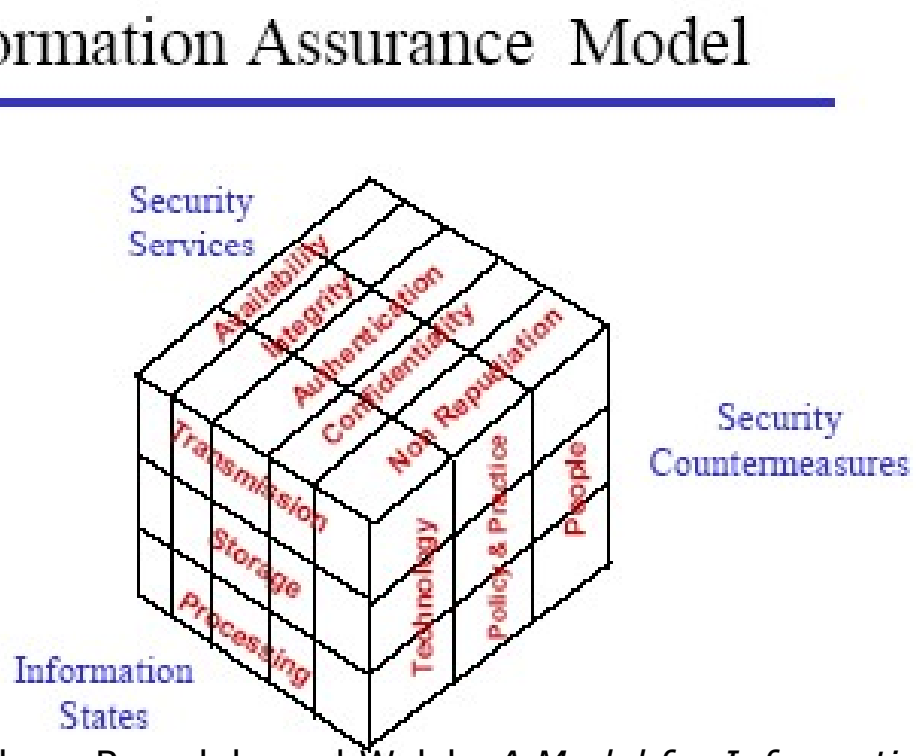
Information Assurance and Security: Overview

Information Assurance

"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

National Information Assurance (IA) Glossary

Maconachy, Schou, Ragsdale (MSR) Cube



Maconachy, Schou, Ragsdale and Welch, *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on IAS, USMA, West Point, NY 5-6 June 2001.

Security Services:
What types of problems can occur?

- Confidentiality
- Integrity
- Availability
- Authentication
- Non Repudiation

Confidentiality

"the assurance that information is not disclosed to unauthorized persons, processes or devices."

Maconachy, Schou, Ragsdale and Welch, *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on IAS, USMA, West Point, NY 5-6 June 2001.

Integrity

"the assurance that data can *not* be created, changed, or deleted without proper authorization"

Wikipedia: Information Assurance

Availability:

"Timely, reliable access to data and information services for authorized users."

Maconachy, Schou, Ragsdale and Welch, *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on IAS, USMA, West Point, NY 5-6 June 2001.

Authentication

Security service "designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information"

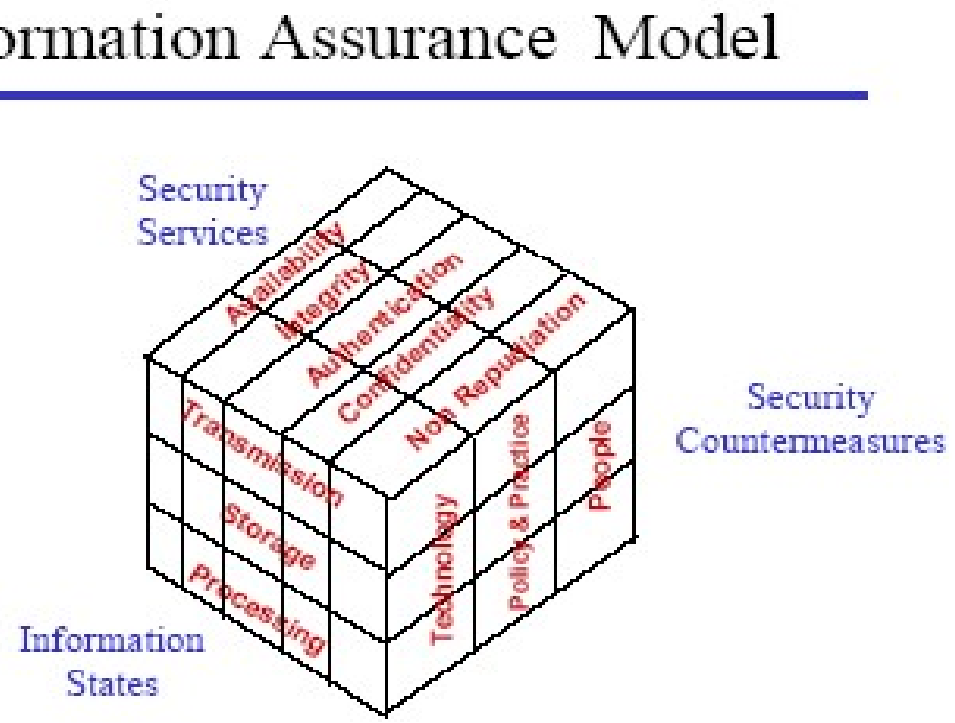
National Information Assurance (IA) Glossary

Non-Repudiation

"The assurance the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data"

Maconachy, Schou, Ragsdale and Welch, *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on IAS, USMA, West Point, NY 5-6 June 2001.

Maconachy, Schou, Ragsdale (MSR) Cube



Maconachy, Schou, Ragsdale and Welch, *A Model for Information Assurance: An Integrated Approach*, Proceedings of the 2001 IEEE Workshop on IAS, USMA, West Point, NY 5-6 June 2001.

Information States:

Where is the data?

- Transmission
- Storage
- Processing

Transmission

Time in which the data is in transit between processing/process steps.

Storage

Time during which data is on a persistent medium such as a hard drive or tape.

Processing

Time during which the data is actually in the control of a processing step.

Security Countermeasures:
Who can enforce/check security?

- People
- Policy and Practice
- Technology

People

- The heart and soul of secure systems.
- Awareness, literacy, training, education in sound practice.
- Must follow policy and practice or the systems will be compromised no matter how good the design!
- Both strength and vulnerability.

Policy and Practice (operations)

- System users
- System administrators
- Software conventions
- Trust validation

Also a countermeasure and a vulnerability.

Technology

- Evolves rapidly
- Crypto systems
- Hardware
- Software
- Network
  - Firewalls
  - Routers
  - Intrusion detection
  - Other….
- Platform
  - Operating systems
  - Transaction monitoring
  - Other….
- Especially vulnerable to misconfiguration and other "people" errors. (Does what we tell it to!)

Time

- Relationships between all parts change over time…

The attack model.

- Threat: Something that might happen
- Vulnerability: point in the system where a Threat could compromise the system.
- Risk: The combination of the probability of an event and its consequences
- Attack: Application of a threat to a system.
- Exploit: A successful attack
- Remediation: security team tries to figure out what happened and come up with a fix to restore things and a countermeasure.
- Countermeasure: What you do to fix a vulnerability so the threat can't be exploited.

Vulnerabilities, Threats and Attacks

- A vulnerability is a weakness in the system that might be exploited to cause loss or harm (and a violation of security services).
- A threat is a potential violation of security. Security services counter threats.
- An attack is the actual attempt to violate security. It is the manifestation of the threat.

Classifying Communication Attacks

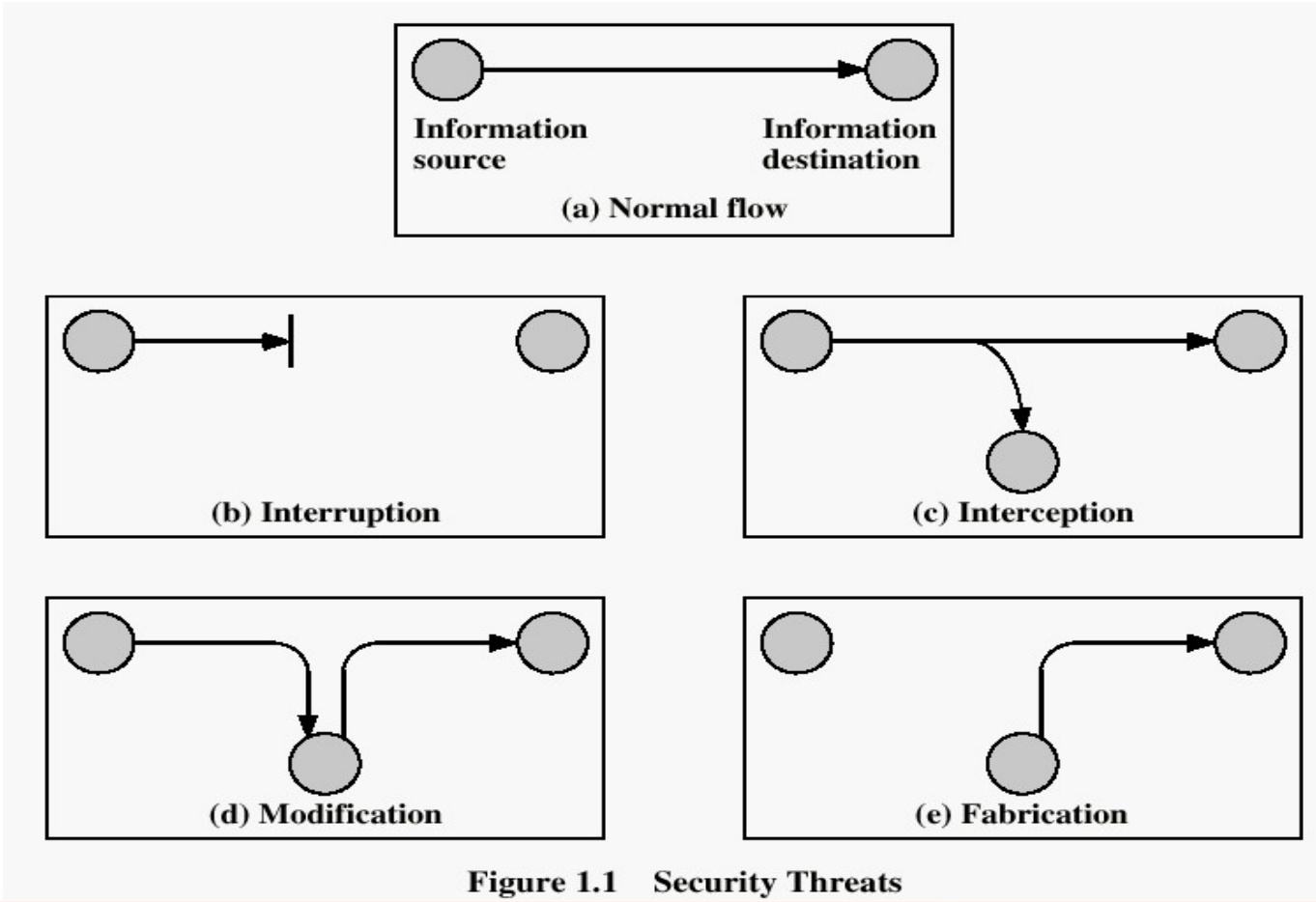


Figure 1.1 Security Threats

Types of Attacks

- Interruption: This is an attack on availability
- Interception: This is an attack on confidentiality
- Modification: This is an attack on integrity
- Fabrication: This is an attack on integrity

Additional Threats/Attacks

- **Repudiation of origin** – a false denial that an entity sent or created something (I didn't send that order to but Enron stock the day before it crashed). Attack on integrity
- **Denial of receipt** – a false denial that an entity received some information or message. (I didn't receive the diamond shipment). Attack on integrity and availability.
- **Denial of Service** – long term inhibition of information or service. Attack on availability.

Passive and Active Threats

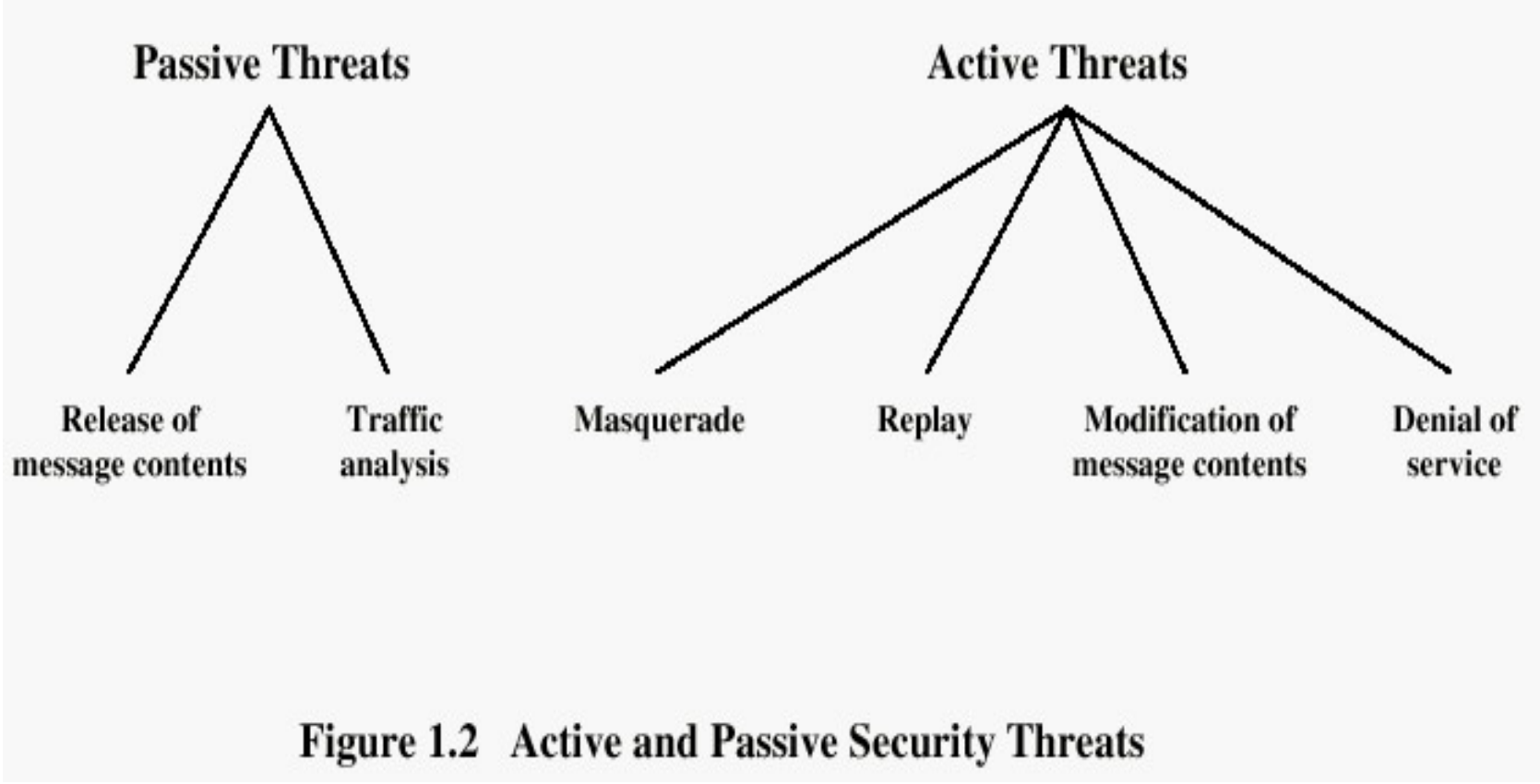


Figure 1.2 Active and Passive Security Threats

Security Policy and Mechanisms

- A **security policy** is a statement of what is and is not allowed.
- A **security mechanism** is a method, tool, or procedure for enforcing security policy.

- These should clearly be separate things.

Policy and Mechanism Example

- Policy – only the systems administrator is allowed to access the password file and then only in encrypted form
- Mechanism – the password file is not stored in clear text, but only in encrypted form with algorithm XYZ. The O.S. checks the access authorization of any process attempting to read the password file immediately before the access; whenever access is denied, that attempt is recorded in a log of suspicious activity.

Security Mechanisms

- Prevention, Detection, Recovery
- Prevention:
  - Encryption
  - Software Controls (DB access limitations, operating system process protection)
  - Enforce policies (frequent password change)
  - Physical Controls
- Detection: Intrusion detection systems (IDS)

Prevention Mechanisms

- Adequate prevention means that an attack will fail. Prevention usually involves mechanisms that the user cannot override.
- Prevention mechanisms are often cumbersome and do not always work perfectly or fail because they are circumvented.
- Passwords are a prevention mechanism to prevent unauthorized access. They fail when the password becomes known to a person other than the owner.

Detection Mechanisms

- Detection is used when an attack cannot be prevented and it also indicates the effectiveness of prevention measures.
- The goal is to determine that an attack is underway or has occurred and report it.
- Audit logs are detection mechanisms. When you log into the design center's unix servers, it gives you the IP address of the last successful login.

Recovery

- Recovery has several aspects. The first is to stop an attack and repair the damage.
- Another is to trace the evidence back to the attacker and discover the identity of the attacker (this could result in legal retaliation).
- Yet another aspect is to determine the vulnerability that was exploited and fix it or devise a way of preventing a future attack.

Example: Private Property

- **Prevention:** locks at doors, window bars, walls round the property
- **Detection:** stolen items are missing, burglar alarms, closed circuit TV
- **Recovery:** call the police, replace stolen items, make an insurance claim …

Example E-Commerce

- **Prevention:** encrypt your orders, rely on the merchant to perform checks on the caller, don't use the Internet (?) …
- **Detection:** an unauthorized transaction appears on your credit card statement
- **Recovery:** complain, ask for a new card number, etc.
- *Footnote: Your credit card number has not been stolen. Your card can be stolen, but not the number. Confidentiality is violated.*