Security/Information Assurance Measurements and Metrics

Wai Tsang, Ph.D.
TecSec
6Th Annual International Software Measurement & Analysis Conference
Richmond, VA
September 13, 2011

Agenda

- Software estimation and measurement
  - Sizing estimation (SLOC, FP, Feature Point)
  - Cost and schedule estimation
  - Metrics and Measurements
- Cyber Impact
  - Attacks
  - Security/Privacy
- Cyber Security/Privacy/Information Assurance
  - Risk management standards
  - Metrics and measurements
  - Information assurance standards
- Verticals in need of cyber security/privacy

Software Estimation (Sizing, Cost and Schedule) and Measurements Phases

- Concept of Operation
- Requirement Specification
- Product Design Specification
- Detailed Design Specification
- Software Acceptance

Software Sizing Estimation Methodologies

- Source Lines-Of-Code (SLOC)
- Function Points (FP)
- Feature Points

Software Sizing Estimators

SLOC

- SLOC factors: Executable Instructions, Data Declarations
- Analog-based
- Language dependent
- Design-oriented
- Variations a function of languages
- Convertible to function points
- SLOC with a Predictive Model (COnstructive COst MOdel or COCOMO)

FP

- Core factors: Inputs, Outputs, Logic Files, Inquiries, Interfaces
- Specification-based
- Language independent
- User-oriented
- Variations a function of counting conventions
- Expandable to SLOC

Feature Points

- Derivative of FP for real time system software
- Core FP factors
- Add algorithm parameter

Cost and Schedule Estimation Methodologies

- Analogies
  - Subsystem, computer software configuration item (CSCI), computer software component (CSC), computer software unit (CSU)
- Expert (engineering) opinion
  - Personnel w/ experiential knowledge
- Parametric models
  - Cost drivers based on statistical formulas, Development and operational environments, SW characteristics
- Engineering build
  - Effort summation of detailed functional task breakouts (CSC and CSU)
- Cost performance report analysis
  - Requirements/design, code/unit test, integration/test
- Cost estimation relationship factors
  - Algebraic relationship

Software Metrics and Measurements

- Metrics
  - Monitor
  - Predict
  - Track
  - Understand
- Measurements
  - Quantifiable dimension, attribute, software program, product, process

Cyber World (1)

- Cyber space is a de-perimeterized, distributed data environment
- It is global, densely connected and dynamic
- Cloud computing As-A-Service (AAS) offerings to reduce TCO
  - Software or SAAS
  - Platform or PAAS
  - Infrastructure or IAAS
- Service Oriented Architecture (SOA)

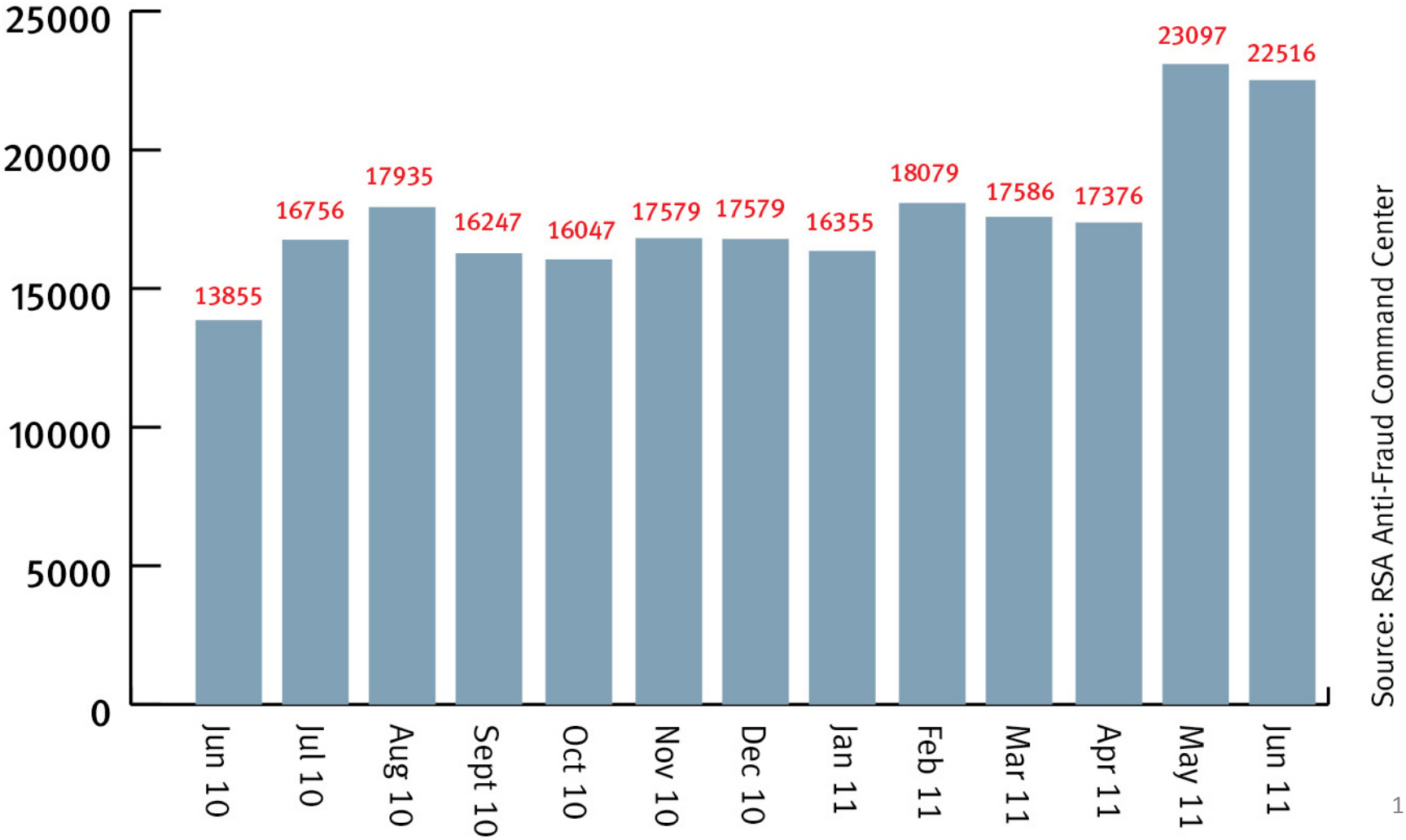
Cyber World (2)

- Not friendly: Trojan, worms, viruses, malware, botnets… => DDoS, identity theft, phishing/pharming, fraud, …
- Communications Security (COMSEC) => Information Security (INFOSEC)
  - Security, privacy, and information assurance
  - Self protecting data objects
  - User-centric
  - Fine grained access control
- Arbitrate assets with risks (i.e., threats, exploits, vulnerabilities)
- Preserve privacy to address liabilities
- Who is involved? (DHS, DoD, NSA, DoE labs, ENISA, MITRE, Verizon Business, ….

Web Browser

- Web browser is a security critical component in the ICT environment. It is the channel for:
  - Information sharing, banking, social networking, shopping, payments, cloud services, critical infrastructure…..
- Target for cyber attacks [Symantec]
  - Web-based attack increased by 93% from 2009 to 2010
  - 40 million attacks for September 2010

Phishing


25000
20000
15000
10000
5000
0
13855
16756
17935
16247
16047
17579
17579
16355
18079
17586
17376
23097
22516
Jun 10
Jul 10
Aug 10
Sept 10
Oct 10
Nov 10
Dec 10
Jan 11
Feb 11
Mar 11
Apr 11
May 11
Jun 11
Source: RSA Anti-Fraud Command Center

Security/Privacy Requirements

Security

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Identity management
- Authorization, Authentication and Accountability (AAA)

Privacy

- Notice
- Consent
- Minimization
- Control
- Access
- Retention
- Secondary use
- sharing

Security/Privacy Considerations within the Software Development Life Cycle (SDLC)

- Like project, quality and risk issues, security/privacy related issues can cause the project to fail
- To ensure success, security/privacy must be the default (built-in not bolted on) and implemented across the entire SDLC
- Security/privacy must be adaptive and preferably are concurrent with implementation of the formalized programs

Risk Management Standards and Guidelines

- NIST SP 800-3--Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Rev 1—Guide for Risk Management Framework to Federal Information Systems: A Security Life Cycle approach
- NIST SP 800-39—DRAFT Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View
- NIST SP 800-53 Rev 3--Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-53A Rev 1--Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
- NIST SP 800-64--Security Considerations in the System Development Life Cycle
- NIST SP 800-13--DRAFT Information Security Continuous Monitoring for Federal Information Systems and Organizations
- ISO
- ENISA
- …

Security/Privacy Metrics and Measurements

- Measurements are single-point-in-views of specific discrete factor, generated by counting
- Metrics are derived by comparing to a pre-determined baseline two or more measurements taken over time, generated from analysis
- Security/privacy attributes are not mutually commensurable
- Security/privacy are often measured in terms of Information Assurance (IA)
- IA controls: Technical, operational and management

Information Assurance (IA) Standards and Guidelines

- NIST SP 800-55 Rev 1—Guide to Performance Measures for Information Security (SP 800-55 and SP 800-80)
- ISO/IEC 15408—IT-Security Techniques-Evaluation Criteria for Information Security
- ISO/IEC 15939—Systems and Software Engineering-Measurement Process
- ISO/IEC 21827—IT-System Security Engineering-Capability Maturity Model-SSE-CMM
- ISO/IEC 27001—IT-Security Techniques, Information Security Management Systems-Requirements
- ISO/IEC 27004—IT-Security Techniques, Information Security Management Systems-Measurements
- ISA 99.03.01 and 99.03.02
- FIPS 140 Evaluation
- …

Verticals in Need of Cyber Security/Privacy

- Financial
  - Mobile payments, web-based transactions

  PCI-DSS, FFIEC
- Healthcare
  - Electronic Health Record (EHR), Health Information Exchange (HIE)

  HIPAA, HITECH
- Smart Grid
  - Information sharing among domains/stakeholders

THANK YOU

Wai Tsang, Ph.D.

(o) 571-299-4129

(m) 703-303-4376

wtsang@tecsec.com