Cyber R &D Research Roundtable

2 May 2013
Changing Environment

- Rapidly Evolving Threat
  - Changes faster than the assumed risk we think we have
  - The bad guys are sophisticated
    - Organized Crime
    - Nation States

- Cybersecurity Enhancement Act of 2009 (S.773)
  - US legislation intended to improve cybersecurity within the federal government and throughout the public and private sectors
  - Establishes research and development (R&D) requirements for federal agencies and promotes public-private partnerships

- Cyber Intelligence Sharing and Protection Act (CISPA) (H.R. 624)
  - Proposed US federal law that would allow for the sharing of Web data between the government and technology companies
SAIC Cyber Overview

Full Spectrum Cyber Security Solutions

- Secure Network Deployment
- Vulnerability Assessments
- Security Engineering
- Policy and Standards Requirements
- Penetration Testing
- Research and Development
- Awareness and Training

System Owner Support

- Embedded Information Systems Security Engineers at the PEOs
- Integrate System Security
- Core Project Team members

Software Assurance

- Scan New or Existing Code to Detect Vulnerabilities
- Train SW Developers on Secure Coding Practices

Agent of the Certification Authority

- Provide independent, 3rd party evaluations to determine the security posture of Army systems
- Scan to Identify and Report Discovered Vulnerabilities

Penetration Testing

- Exploit Identification / Vulnerability Scanning
- Operational Assessment of Networks
- System Hardening
- Network Attack Simulation
- Handheld Device Security Analysis

Computer Network Defense

- Detect, identify and analyze malicious attack vectors against DoD Systems
- Developed POI for CND Training
- ALARNG received a 40-hour block of instruction on Interrogator

Training

- Cyber Security Awareness Training
- ISC2 CISSP / CompTia Security+
- Certified Ethical Hacker (CEH) Accredited Training Center

Supply Chain Risk Management

- Work With SMDC To Support Integrity Engineering Analysis
- Invest AMRDEC Core S&T Funds For A Study To Develop AMRDEC Path Forward

Blue Team Assessments

- Determine security posture for DoD systems
- Network and vulnerability scanning
- NIST Guidelines
Definitions

• **Confidentiality** concerns the protection of sensitive information from unauthorized disclosure.

• **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

• **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

• **Risk** = Threat * Vulnerability * Cost
Bottom Line

• If a soldier receives an order to launch a missile, he needs to be assured that it is a valid order (integrity) and the missile will actually launch (availability). The commander needs to ensure only the correct people receive the order (confidentiality)

• Mission Assurance
Change in Mind Set - Continuous Security

- Real Time Assessments
- Continuous Monitoring
- Don’t just assess systems periodically
- Create a realistic Residual Risk
- Follow NIST Guidelines – Holistic Risk Management
- Constant Improvement
Software Development – Application Security

• Where do you begin?
  – Integrate from the onset – key component of the Software Development Lifecycle
  – “Tacked on” at the end is usually expensive
  – Cradle to grave - Evolving

• Support identified requirements

• Identify and mitigate risks early
Software Development Security Trends

- Common Coding Practices Not Followed
- User Input Validation not Implemented
- Old Applications – More Vulnerable
- Clear Text Connection Strings
- Single Tier Applications
- Common Attacks
  - SQL Injection
  - OS Command Injection
  - Buffer Overflow
  - Path Manipulation

```c
struct frame{  
  unsigned long framesize;
  ...
}
void decode_header(struct frame *fr, unsigned long newhead){  
  ...
  if(!head_check(newhead))  
    return 0;
  ...
  fr->framesize=(newhead>>12)&0x1f;
  void *p=(void *)malloc(fr->framesize);
  ...
  int head_check(unsigned long head){  
    if( (head>>12)&0xf ) == 0x0f )  
      return false;
    ...
    return true;
  }
}
```

```xml
<connectionStrings>
<add name="SqlConnectionProvided"
    connectionString="Data Source=.; Initial Catalog=TestApp; User Id=User1;Password=P@$$WO$$d; enlist=true;"
    providerName="System.Data.SqlClient" />
</connectionStrings>
```
User – Insider Threat Trends

- Insider Threat – Not Necessarily Malicious
- Basic Education - Training – Knowing
- Certifications
  - CISSP
  - Security+
  - Certified Ethical Hacker
  - Operating System Certification
- More Awareness – Less Reliance
- Lack of Policies
- Social Engineering
  - Phishing
  - Tailgating
  - Dumpster Diving
- Social Networks – Information Sharing
- Logins/Passwords Taped to a Computer
System Configuration Trends

- Patching – Mainly 3rd Party (Java and Adobe)
- Outdated Operating Systems
- Lack of Auditing Consolidation/Alerting
- Back-up and Restoration Plan
- Excessive Permissions
- Wireless Configuration
- Handheld Device Configuration
- Big Data Consolidation
- Default Passwords