ISSE: A Critical Component of the Systems Engineering Lifecycle

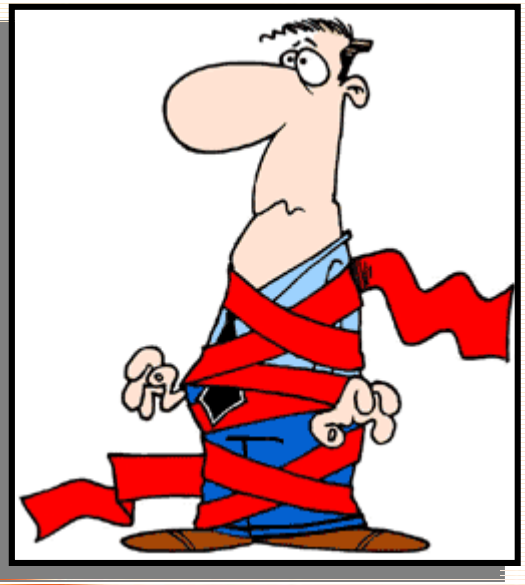
Presented by James Davis

Graduate Student, Master of Software Engineering

University of Maryland University College

Disclaimer

This presentation, both discussion and content, as well as the content of the paper in no way reflect the opinions, standards or policy of the United States Air Force, Department of Defense or the United States Government.



Overview

- *What we've seen so far at SIGAda '04*
- *Why present this at a SIGAda Conference?*
- *Importance/Current state of IT security*
- *What's an ISSE?*
- *How an ISSE fits in the SWE/SE lifecycles*
- *How to become an ISSE*
- *How to get ISSE Services*
- *The Future for ISSE in SWE/SE*

What we've seen so far for SIGAda '04?

- *Ada best used for*
  - *Systems requiring high reliability, integrity, portability, high reuse*
  - *Safety systems, Flight Control Systems*
- *C/C++ not as safe as Ada*
- *Ada error rates and cost-to-fix rates are lower than C/C++*

- ***Ada is good for safety***

What about Security? (1 of 2)

- *Watts Humphrey's "Security Changes Everything"*
- *Praxis' "…Information Flow Analysis Tool"*
- *Retrospective|Reactive|Response Security doesn't work*
  - *"The system you find the most defects in has the most defects left" vs. another system undergoing comparable testing methodologies*
- *Cross' "…home security built in with the home architecture…"*
- ***Security is a quality problem***

What about Security? (2 of 2)

- *Ok, let's assume that we've found the silver bullet and now S/W is of the highest quality wrt security and safety…are we done?*
- *No! How do we know if we have the right security mechanisms in the right places to protect the right things?*
- *Baking in security requires two disciplines*
  - *Building high quality, verifiable and proven software*
  - *Engineering support to address security throughout the S/W and Systems Engineering Lifecycles*
    - *Security Requirements Engineering*
    - *System Threat Analyses*
    - *System Risk Analyses*
    - *Certifications and System Accreditations*

Why present this at a SIGAda Conference?

- *Ada is a "safer" programming language*
- *"Safer" programming enables a higher level of confidence in software and systems*
- *Everybody {designers, programmers, maintainers, managers, etc.} must understand and be Security Aware*
- *An ISSE is essentially a certified Security Aware professional*

Importance/Current state of IT Security

- *S/W continues to exponentially become ever more complex*
  - *Windows OS ~10's of MSLOCs[1]*
  - *GNU Linux Kernel ~4.3 MSLOCs[2]*
- *New S/W must be compatible w/ old S/W*
- *Cost of Security in a System's Lifecycle is difficult to represent*
- *Users demand more functionality without directly understanding impact to security*

- ***DEFENSE is becoming ever more difficult!***

[1] – As presented during SIGAda 2004
[2] – http://www.dwheeler.com/essays/linux-kernel-cost.html

Importance/Current state of IT Security

- *Rate at which faults are detected continues to grow*
- *Time from fault detection to public-exploitation continues to narrow*
- *Ability to control proliferation of fault knowledge and exploitation continues to weaken*

- ***OFFENSE is getting much better and easier!***

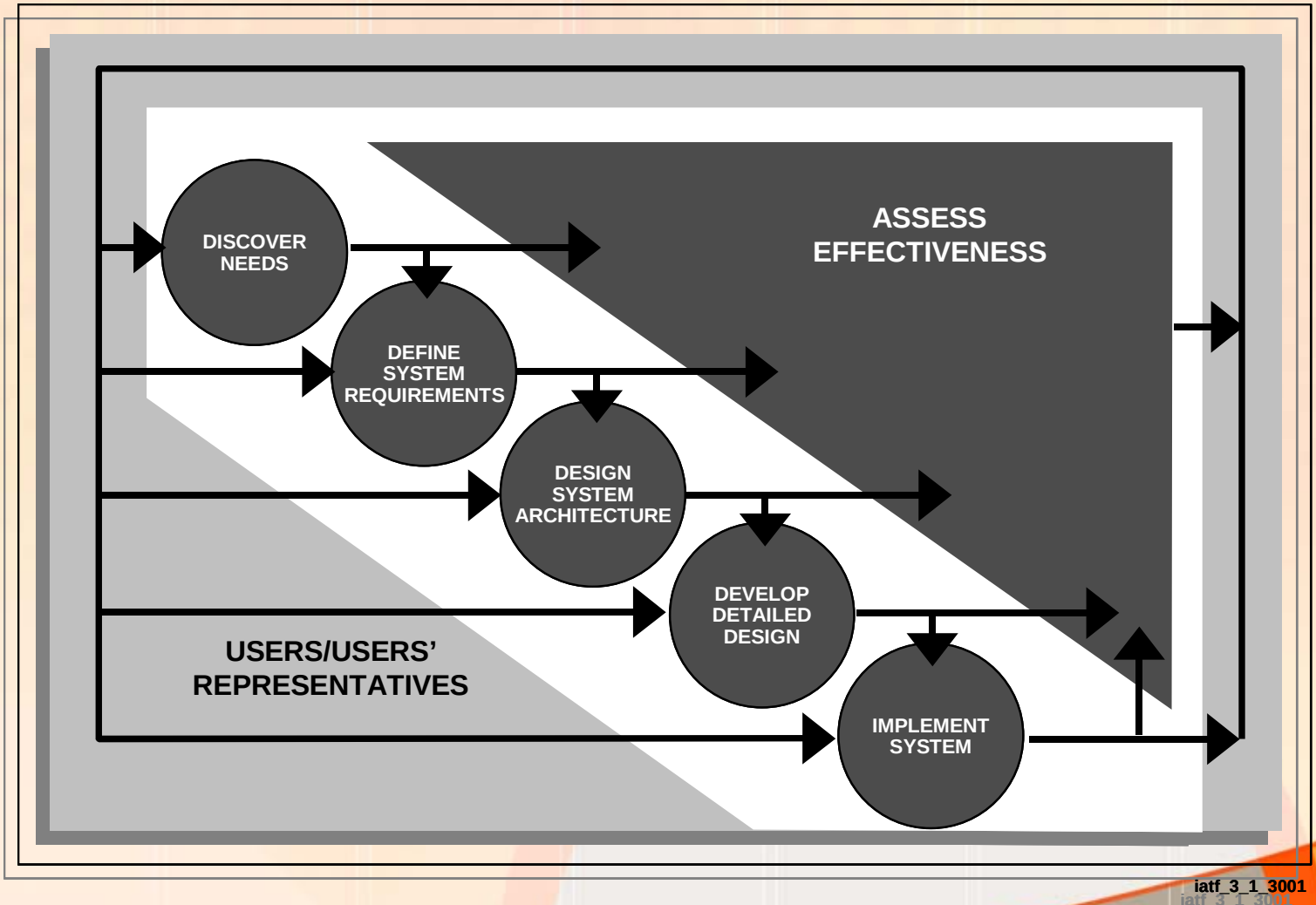
What's an ISSE?

- *"The art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected" – IA Technical Framework Forum*

- *In essence, comprises a set of systematic processes that bakes Information Assurance (IA) into the engineering process.*

[1] – http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1 -

Generic ISSE Framework



[1] – http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1 -

How an ISSE fits in the SWE/SE lifecycle

- From Cradle-to-Grave

SE Activities	ISSE Activities
Discover Needs	Discover Information Protection Needs
Define System Requirements	Define System Security Requirements
Design System Architecture	Design System Security Architecture
Develop Detailed Design	Develop Detailed Security Design
Implement System	Implement System Security
Assess Effectiveness	Assess Information Protection Effectiveness

[1] _ http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1 -

How an ISSE fits in the SWE/SE lifecycle

DoD 5000.2-R Systems Engineering Process	ISSE Process
Systems Engineering Process Inputs	Discover Information Protection Needs
Requirements Analysis	Define System Security Requirements
Functional Analysis/Allocation	Design System Security Architecture
Requirements Loop	Assess Information Protection Effectiveness Support System C&A
Synthesis	Develop Detailed Security Design
Design Loop	Assess Information Protection Effectiveness Support System C&A
Process Output	Implement System Security
Verification	Assess Information Protection Effectiveness Support System C&A

IEEE Std 1220-1998 Systems Engineering Process	ISSE Process
Requirements Analysis	Discover Information Protection Needs
	Define System Security Requirements
Requirements Verification and Validation	Assess Information Protection Effectiveness Support System C&A
Functional Analysis	Design System Security Architecture
Functional Verification	Assess Information Protection Effectiveness Support System C&A
Synthesis	Develop Detailed Security Design
Design Verification	Assess Information Protection Effectiveness Support System C&A
System Analysis	Implement Systems Security Assess Information Protection Effectiveness Support System C&A
Control	Plan Technical Effort Manage Technical Effort

[1] – http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1 -

How to become an ISSE

- *Follow the (ISC)^2 steps to becoming a Certified Information Systems Security Professional (CISSP)*
- *Pay for and successfully complete exam*
  - *250 multiple-choice questions covering:*
    - *Access Control Systems & Methodology*
    - *Application & Systems Development*
    - *Business Continuity Planning*
    - *Cryptography*
    - *Law, Investigation & Ethics*
    - *Operations Security*
    - *Physical Security*
    - *Security Architecture & Models*
    - *Security Management Practices*
    - *Telecommunications, Network & Internet Security*
- *Be endorsed as to possessing 4yrs experience in information security or 3yrs plus a college degree*

How to get ISSE Services

- *Government*
  - *Contact the National Security Agency/Information Assurance Directorate*
- *Industry*
  - *Train in house*
  - *Hire out of house*
  - *As with Ada programmers, if you pay them they will come…*
- *Academia*
  - *Need to build ISSEs from the ground up for Industry and Government service*

The future of ISSE in SWE/SE

- *Retrospective Security due to incorrect set of initial security mechanisms for a system is extremely expensive*
- *Just as system complexity is growing, so needed is the level of trust, confidence and integrity for these systems*
- *ISSE is becoming, and in some cases has already become, a security focal point for system development processes*

Summary

- *What we've seen so far at SIGAda '04*
- *Why brief this at a SIGAda Conference?*
- *Importance/Current state of IT security*
- *What's an ISSE?*
- *How an ISSE fits in the SWE/SE lifecycles*
- *How to become an ISSE*
- *How to get ISSE Services*
- *The Future for ISSE in SWE/SE*

Questions?