Security Patterns in Systems Acquisition & Test

John Jorgensen
Director, IT Security

Crystal City, Virginia
14 November 2013

Track 3
Tools & Methodologies for Cyber Testing

Problem Statement

- We need systems that provide predictable behavior, understandable interactions, and seamless interoperability
- We need systems that can show clear delineations between allowable operations modes. Such behavior must be repeatable, measurable and manageable across systems of systems.
- We need systems whose architecture and design provide corporate knowledge and learning opportunities. We need replicable patterns that are proven, understood and foundational.

Acquisition is Effective When…

- System requirements are met clearly in test and evaluation;
- System performance is predicted and predictable;
- System failure modes are known, and assurance measures have been taken in design and engineering against those failure modes;
- Measurement sensors and reporting mechanisms are built into the system to provide understanding of normal and abnormal operating modes;
- System supportability and maintainability are addressed as part of reliability planning; and
- All system upstream and downstream effects are understood before the system is placed in its intended environment

Test is Both In-Line & In-Parallel

- Testing Assessment and Evaluation Must
  - "Test it in" when certain parameters are not met – but resources are always at the issue at the testing stages
  - Look at functional and nonfunctional requirements to ensure stakeholders' intent is met
  - Evaluate Effectiveness and Suitability in the context of assuring the function is completed within the security conditions
  - Consider operating assumptions for the system – and their effects on the operating environment or platform
  - Assemble a risk register for those issues remaining outstanding against assured function, environmental risks, and nonfunctional requirements left unmet
  - Use shaping questions throughout the early development lifecycle to verify the system becomes effective and suitable

System-Shaping Questions

- What/where are the crown jewels?
- What measures mean the most in the networked environment?
- Are the protective devices and controls effective for those measures?
- Can you detect what you don't know to expect?

- ✓ Is storage consistent?
- ✓ Have we defined access?
- ✓ What are the critical processes whose output we must protect?
- ✓ Can we test critical functions for integrity and availability?
- ✓ What best indicates both normal and abnormal conditions?
- ✓ What indicators show when action is required in response?
- ✓ Are protective devices' functions tuned or oriented to expected threats?
- ✓ Can you detect or react to unexpected threats?

Portfolio-Shaping Questions

- Are investments working?
- What are the highest priorities for investment?
- What are the upstream or downstream effects?

- ✓ Are system investments making a measurable difference in system function or security?
- ✓ Are system investments aligned with the portfolio requirements for system-of-systems functional assurance?
- ✓ Do the crown jewels (data and processes) command appropriate resources?
- ✓ Are the highest and most likely threats prioritized for mitigation or negation?
- ✓ Is the system environment equipped with sensors?
- ✓ Are residual risks known across all connected systems in the environment?

Governance Assessment Questions

- Investment control
- How big is the enterprise attack surface?
- How is enterprise (system of systems) testing done, and how is the residual risk tracked and managed?
- How are individual security contributions and controls managed across the enterprise?

- ✓ Are system sustainability and threat upgrades done with a view toward impacts on connecting systems?
- ✓ Are investments increasing the overall security and functional assurance of the entire enterprise?
- ✓ Is security (non-functional) testing performed in concert with functional testing?
- ✓ How is technical debt tracked and managed?
- ✓ Is the entire governed system of systems (vehicle, mission systems, connected organizations) manageable through visible and known characteristics?

System Factors: Controls

- There are three types of security controls for information systems that can be employed by an organization: (i) **system-specific controls** (i.e., controls that provide a security capability for a particular information system only); (ii) **common controls** (i.e., controls that provide a security capability for multiple information systems); or (iii) **hybrid controls** (i.e., controls that have both system-specific and common characteristics)
- The organization allocates security controls to an information system consistent with the organization's enterprise architecture and information security architecture
- As part of the information security architecture, organizations are encouraged to identify and implement security controls that can support multiple information systems efficiently and effectively as a common capability (i.e., common controls)
- When these controls are used to support a specific information system, they are referenced by that specific system as **inherited controls**

20 Critical Controls

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software


3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers


4: Continuous Vulnerability Assessment and Remediation


5: Malware Defenses

6: Application Software Security

7: Wireless Device Control


8: Data Recovery Capability

In Process 9: Security Skills Assessment and Appropriate Training to Fill Gaps

Partial 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Partial 11: Limitation and Control of Network Ports, Protocols, and Services

In Process 12: Controlled Use of Administrative Privileges


13: Boundary Defense


14: Maintenance, Monitoring, and Analysis of Audit Logs


15: Controlled Access Based on the Need to Know

In Process 16: Account Monitoring and Control


17: Data Loss Prevention


18: Incident Response and Management

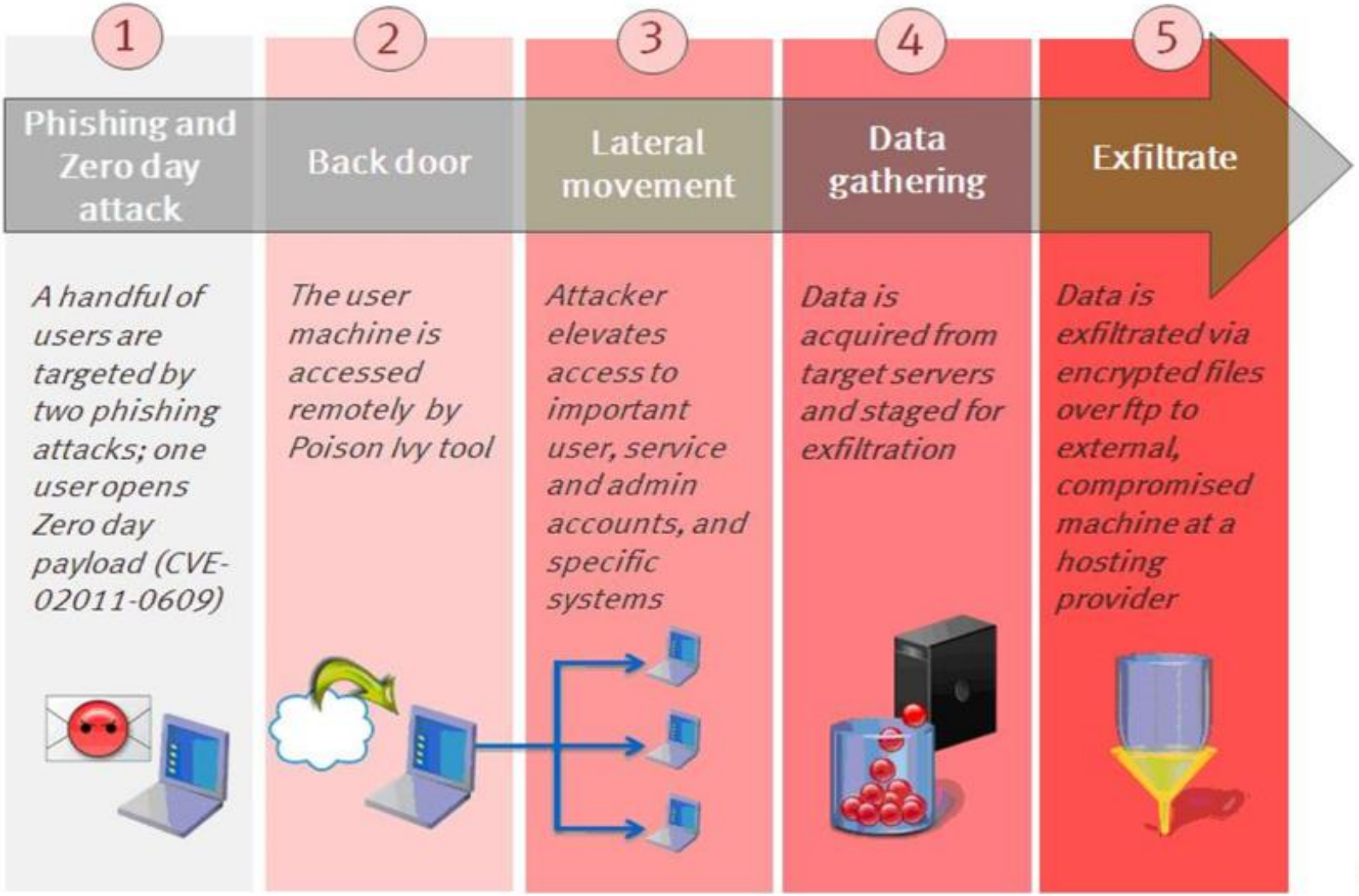
Partial 19: Secure Network Engineering


20: Penetration Tests and Red Team Exercises

These are the POSITIVE decisions in control selection.

Source: http://www.sans.org/critical-security-controls

Attack Event Chain



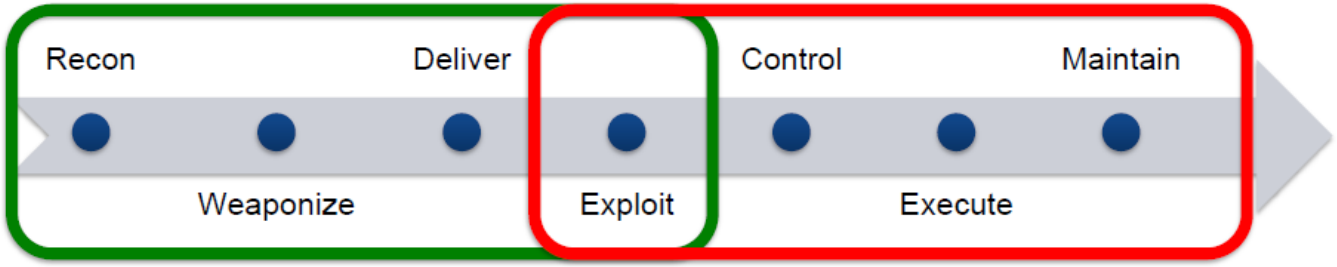
Source: http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Intrusion Process

The Cyber Kill Chain*

Recon	• Obtain information to conduct the attack
Weaponize	• Place payload into delivery vehicle
Deliver	• Send the attack to the potential victim
Exploit	• The point of no return
Control	• Direct the victim system to take actions
Execute	• Fulfill mission requirements
Maintain	• Ensure future access

- **Understand capabilities and intentions**
- **Leverage the kill chain to improve our defenses**
- **Provide resiliency and detection**
- **Create Opportunities for Engagement**
- **Detection "left of exploit"**
- **Research "right of exploit" for mission assurance**



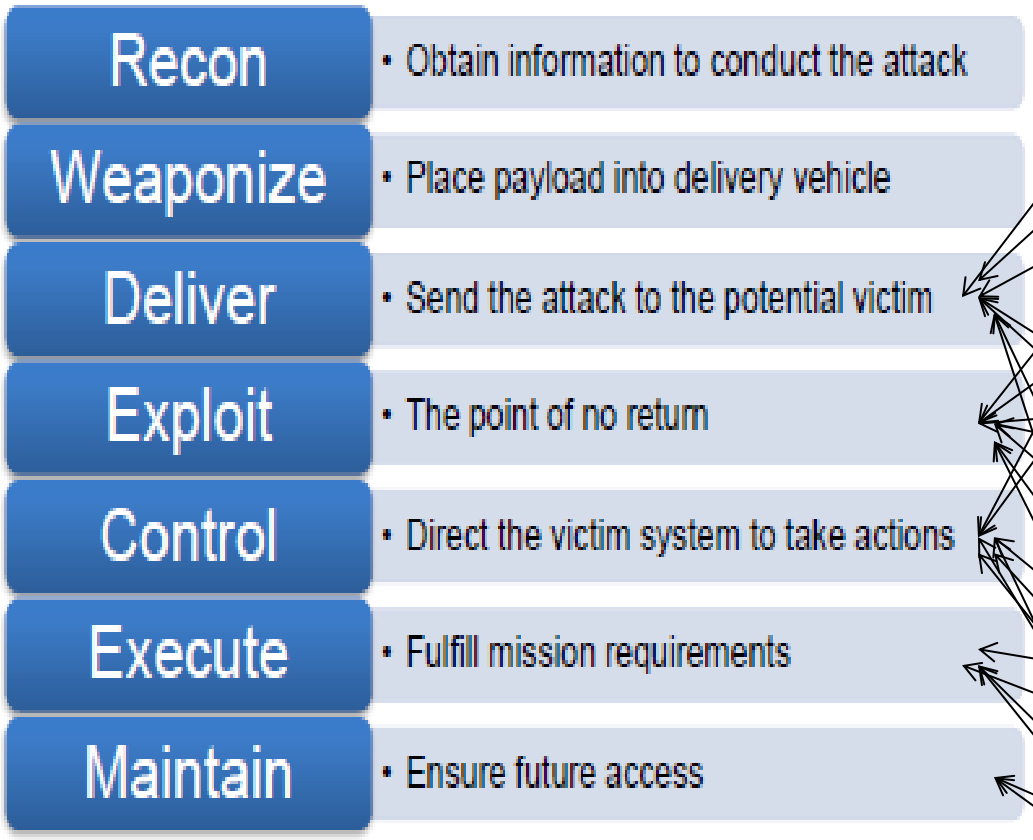
- Each Stage is an Opportunity for Detection
- Safeguards at each stage will provide defense in depth

This is the NEGATIVE decision pole of control selection

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.; Lockheed Martin Corporation

2

Protective Functions Address Attacker's Kill Chain



- Email filtering and detonation chamber
- Web reputation filtering
- Privilege management (admin password escrow)
- End user administrative rights control
- Database protection
- Web application protection (WAF)
- Patch automation and configuration tracking
- Two-factor authentication
- Exfiltration detection
- Application attack prevention
- Log management automation
- Command and Control (C2) and anomaly detection

Source: MITRE 2012, PR12-0886

Protective Functions: More Complete List

- Email encryption
- Email filtering and detonation chamber
- URL/Web reputation filtering
- Packet capture and filtering
- Protocol analysis/tracking
- Endpoint antivirus/anti-malware
- Privilege management (admin password escrow)
- End user administrative rights control
- Database protection
- Web application protection (WAF)
- Mobile device protection
- File integrity checking
- Data At Rest (DAR) encryption
- Threat intelligence and warning
- Intrusion detection and prevention
- Patch automation and configuration tracking
- Network access control (NAC)
- Two-factor authentication
- Exfiltration detection
- Application attack prevention
- Log management automation
- Command and Control (C2) and beaconing detection
- Forensic evidence capture

Now Add the Two Sides Together

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Device Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

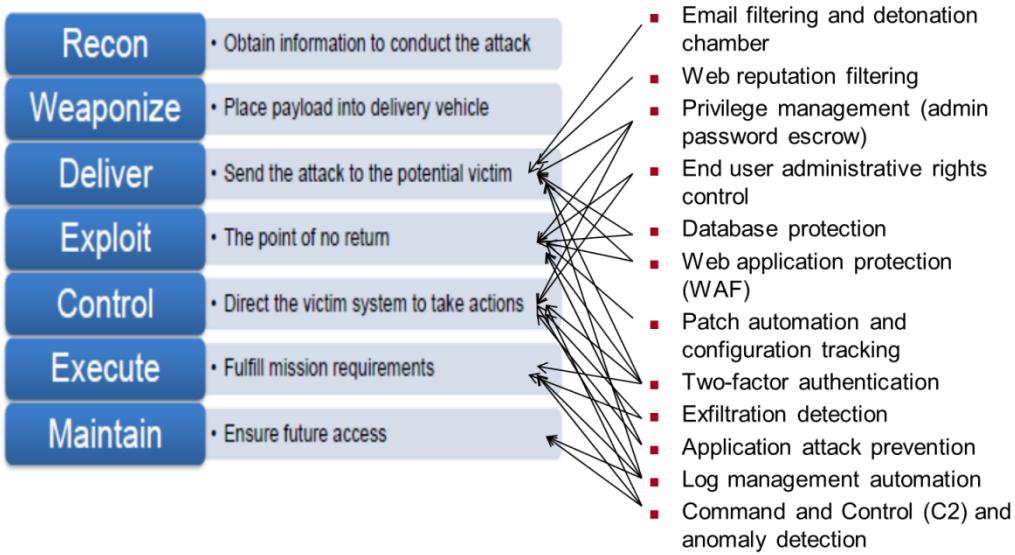
16: Account Monitoring and Control

17: Data Loss Prevention

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises



Required capabilities list

Required protective functions list

Pattern Capability Requirement List

Pattern Capability Requirement List

- Positive Pole Capabilities
  - System (program) shall provide capabilities for _____
  - Operations and maintenance shall do _____
  - Any capabilities not addressed become risk register entries
    - If the system cannot enumerate its networked components, then the system may suffer unnoticed intrusion
    - If the system is not periodically tested against hostile penetration methods, then the system may suffer from vulnerabilities due to hostile developments in attack methods

Pattern Capability Requirement List

- Negative Pole Capabilities
  - System (program) shall provide protective functions _____
  - Operations and maintenance shall support by _____
  - Any capabilities not addressed become risk register entries
    - If the system cannot screen its web access requests, then it may suffer from drive-by malware insertions
    - If the system cannot decrypt internal ssl transmissions, operators may not detect illicit data aggregation and exfiltration
    - If the system cannot detect and prevent outbound command and control beaconing, then the system may suffer infection and unbounded spread of malware on internal nodes

Pattern Templates

- Individual endpoints
- Basic network – nodes and peripherals
- Basic plus mail
- Shares and data repositories
- Application and web servers
- VoIP and streaming media
- Databases and DB applications
- Cloud storage and applications
- Programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), and sensors

Shaping Patterns With Lessons Learned

- Lesson
  - Architecture can be stable, but not static
  - Policies and procedures must complement functional controls
  - Risk management is challenging unless matching use cases against protective controls, methods and devices
    - Risk planning must include reviews of all categories of threats, not simply those considered most likely
    - Intelligence sharing is a very powerful tool for collective action and collaborative protective postures

- Survey in Test by:
  - Architecture transition planning and change procedures
  - Completeness of policies and procedures
  - Complementary nature of positive and negative pole capabilities
  - Risk register compilation
    - Outstanding risks remaining from positive and negative pole capability lists
    - Threats left unaddressed (lack of priority)
    - Technical debt remaining from program development

Shaping Patterns with Lessons Learned

- Lesson
  - Data Flows Are Voluminous
    - Data begs automation
    - Data determines measures, but measures must be relevant to the organization and lines of business and/or mission areas
    - Outcomes are most important
  - Security Architecture must fit the mission context and the Enterprise Architecture
  - Business capability mapping may help identify gaps and overlaps in Security Methods and Controls
- Survey in Test by:
  - Assess program's ability to
    - Capture protective device data streams
    - Prioritize events relevant to system (platform) health and operations
    - Highlight events that require action
    - Provide human-readable output
  - Consider supportability and the operational context
    - Cognitive support for differing devices
    - Seamless (or not) indicators and metrics that fit operator context (i.e., HSI to support mission and security)
    - Staffing for operations and maintenance

What We Need to Understand

- Information sensitivity and implications of aggregation – know how to optimize storage for security and workflow
- Threat and risk intelligence – information to help aid understanding of relative risks against system(s), organizations and critical data
- Protective mechanism completeness – when to consider that one has sufficient border and defense-in-depth resources in place to understand adequacy
- Measures and metrics to apply against the protective mechanisms in place, thereby to have (and maintain) cyber situational awareness.
- Holistic sustainability for the mechanisms, metrics and policies and procedures in place, with an eye toward building a self-sustaining security organization

www.eagle.org