I use WI-FI in a café
5. Emails and messages are safe from prying eyes
6. Using a mobile phone constitutes out-of-band communications
7. I trust the integrity of data and applications on a smart phone
8. Information deleted from a smart phone is gone, right?
9. Spying on my smart phone is hard
10. Abuse is minimal because the network and phones are constrained