Computer and Distributed Security: Introductory Overview for Researchers

Konstantin Beznosov
beznosov@cs.fiu.edu

Presentation at CADSE, FIU
October 2, 1998

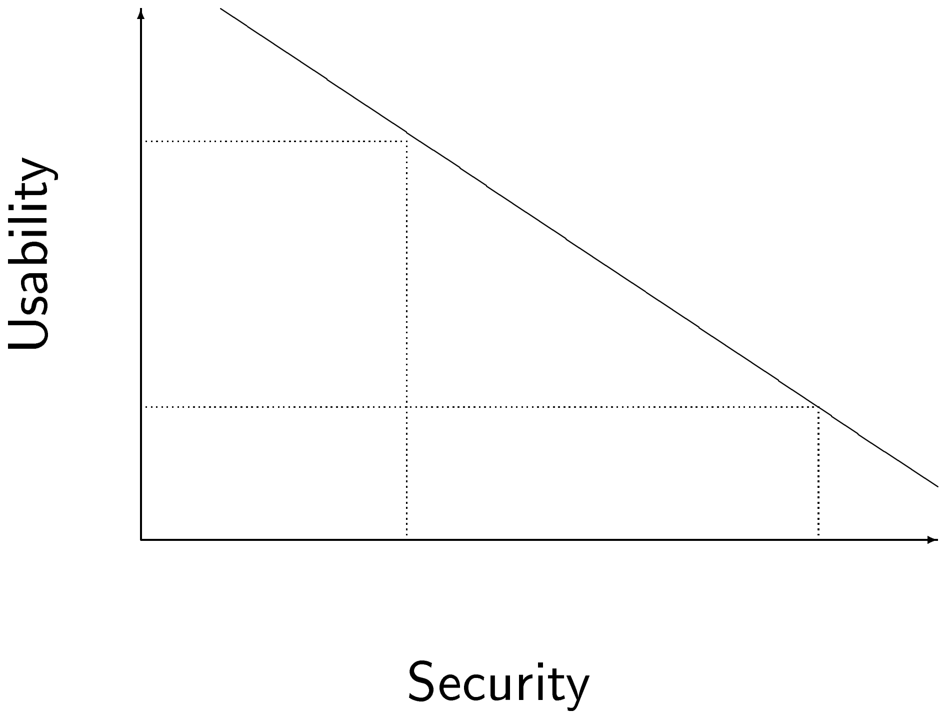
We Will Discuss Today:

- What is security of computer systems
- Security and usability
- The main challenge for security
- Threats, Vulnerabilities, and Attacks
- Security Concerns
- Distributed Security
- Security Functionalities
- Summary
- References

What is security of computer systems

- Security – "the quality or state of being secure" [5]
- Secure – "free from danger; free from risk of loss; affording safety" [5]
- "The goal of computer security is to provide *insights, techniques, and methodologies* that can be used to *mitigate threats*." [2]

Security and Usability[1]



[1] From [2]

The Main Challenge for Security Research and Practice

How do we build computer systems that are:

- secure
- useful
- cost-effective
  - require reasonable resources to
    - design
    - test
    - implement
    - administrate
    - maintain
    - deploy
- efficient
- etc.

Threats, Vulnerabilities, and Attacks

From [2]:

- "A THREAT to a computer system is any potential occurrence, malicious or otherwise, that can have an undesirable effect on the assets and resources associated with a computer system."

- "A VULNERABILITY of a computer system is some unfortune characteristic that makes it possible for a threat to potentially occur."

- "An ATTACK on a computer system is some action taken by a malicious intruder that involves the exploitation of certain vulnerabilities in order to cause an existing threat to occur."

Main Types of Threats

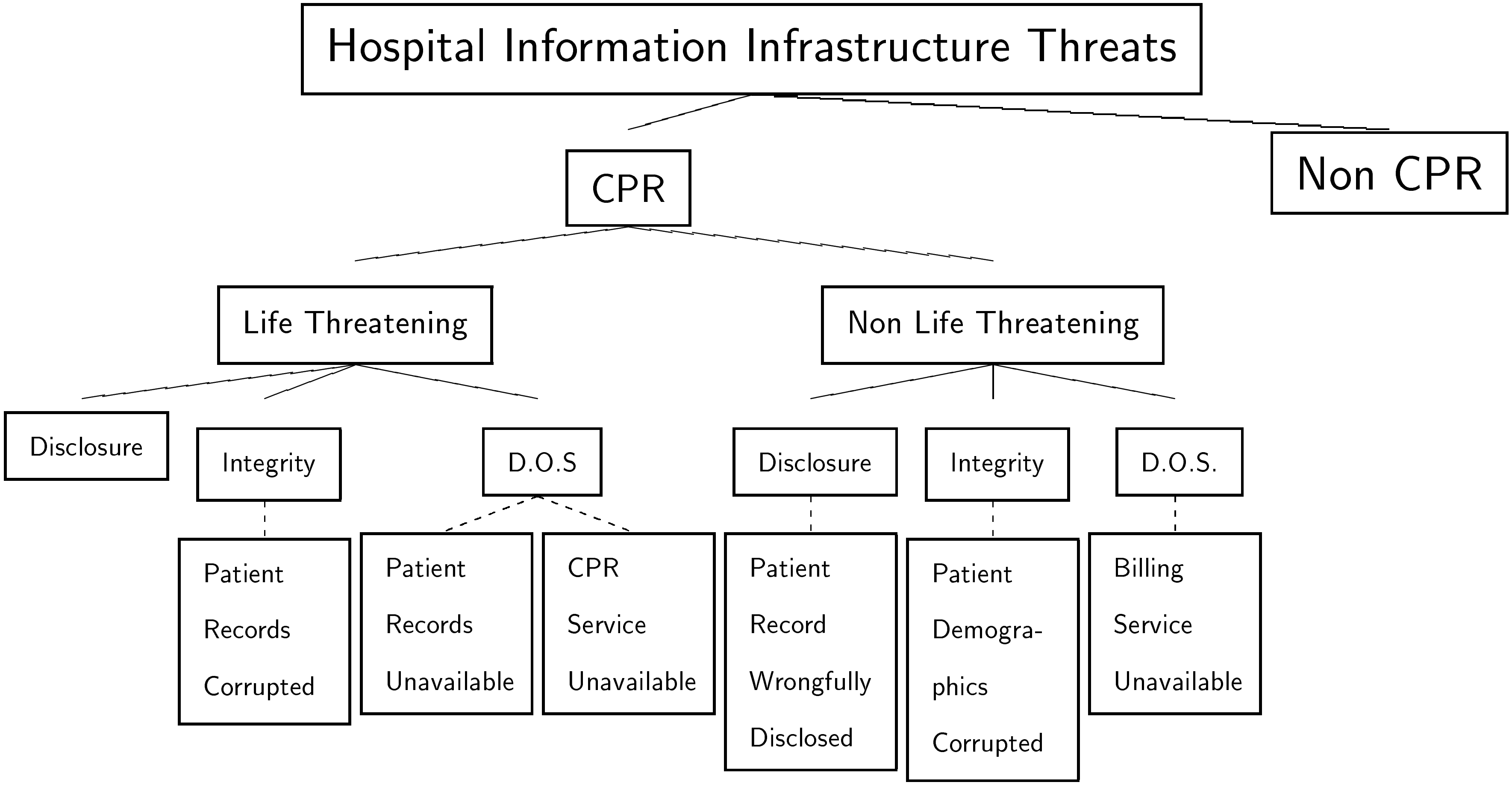
From [2]:

- DISCLOSURE – "dissemination of information to an individual for whom that information should not be seen."

- INTEGRITY – "unauthorized change to information stored on a computer system or in transit between computer systems."

- DENIAL OF SERVICE – "access to some computer system resource is intentionally blocked as a result of malicious action taken by another user."

Threat Tree Example


Hospital Information Infrastructure Threats
CPR
Non CPR
Life Threatening
Non Life Threatening
Disclosure
Integrity
D.O.S
Disclosure
Integrity
D.O.S.
Patient Records Corrupted
Patient Records Unavailable
CPR Service Unavailable
Patient Record Wrongfully Disclosed
Patient Demogra-phics Corrupted
Billing Service Unavailable

Threats: Probability, Damage, Effort, Criticality and Risk

- PROBABILITY of occurrence
- potential DAMAGE ≈ CRITICALITY
- level of EFFORT required to enact the threat
- RISK
  - risk $== \frac{criticality}{effort}$
  - risk $== damage * probability$

Security Concerns

- From [6]:

  Confidentiality – Information is disclosed only to users authorized to access it.

  Integrity Information is modified only by users who have the right to do so, and only in authorized ways. It is transferred only between intended users and in intended ways.

  Accountability – Users are accountable for their security-relevant actions.

  Availability – Use of the system cannot be maliciously denied to authorized users.

Distributed Security

- Distributed systems are different in the following ways from stand-alone computer systems from the point of view of security [3]:

  1. Have many components
  2. Have rich interactions between components
  3. Can introduce intricate boundaries of trust

Security Functionalities/Services

- Security Service – "a combination of functional and data elements that are exercised through a well defined interfaces, provided by a security infrastructure, which ensures adequate security of computing information resources" [3]
  - Authentication
  - Access Control / Authorization
  - Communication Confidentiality
  - Communication Integrity
  - Communication Authenticity
  - Data Semantic Integrity
  - Audit
  - Non-repudiation

Authentication

“making sure that a user or a service is who they claim to be” [7]

Authentication approaches [2]: something known, something embodied, something possessed

Result of authentication – a set of the user credentials: identity (for access, audit, non-repudiation), roles, affiliations, clearance

Research Issues:

- Strong, convenient, cheap, configurable authentication
- “Single Sign on”
- Delegation of credentials & composition of delegated credentials
- Anonymous identity
- Identity relationships in federations

Access Control

"making and enforcing authorization decisions" [7]

Mandatory Access Control (MAC) – "enforces the specified mediation at the discretion of a centralized system administration facility" [2]

Discretionary Access Control (DAC) – "enforces the specified mediation at the discretion of individual users" [2]

Authorization

"making decisions about what users and what services can access what system services and endorsing those decisions" [7]

Access Matrices, "Who to what?" vs "What by whom?"

Popular types of authorization mechanisms:

- Security Labels – confidentiality and integrity labels
- Permission Mechanisms (ala Unix permission bits)
- Access Control Lists (ACL – [akl])

Authorization Research Areas

- Fine-grain authorization v.s. scalability

- Role-based authorization (RBAC)

- Federations

- Support for policies specific to particular vertical domains (healthcare, finance, electronic commerce, military)

- Decoupling authorization logic from application logic in COTS

- System property verification: "deadlocks", who has access to what, what can be accessed by whom.

- "Soft" access control

Communication Protection

Communication confidentiality – protecting communicated data from unauthorized disclosure

Communication integrity – protecting communicated data from unauthorized modifications

Communication authenticity – protecting communicated data from impersonation

Research Areas:

- See “Cryptography”

Data Semantic Integrity

Application-specific data integrity

- Example: Errors in critical applications such as atomic stations, planes, killing systems, healthcare systems

Research Areas:

- Semantic integrity checks

Cryptography

Research areas:

- Hard computational problems
  - Worst-case/average-case equivalence [1]
- Two-party computation protocols (e.g. notary signature) and Zero-knowledge protocols
- Interactive and probabilistic proof systems
- Pseudo randomness
- Proof techniques
- Distributed cryptography
- More in [4]

Audit

Research areas:

- audit log analysis: detailed “recreation of picture” and real-time alerts
- selection of “interesting” events

Non-repudiation

“protecting against originator of a message or action denying that it originated the message or the action as well as against the recipient of a message or action denying that they have received the message or was requested action” [7]

Example: Proving that service was provided in telecommunication market

Research Areas:

- Generating and storing evidence

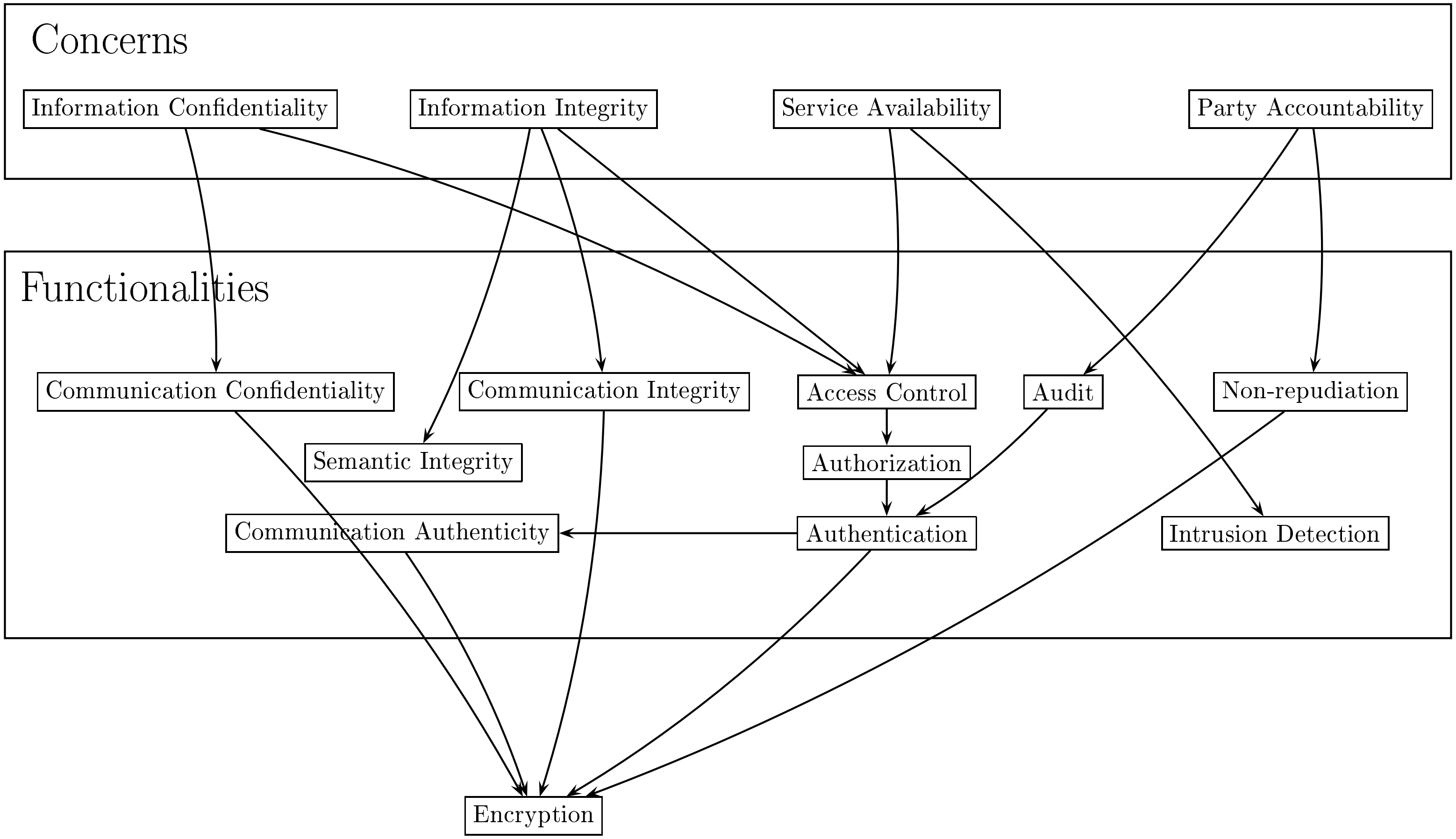
Intrusion Detection

It can be cheaper to detect intrusions than to control them

Traffic analysis

Event sequence analysis

Patterns


Concerns
Information Confidentiality
Information Integrity
Service Availability
Party Accountability
Functionalities
Communication Confidentiality
Communication Integrity
Access Control
Audit
Non-repudiation
Semantic Integrity
Authorization
Communication Authenticity
Authentication
Intrusion Detection
Encryption

Summary

Threat is a potential occurrence that can have an undesirable effect on the system assets and resources.

Vulnerability is an unfortune characteristic that makes it possible for a threat to potentially occur

Attack is an action that involves the exploitation of certain vulnerabilities in order to cause an existing threat to occur

Security **Concerns**: Information Confidentiality, Information Integrity, Party Accountability, Service Availability

Security **Functionality** can be decomposed into: Authentication, Communication Confidentiality, Communication Integrity, Communication Authenticity, Access Control/Authorization, Audit, Non-repudiation

References

[1] Miklos Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of Symposium on Theory of Computing*, pages 284–293. IBM, May 1997.

[2] Edward Amoroso. *Fundamentals of Computer Security Technology*. AT&T Bell Laboratories, 1994.

[3] Belinda Fairthorne. OMG white paper on security. OMG document number 1994/94-04-16, April 1994.

[4] Shafi Goldwasser. New directions in cryptography: Twenty some years later. In *Crypto '97*, pages 314–324, 1997.

[5] Merian-Webster. *Merriam Webster's Collegiate Dictionary*, 10th edition, 1994.

[6] Object Management Group. *CORBAservices: Common Object Services Specification, Security Service Specification*, 1996.

[7] Wayne Wilson and Konstantin Beznosov. *CORBAmed Security White Paper*. Object Management Group, November 1997. OMG document number: corbamed/97-11-03.