

System Integration

Mini Case Studies © 2010

Security Integration

Shawn A. Butler, Ph.D.
Senior Lecturer, Executive Education Program
Institute for Software Research
Carnegie Mellon University

Objectives

- Understand some of the essential elements of security
- Identify some of the problems integrating security architectures





Agenda

- A quick overview of security
- Authentication
- Access Control
- Auditing
- IPv?




Risk

- Risk management methods and security engineering principles *guide* selection of risk-mitigation controls for a system's security architecture
- The purpose of risk management is to ensure that security risks are brought to an acceptable level
- The system security architecture are the policies, procedures, and technologies that mitigate the risk








Design Decisions

- Support security design principles 
- Cost and effectiveness
 - Maintenance
 - Skill level
 - Out source
- Organizational adoptability 
- Marginal benefit 
- Due diligence 

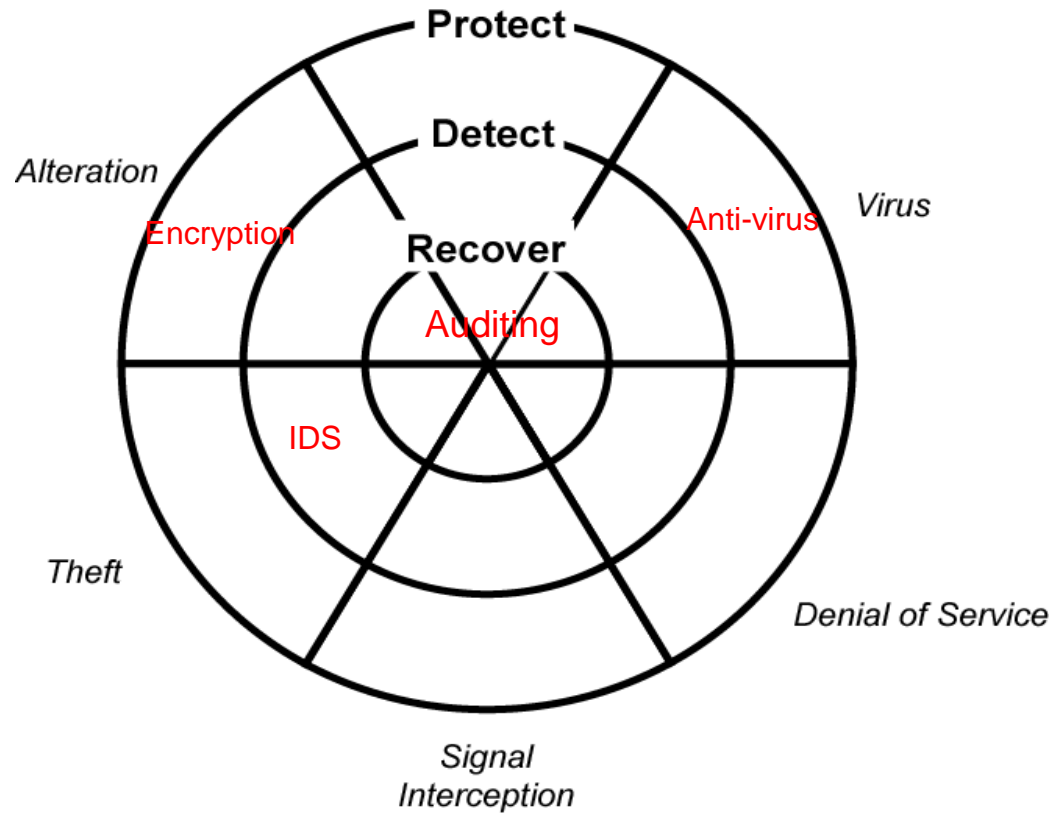
Important Security Terms

- **Authentication** – The determination of claimed identity
- **Authorization** – The determination of access to resource(s)
- **Non-repudiation**  – The prevention of a principal from denying participation 
- **Security Protocols** – The rules that govern communications between principals
- **Trust**  – Confidence that the principals' activities will be protected and conducted as intended

Security Heuristics

- **Prevention** – Prevention is preferred over detection and recovery 
- **Completeness** – Consider all assets when designing the security architecture 
- **Defense in breadth and depth** – Countermeasures should be deeply staggered and widespread 
- **Reduce external relationships** – Dependencies on others introduce vulnerabilities 
- **Integration** – Countermeasures should be seamlessly integrated 
- **Anticipation** – Your risk environment will change 
- **Simplicity** – The KISS principle applies 



Defense-in-Depth



What do we trust?

- Trust that the other principal is really who it claims to be – **Authentication and Authorization**
- Trust the process and mechanisms by which principals communicate – **Encryption**
- Trust the information exchanged – **Data Integrity**
- Trust the other principal will not deny participation in the exchange – **Non-repudiation**

Authentication Criteria

- What you know - Passwords
- What you have – Physical keys, ATM cards
- What you are - Biometrics 
- Who you know – Chain of authentication 
- Where you are - Workstations

Password Policies

- What is an acceptable password?
- How often must the user change the password?
- How many times can a user attempt logon?
 - What is the business cost?
- What is the process for getting an initial password?
- What forms of verification are acceptable?
- How does the user re-establish access after forgetting the password?
- Will you enforce or encourage good password selection?
- How many different passwords?

Single Sign-on?

Symmetric-key Cryptography

■ Advantages

- The encryption and decryption algorithms can be fast in both hardware and software
- Keys are relatively short
- Ciphers can be used to generate pseudo-random numbers, hash functions, and digital signatures
- Ciphers can be combined to create very secure encryption

■ Disadvantages

- Key distribution is a problem
- Key must be replaced often
- Not administratively easy for digital signature algorithms

Asymmetric-Key Cryptography



■ Advantages

- Key distribution problem solved
- Key does not have to be replaced as often
- Only a small number of keys are needed in a large network

■ Disadvantages

- Encryption algorithms are normally slower than symmetric-key ciphers
- Keys are much longer (1,000 bits)
- Security is based on the difficulty of factoring large numbers

Public Key Encryption

- Provides
 - Confidentiality
 - Non-Repudiation
 - Authentication
 - Public and Private Keys have a unique relationship
 - Examples of PKE: Diffie Helman, RSA, Digital Signature Standard (DSS)
 - Examples of Protocols using PKE
 - PGP
 - Ssh
 - SSL (TLS)
 - IKE

Public/Private Key Integration

- Different Key Management Infrastructures (KMIs) provide different levels of trust
- How did the entities obtain their credentials?
- How often are revocation lists updated?
- Are the technologies/protocols compatible?
- Do all systems assume the same level of trust?

Country	Year	Value
China	2010	1.00
China	2011	1.00
China	2012	1.00
China	2013	1.00
China	2014	1.00
China	2015	1.00
China	2016	1.00
China	2017	1.00
China	2018	1.00
China	2019	1.00
China	2020	1.00
China	2021	1.00
China	2022	1.00
China	2023	1.00
China	2024	1.00
China	2025	1.00
China	2026	1.00
China	2027	1.00
China	2028	1.00
China	2029	1.00
China	2030	1.00
China	2031	1.00
China	2032	1.00
China	2033	1.00
China	2034	1.00
China	2035	1.00
China	2036	1.00
China	2037	1.00
China	2038	1.00
China	2039	1.00
China	2040	1.00
China	2041	1.00
China	2042	1.00
China	2043	1.00
China	2044	1.00
China	2045	1.00
China	2046	1.00
China	2047	1.00
China	2048	1.00
China	2049	1.00
China	2050	1.00
China	2051	1.00
China	2052	1.00
China	2053	1.00
China	2054	1.00
China	2055	1.00
China	2056	1.00
China	2057	1.00
China	2058	1.00
China	2059	1.00
China	2060	1.00
China	2061	1.00
China	2062	1.00
China	2063	1.00
China	2064	1.00
China	2065	1.00
China	2066	1.00
China	2067	1.00
China	2068	1.00
China	2069	1.00
China	2070	1.00
China	2071	1.00
China	2072	1.00
China	2073	1.00
China	2074	1.00
China	2075	1.00
China	2076	1.00
China	2077	1.00
China	2078	1.00
China	2079	1.00
China	2080	1.00
China	2081	1.00
China	2082	1.00
China	2083	1.00
China	2084	1.00
China	2085	1.00
China	2086	1.00
China	2087	1.00
China	2088	1.00
China	2089	1.00
China	2090	1.00
China	2091	1.00
China	2092	1.00
China	2093	1.00
China	2094	1.00
China	2095	1.00
China	2096	1.00
China	2097	1.00
China	2098	1.00
China	2099	1.00
China	2100	1.00
China	2101	1.00
China	2102	1.00
China	2103	1.00
China	2104	1.00
China	2105	1.00
China	2106	1.00
China	2107	1.00
China	2108	1.00
China	2109	1.00
China	2110	1.00
China	2111	1.00
China	2112	1.00
China	2113	1.00
China	2114	1.00
China	2115	1.00
China	2116	1.00
China	2117	1.00
China	2118	1.00
China	2119	1.00
China	2120	1.00
China	2121	1.00
China	2122	1.00
China	2123	1.00
China	2124	1.00
China	2125	1.00
China	2126	1.00
China	2127	1.00
China	2128	1.00
China		




Access Control Criteria

- What objects can you access?
- What can you do to objects?
- What can you allow others to do?
- What can the group access?
- What can the group do to the object?
- What can group members allow others to do?
- What is the lowest level of control?




Across domains or enclaves, these may not be the same

Principles of Access Control



- Principle of Least Privilege
- Subjects, Objects, Capabilities, Roles
-  Mandatory, Discretionary, Role Based Access Control
- Two Models for Multi-level Security
 - Bell-LaPadula Model – No Read up:No Write down
 - Biba Model – No Write up – Read up only

Access Control Integration

- Different access control mechanisms are often not compatible 
- Changes in sensitivity levels of information 
- Data aggregation
- Merging directories is not trivial
- Access control decision rules are based on a pre-existing assumption of authentication trust
- Granularity of accessible  objects

Audit

- Account logon events
- Account management
- Object access
- Policy change
- System events

Logging Integration

- What events are being logged?
- How much additional space will be required?
- Will old logs still be accessible?
- Are the logs semantically equivalent?
- Do logs overlap?
- Is there a specific reason for logs?

Summary

- Integration of security services is difficult and takes considerable planning
- Integration of security services may introduce more risk than the risk of each component
- Authentication, access control, and auditing are the fundamentals of system security
- Not all system integration tasks involve security, but when they do, find a security engineer with experience