System Integration

Mini Case Studies

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

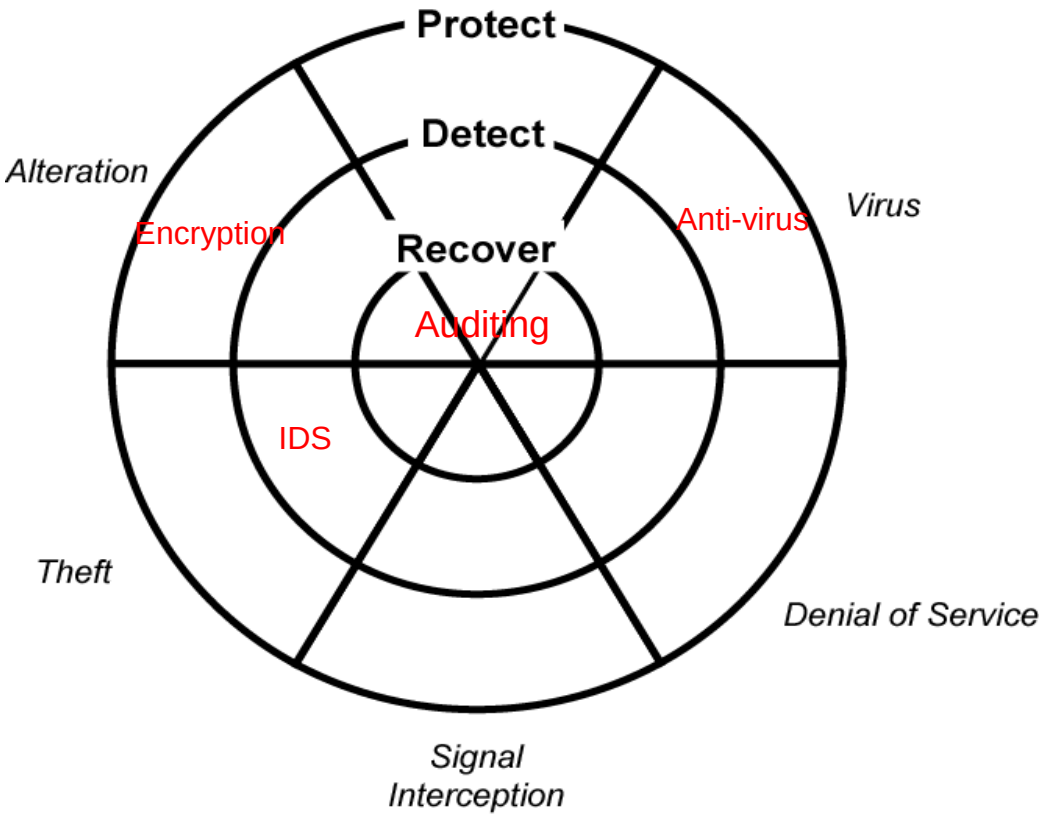
Important Security Terms

- 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

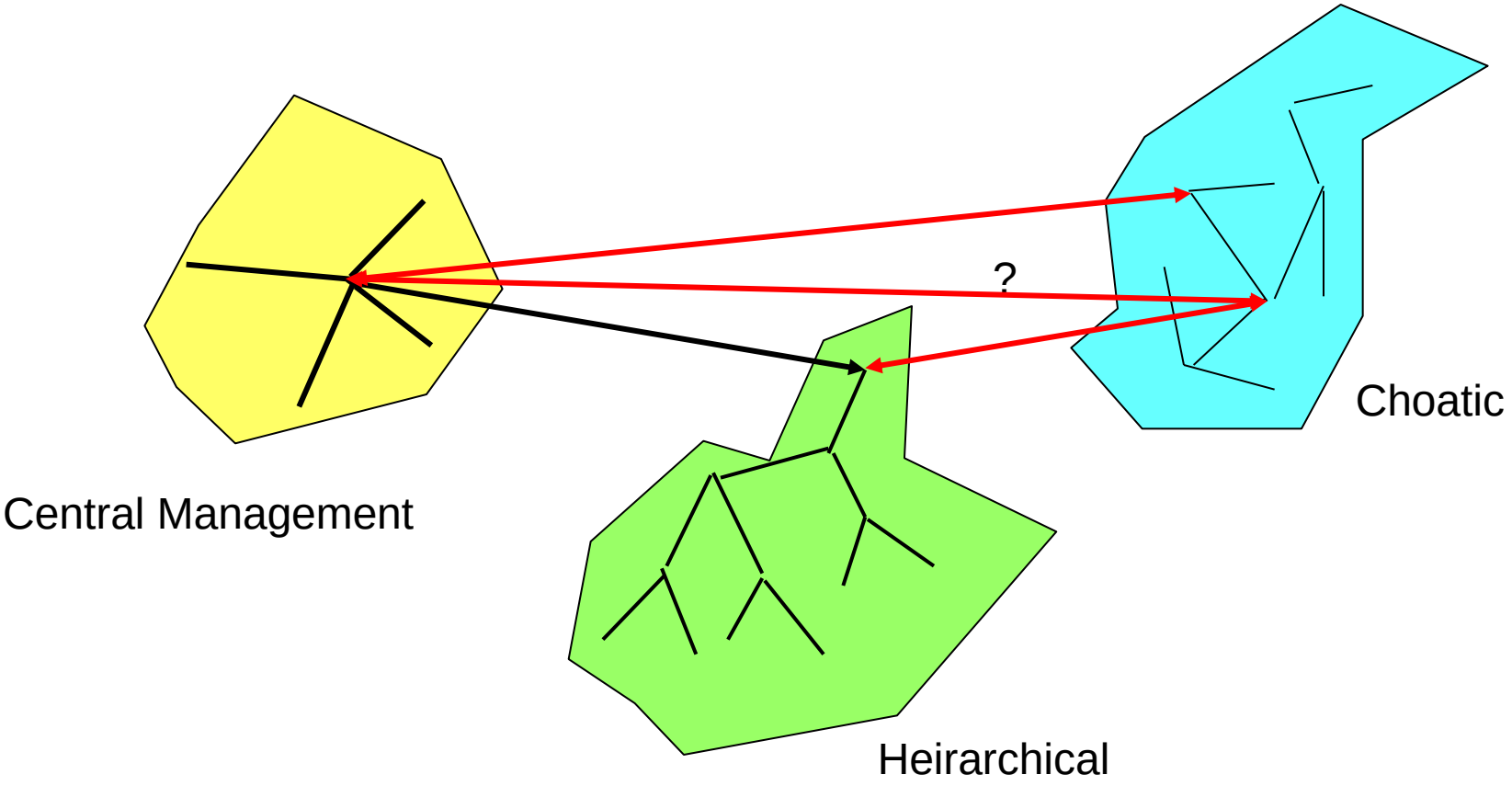
Public Key Encryption

- 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?

Key Management Infrastructure



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