CS-552

CYBER FORENSICS

Introduction

WHAT SECURITY IS ABOUT IN GENERAL?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

REAL WORLD EXAMPLE

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, burglar alarms, closed circuit TV
- Reaction
  - attack on burglar (not recommended ☺), call the police, replace stolen items, make an insurance claim

INTERNET SHOPPING EXAMPLE

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don’t send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue (if you can find of course ☺)
  - Or, pay and forget (a glass of cold water) ☺

INFORMATION SECURITY IN PAST & PRESENT

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general: physical and administrative mechanisms
- Modern World
  - Data are in computers
  - Computers are interconnected

Computer and Network Security

TERMINOLOGY

- Computer Security
  - 2 main focuses: Information and Computer itself
  - tools and mechanisms to protect data in a computer (actually an automated information system), even if the computers/system are connected to a network
  - tools and mechanisms to protect the information system itself (hardware, software, firmware, *ware ☺)
- Against?
  - against hackers (intrusion)
  - against viruses
  - against denial of service attacks
  - etc. (all types of malicious behavior)

TERMINOLOGY

- Network and Internet Security
  - measures to prevent, detect, and correct security violations that involve the transmission of information in a network or interconnected networks

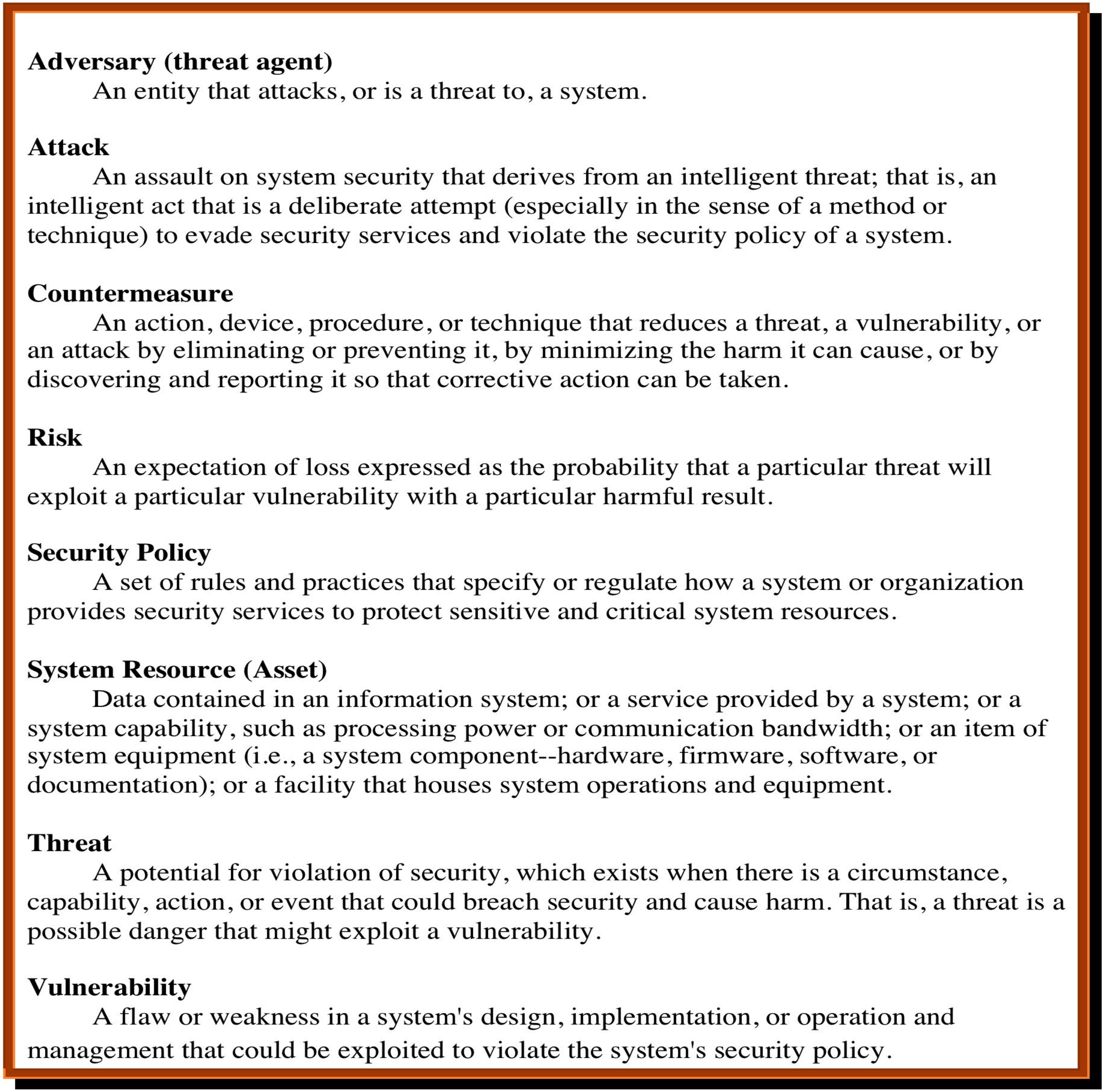
A NOTE ON SECURITY TERMINOLOGY

- No single and consistent terminology in the literature!
- Be careful not to confuse while reading papers and books

- See the next slide for some terminology taken from Stallings and Brown, Computer Security who took from RFC4949, Internet Security Glossary

COMPUTER SECURITY TERMINOLOGY

RFC 4949, *INTERNET SECURITY GLOSSARY*, MAY 2000



Adversary (threat agent)

An entity that attacks, or is a threat to, a system.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)

Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

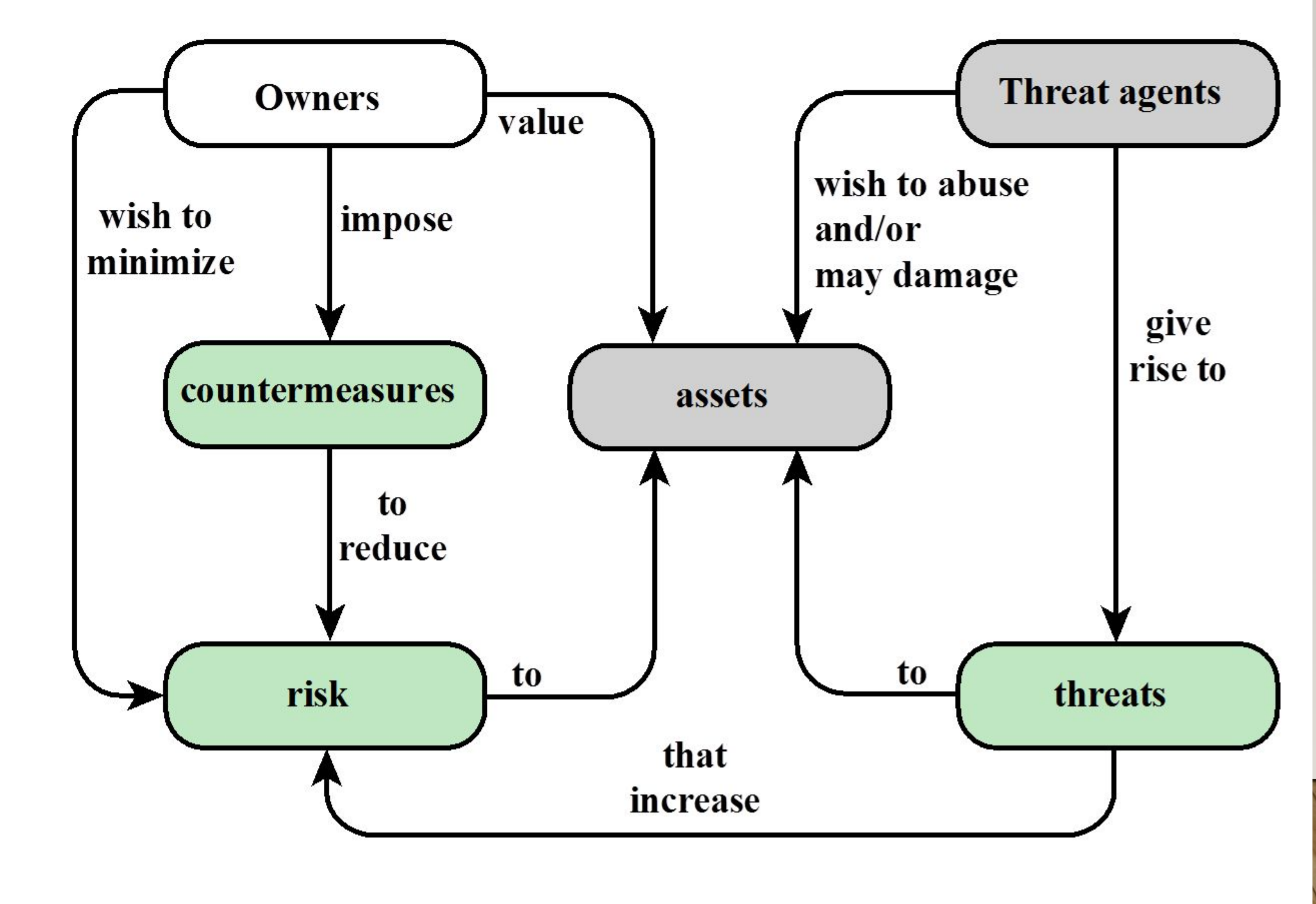
Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability

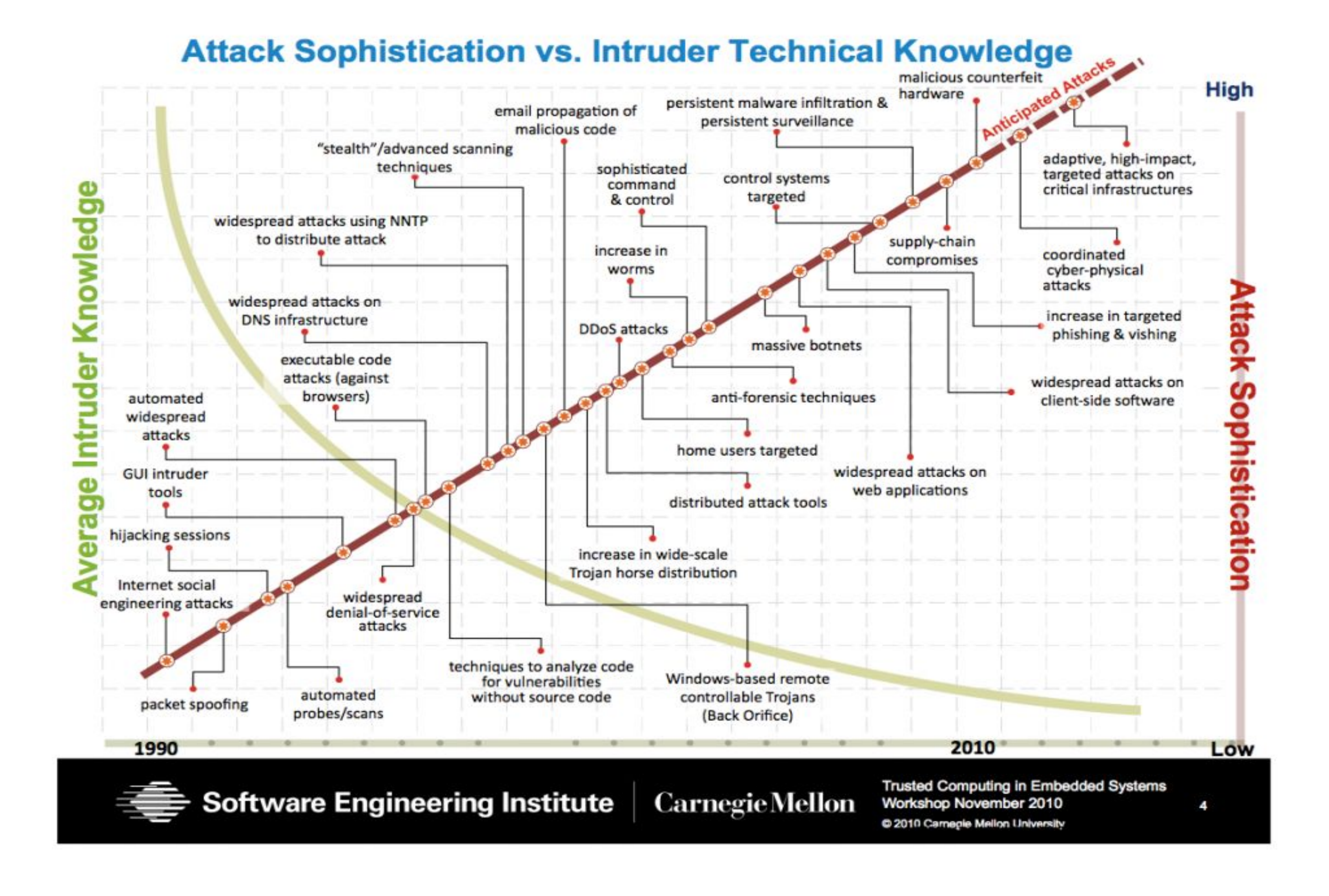
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

RELATİONSHİPS AMONG THE SECURİTY CONCEPTS



SECURITY TRENDS

Skill and knowledge required to mount an attack



Attack Sophistication vs. Intruder Technical Knowledge

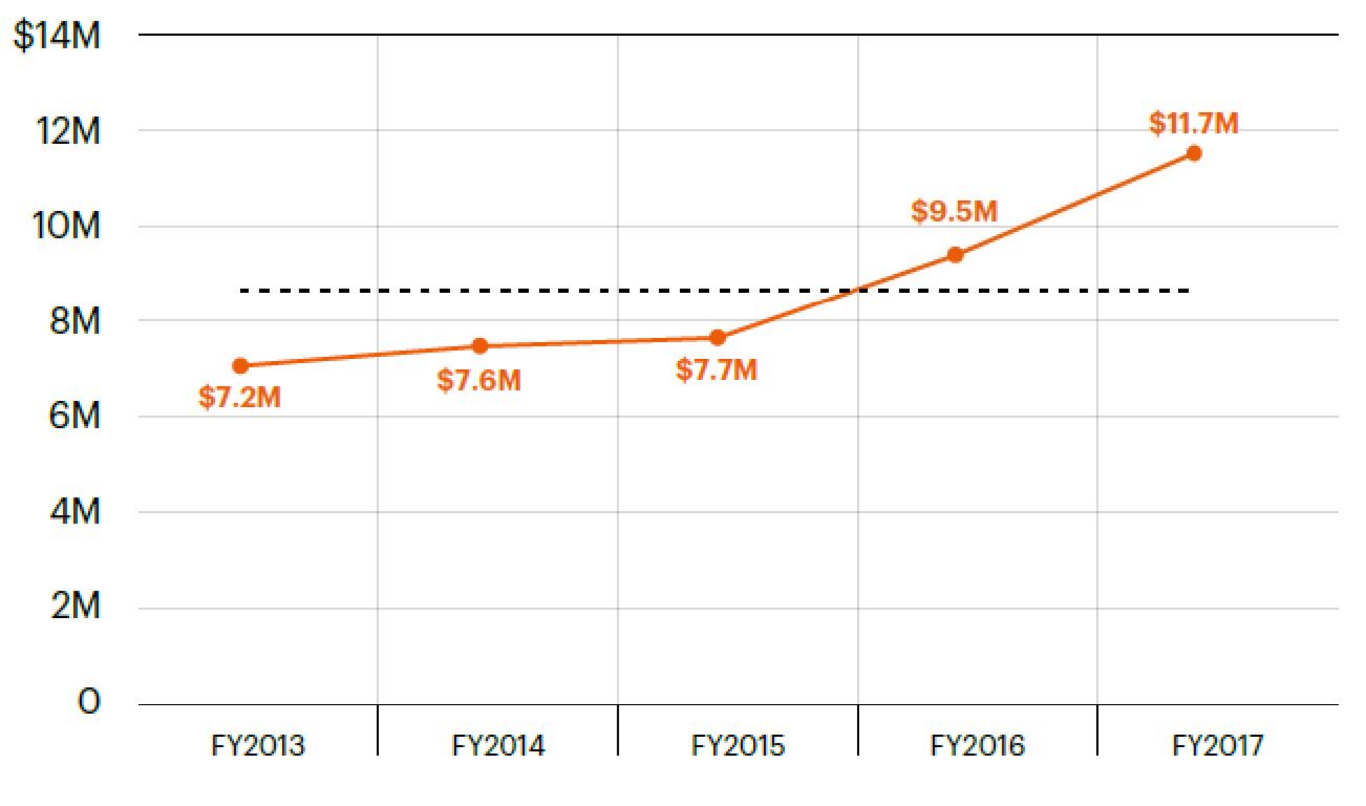
Software Engineering Institute | Carnegie Mellon

Trusted Computing in Embedded Systems Workshop November 2010

© 2010 Carnegie Mellon University

4

THE GLOBAL AVERAGE COST OF CYBER CRIME/ATTACKS

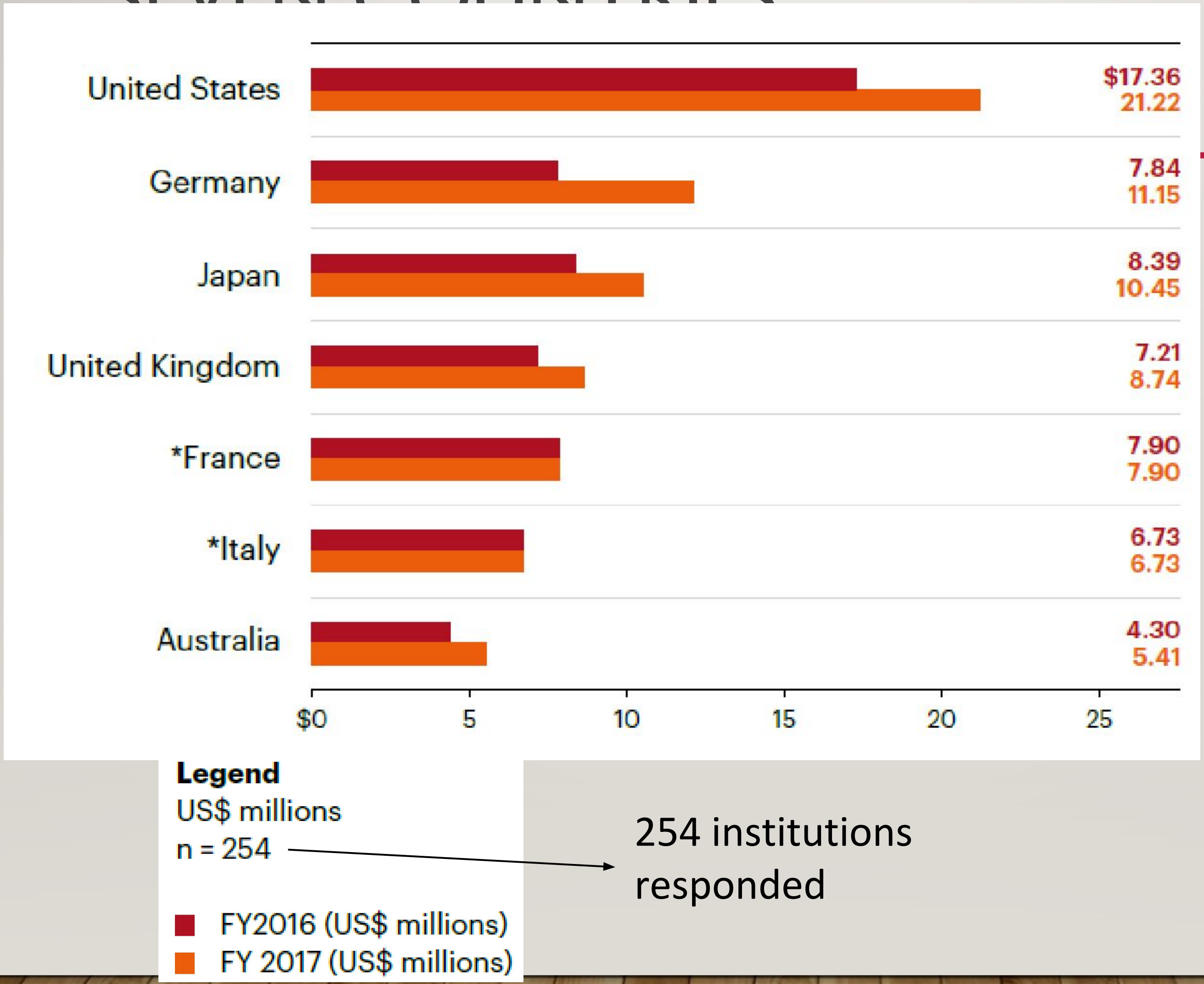


2017 Cost of Cyber Crime Study by Accenture*

Steeper increasing trend in the recent years

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

AVERAGE COST OF CYBER CRIME FOR SEVEN COUNTRIES



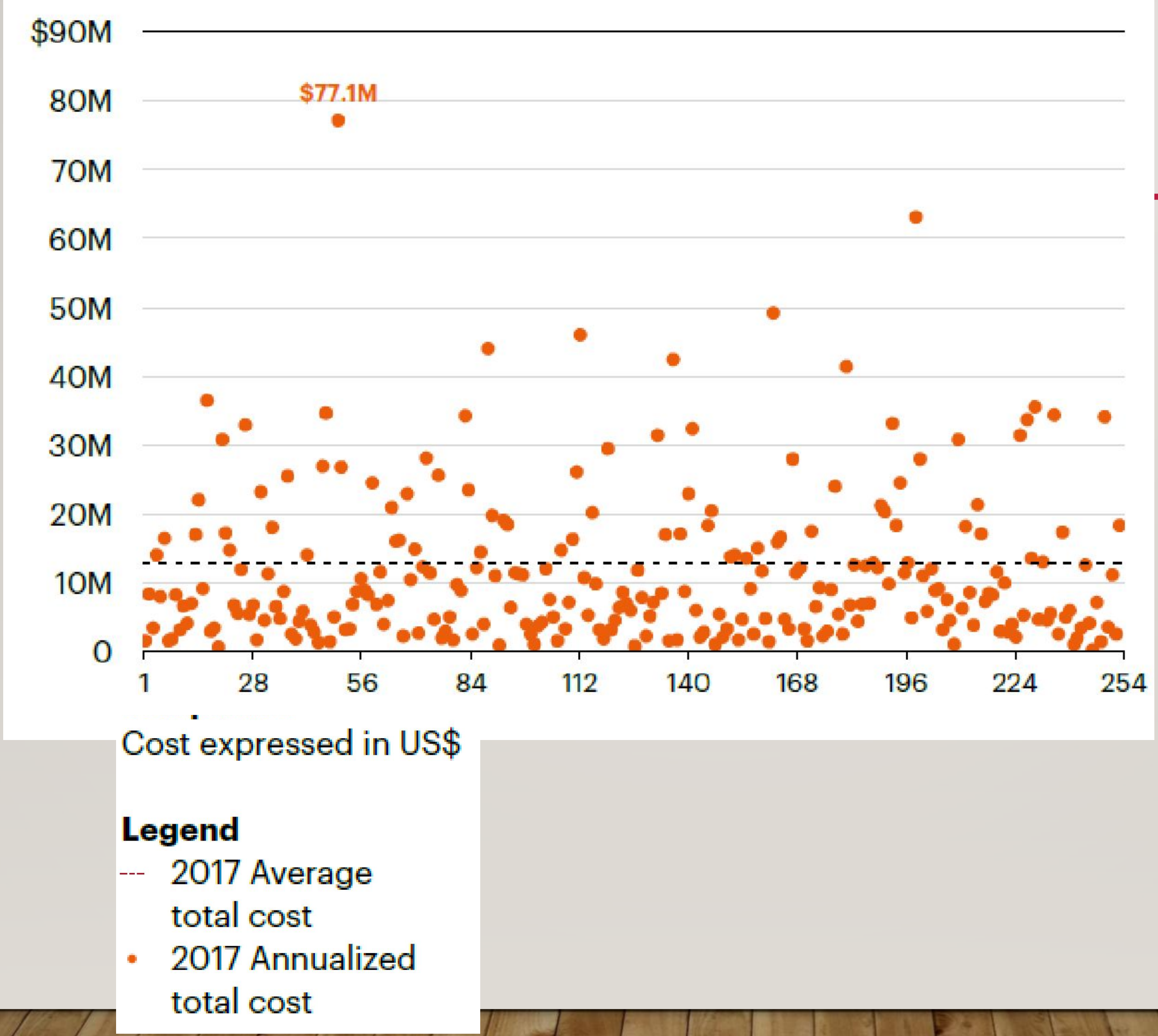
254 institutions responded

2017 Cost of Cyber Crime Study by Accenture*

- Germany has highest percentage increase;
- UK, US are around the mean in percentage increase

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

A SCATTERGRAM OF RESPONDENTS

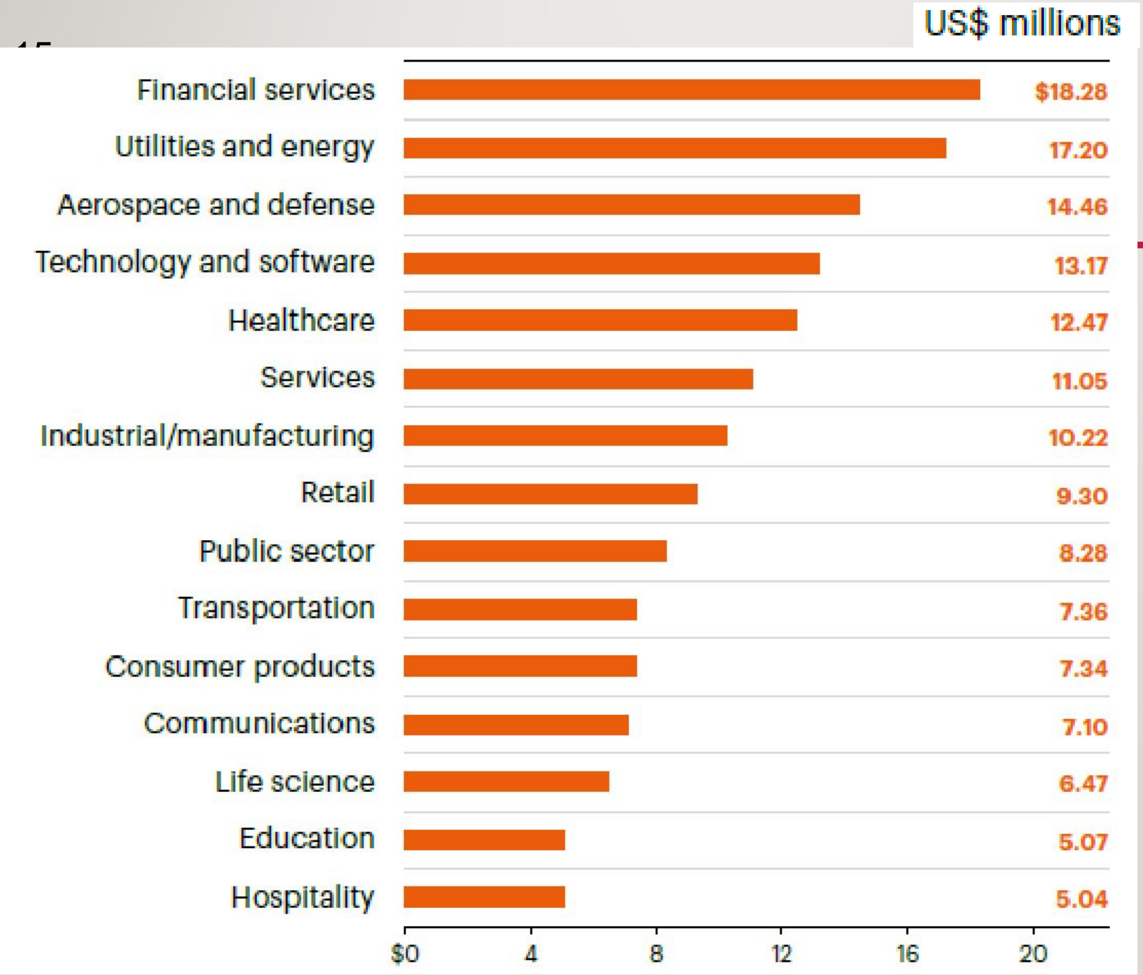


2017 Cost of Cyber Crime Study by Accenture*

- Mean is US$11.7 M
- High variance
- 163 institutions are below mean (out of 254)

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

BREAKDOWN BY SECTOR

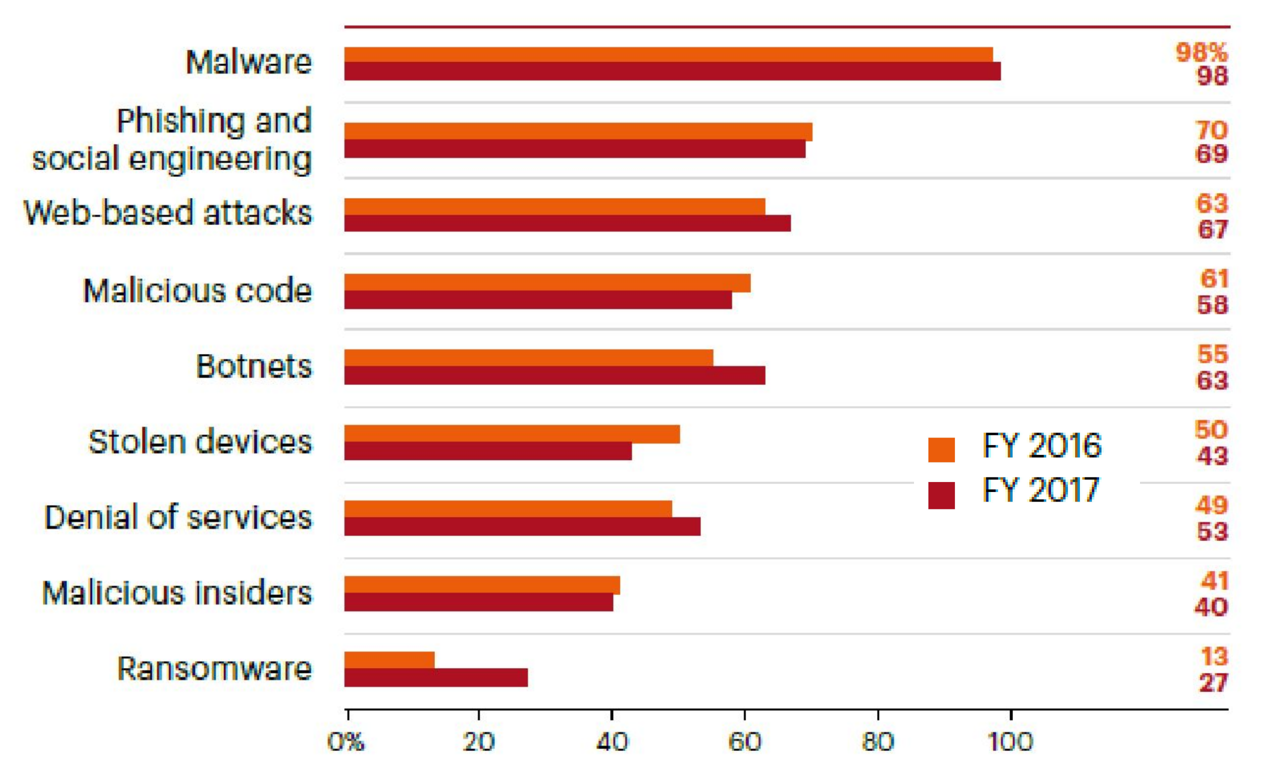


2017 Cost of Cyber Crime Study by Accenture*

- Financial Services Sector has the Highest Cost due to Cyber Crime

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

TYPES OF CYBER ATTACKS EXPERIENCED

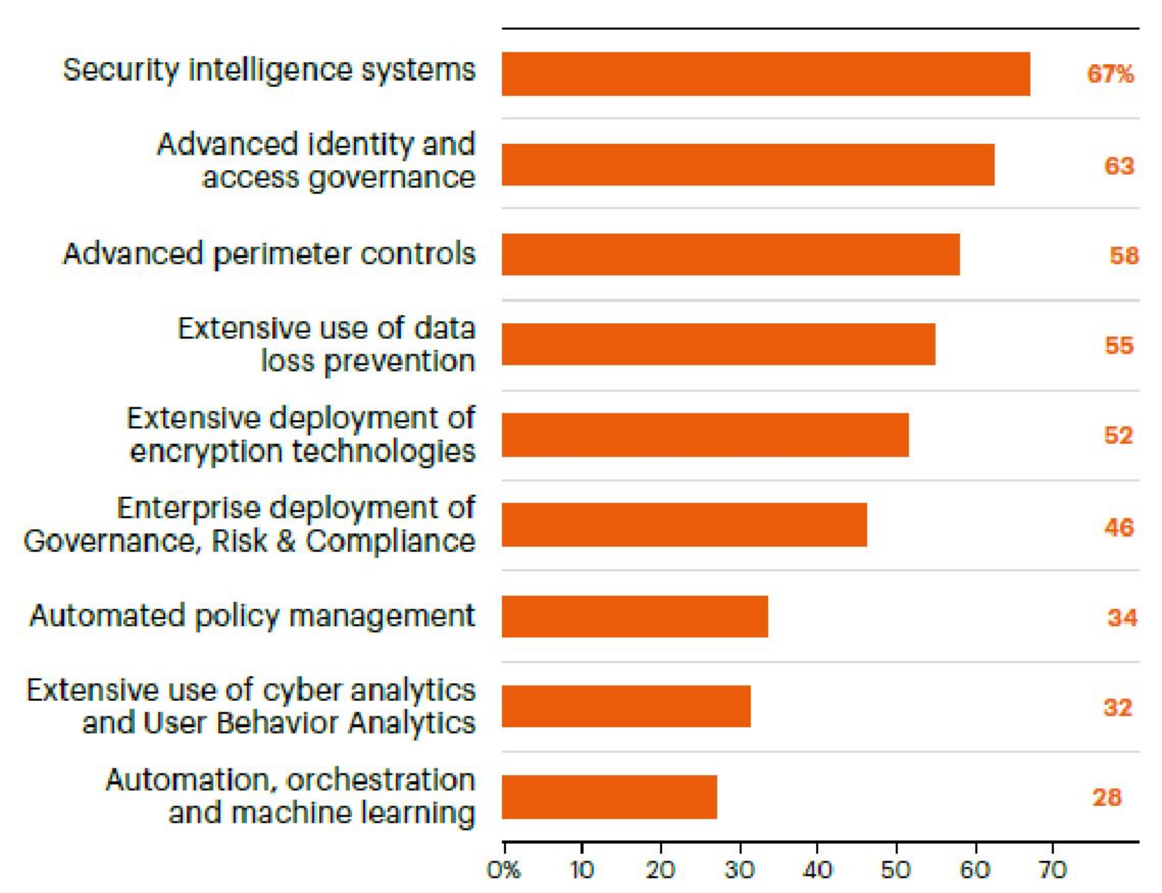


2017 Cost of Cyber Crime Study by Accenture*

- Percentage of the respondents experienced
- Ransomware doubled

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

DEPLOYMENT RATE OF SECURITY TECHNOLOGIES

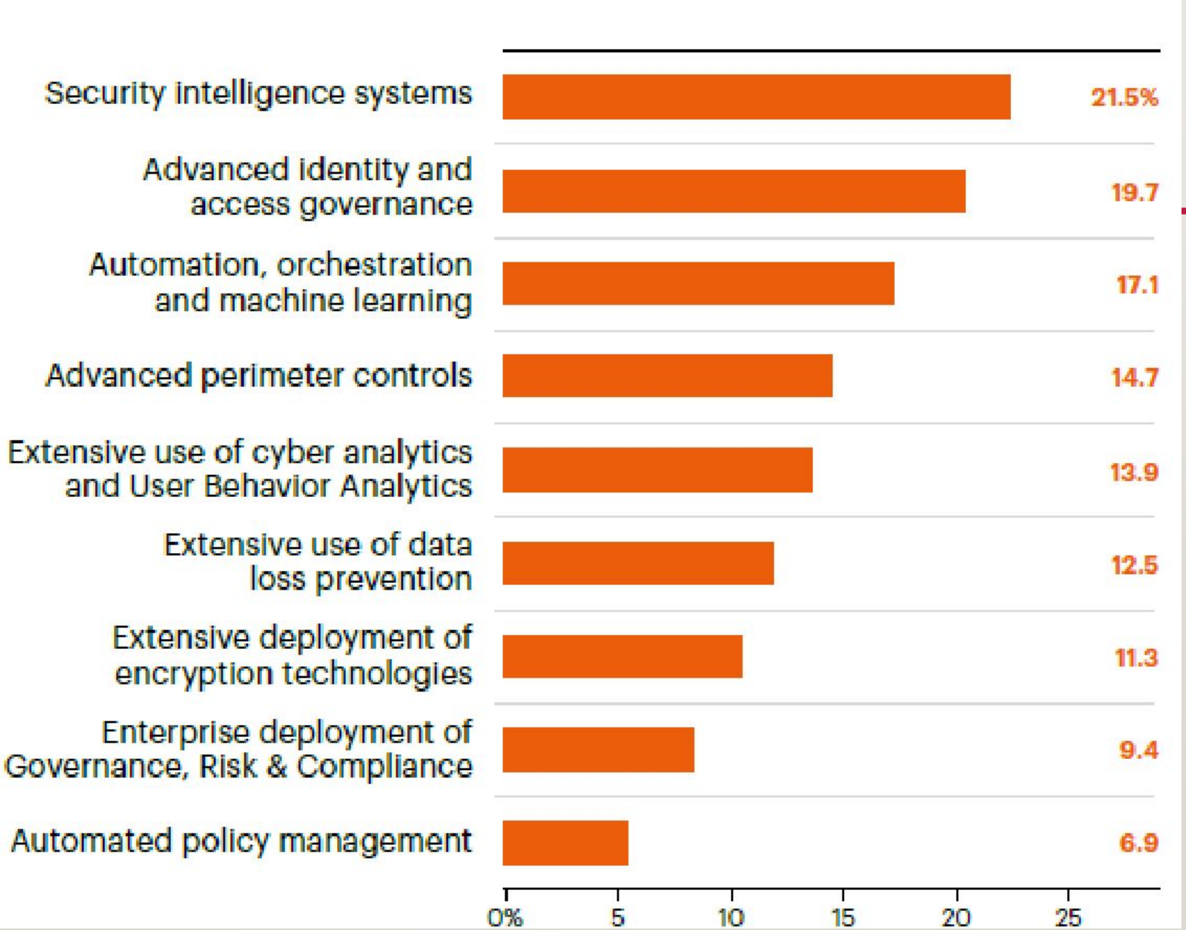


2017 Cost of Cyber Crime Study by Accenture*

- Percentage of the respondents experienced
- Ransomware doubled

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

ANNUAL RETURN OF INVESTMENT (ROI)

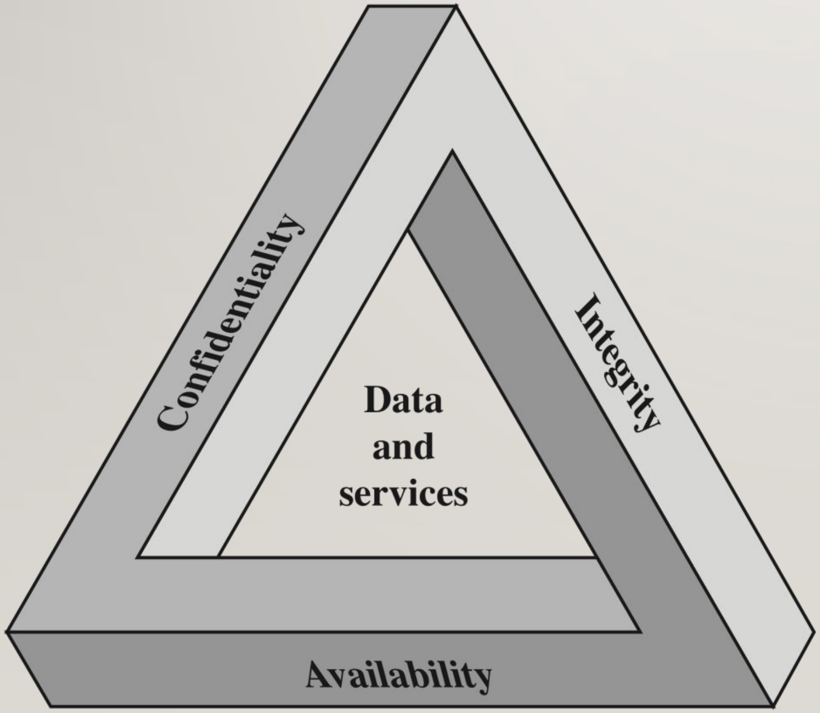


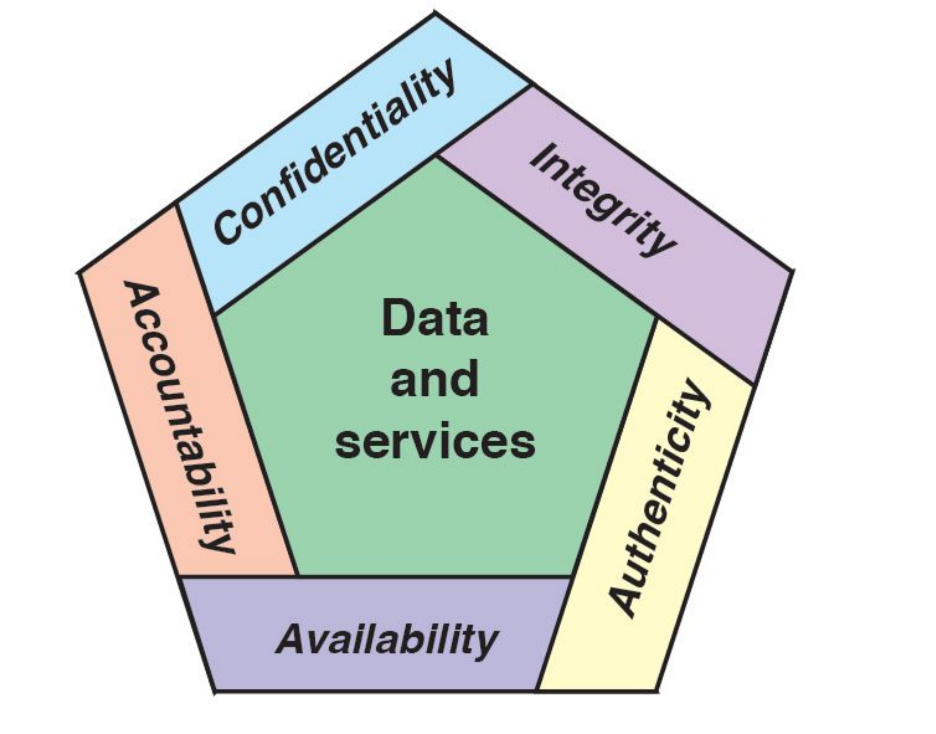
2017 Cost of Cyber Crime Study by Accenture*

- More or less in parallel with deployment rate
- But AI, Data Mining based novel techniques have higher RoI
- Bad performance for encryption and DLP, but they are needed

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

SECURITY OBJECTIVES: CIA TRIAD AND BEYOND





COMPUTER SECURITY OBJECTIVES

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

ADDITIONAL CONCEPTS:

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- Being able to trace the responsible party/process/entity in case of a security incident or action.

SERVICES, MECHANISMS, ATTACKS

- 3 aspects of information security:
  - security attacks (and threats)
    - actions that (may) compromise security
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - e.g. secrecy is a service, encryption (a.k.a. encipherment) is a mechanism

ATTACKS

- Attacks on computer systems
  - break-in to destroy information
  - break-in to steal information
  - blocking to operate properly
  - malicious software
    - wide spectrum of problems

- Source of attacks
  - Insiders
  - Outsiders

ATTACKS

- Network Security
  - Active attacks
  - Passive attacks
- Passive attacks
  - interception of the messages
  - What can the attacker do?
    - use information internally
      - hard to understand
    - release the content
      - can be understood
    - traffic analysis
      - hard to avoid
  - Hard to detect, try to prevent

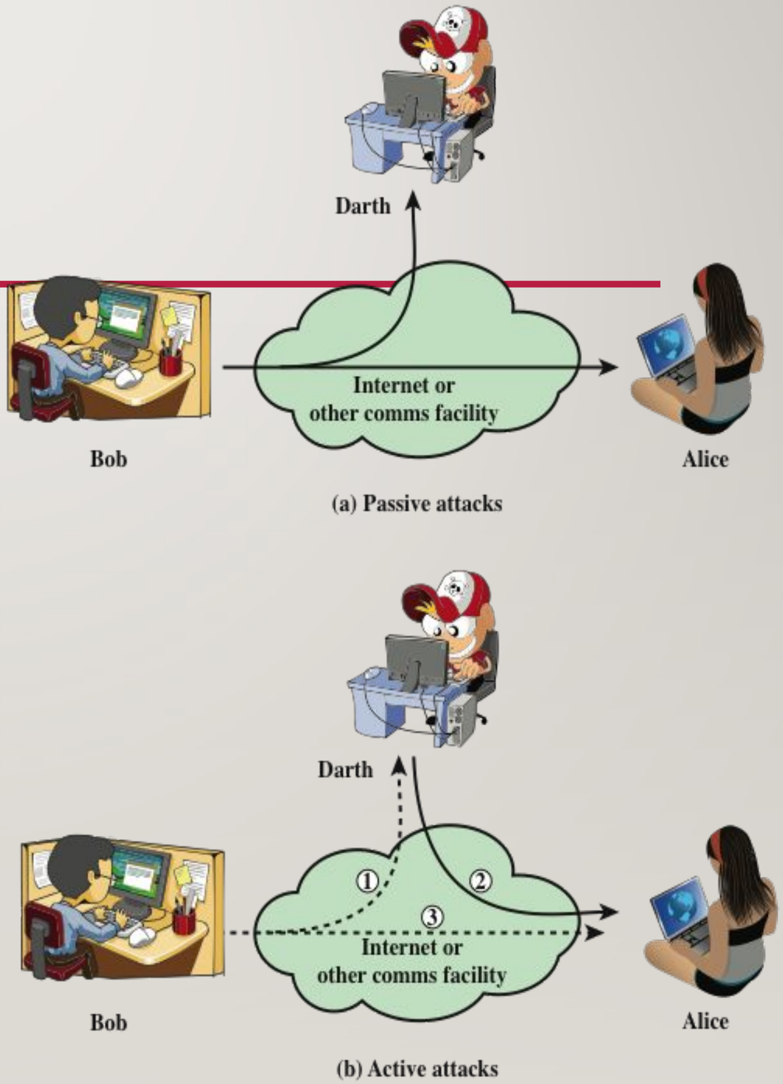
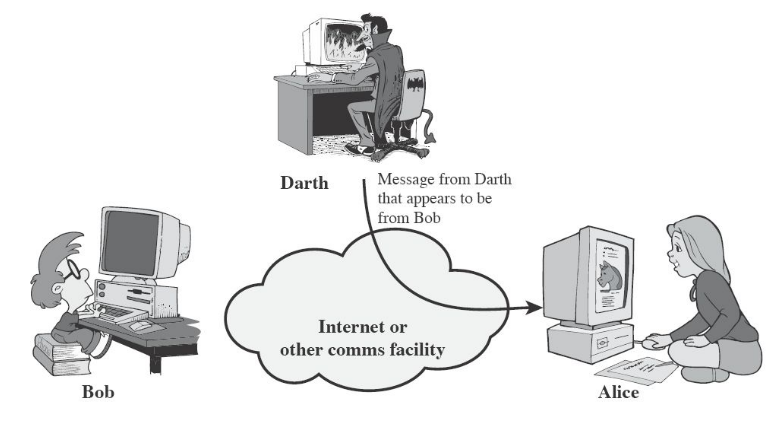
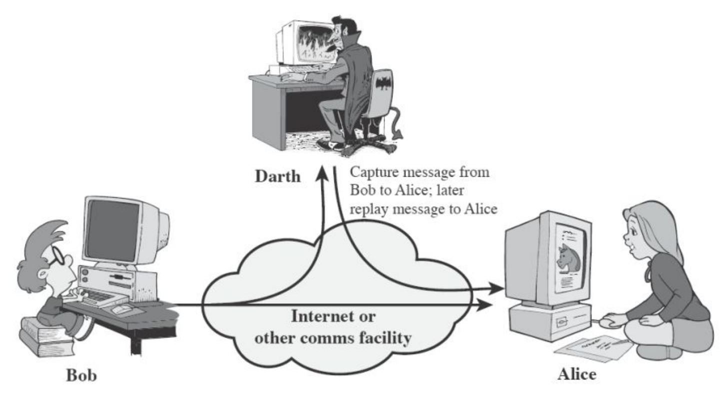


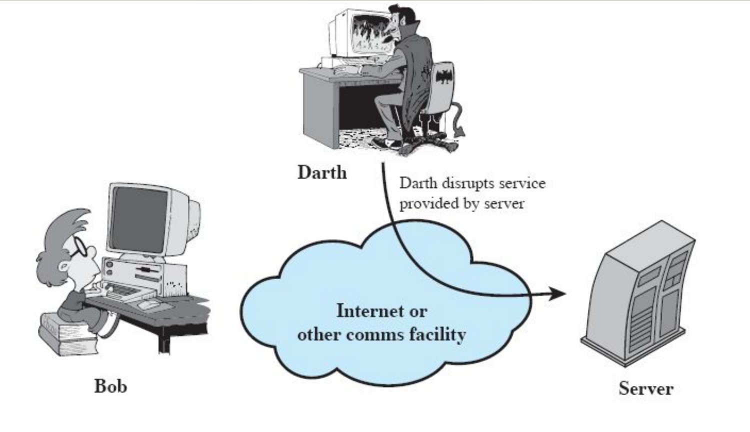
Figure 1.2 Security Attacks

ATTACKS

- Active attacks
  - Attacker actively manipulates the communication
  - Masquerade
    - pretend as someone else
    - possibly to get more privileges
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself

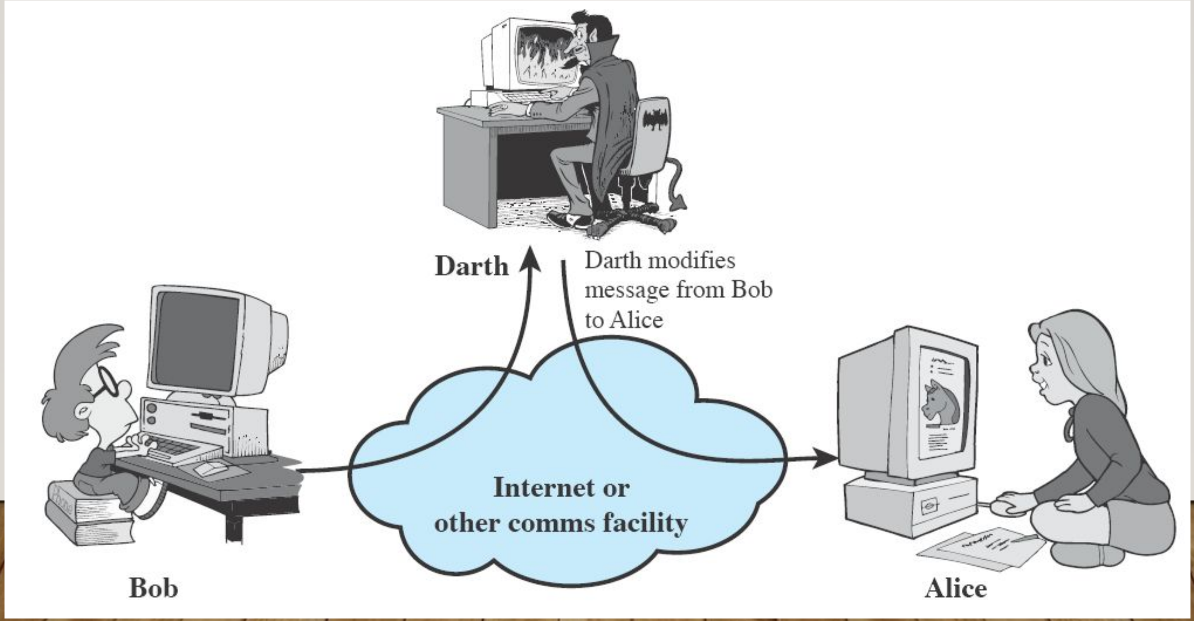

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

ATTACKS

- Active attacks (cont'd)
  - deny
    - repudiate sending/receiving a message later
  - modification
    - change the content of a message


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

SECURITY SERVICES

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates
    - need protection from disclosure, tampering, or destruction
    - notarize
    - record

BASIC SECURITY SERVICES

- Authentication
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - Data-origin authentication
    - assurance about the source of the received data
- Access Control
  - prevention of the unauthorized use of a resource
  - to achieve this, each entity trying to gain access must first be identified and authenticated, so that access rights can be tailored to the individual

BASIC SECURITY SERVICES

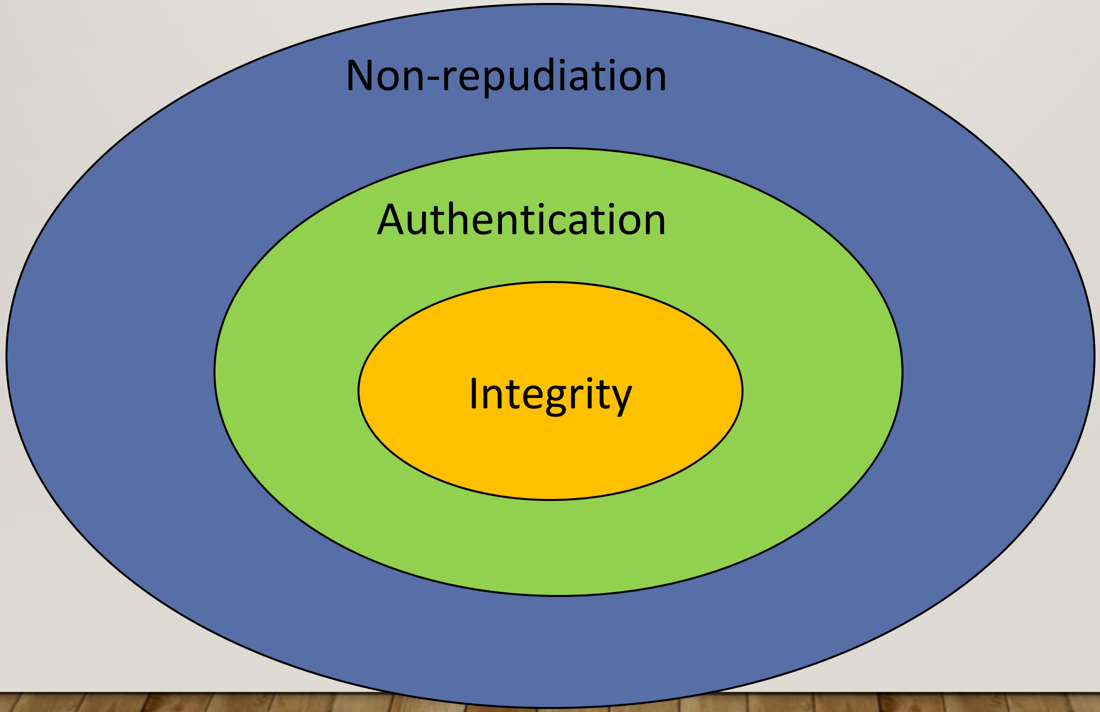
- Data Confidentiality
  - protection of data from unauthorized disclosure (against eavesdropping)
  - traffic flow confidentiality is one step ahead
    - this requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility
- Data Integrity
  - assurance that data received are exactly as sent by an authorized sender
  - i.e. no modification, insertion, deletion, or replay

BASIC SECURITY SERVICES

- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

RELATIONSHIPS

- among integrity, data-origin authentication and non-repudiation



SECURITY MECHANISMS

- Cryptographic Techniques
  - A lot of…
- Software and hardware for access limitations
  - Firewalls
- Intrusion Detection and Prevention Systems
- Traffic Padding
  - against traffic analysis
- Hardware for authentication
  - Smartcards, security tokens
- Security Policies / Access Control
  - define who has access to which resources.
- Physical security
  - Keep it in a safe place with limited and authorized physical access

CRYPTOGRAPHIC SECURITY MECHANISMS

- Encryption (a.k.a. Encipherment)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible
    - keys are involved

CRYPTOGRAPHIC SECURITY MECHANISMS

- Message Digest
    - similar to encryption, but one-way (recovery not possible)
    - generally no keys are used
- Digital Signatures and Message Authentication Codes
    - Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data
- Authentication Exchange
    - ensure the identity of an entity by exchanging some information

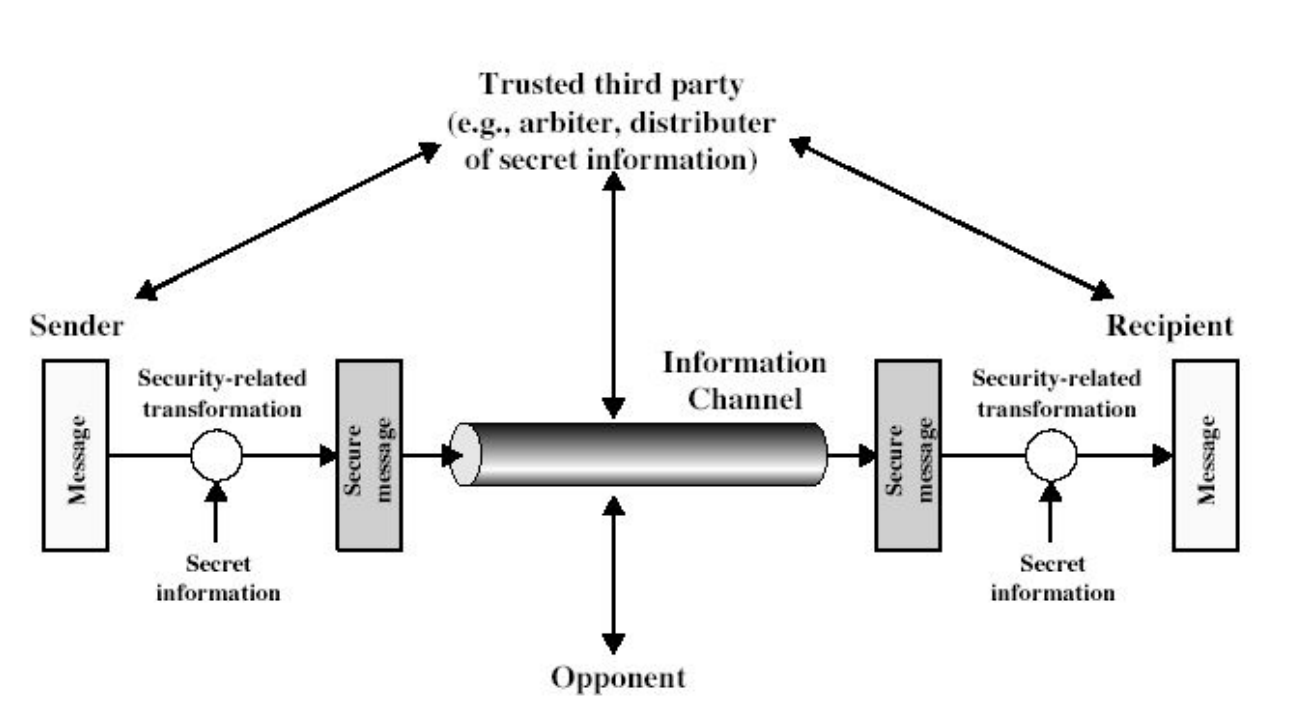
SECURITY MECHANISMS

- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Timestamping
  - inclusion of correct date and time within messages

AND THE WINNER IS …

- On top of everything, the most fundamental problem in security is
  - SECURE KEY EXCHANGE
    - mostly over an insecure channel

A GENERAL MODEL FOR NETWORK SECURITY



MODEL FOR NETWORK SECURITY

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

MODEL FOR NETWORK ACCESS SECURITY

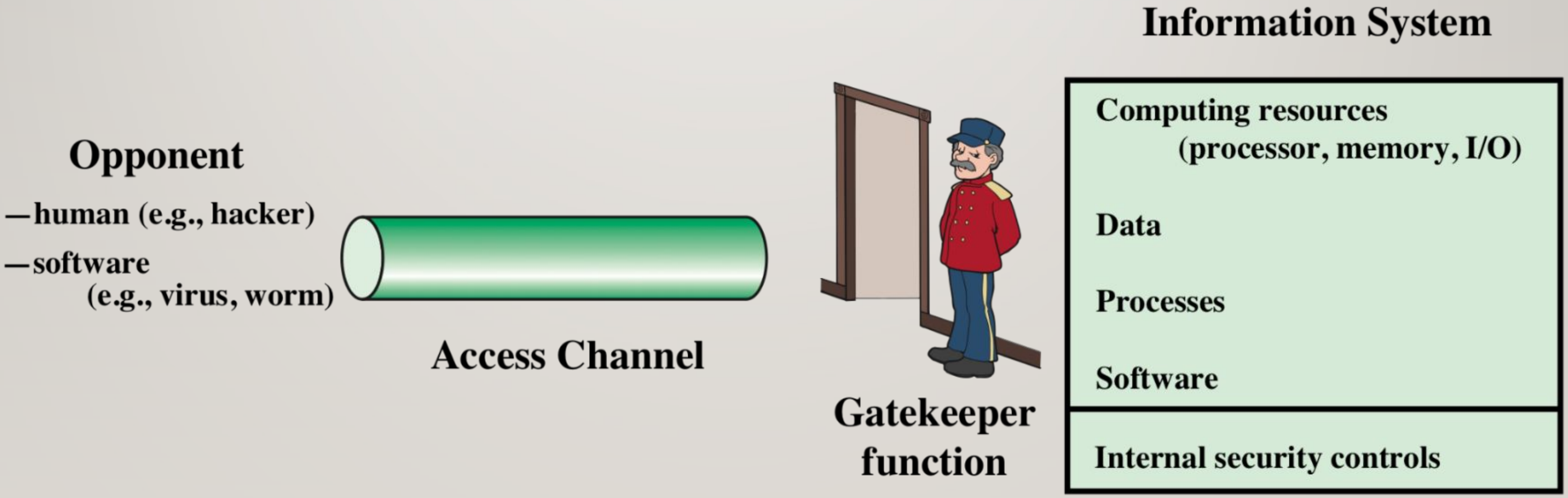


Figure 1.3 Network Access Security Model

MODEL FOR NETWORK ACCESS SECURITY

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users and processes and ensure only authorized users and processes access designated information or resources
  - Internal control to monitor the activity and analyze information to detect unwanted intruders

MORE ON COMPUTER SYSTEM SECURITY

- Based on “Security Policies”
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved
  - Assurance and Evaluation
    - Assurance: degree of confidence to a system
    - Security products and systems must be evaluated using certain criteria in order to decide whether they assure security or not

ASPECTS OF COMPUTER SECURITY

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Dependability

ASPECTS OF COMPUTER SECURITY

- Confidentiality
  - Prevent unauthorised disclosure of information
  - Synonyms: Privacy and Secrecy
    - any differences? Let’s discuss
- Integrity
  - two types: data integrity and system integrity
  - In general, “make sure that everything is as it is supposed to be”
  - More specifically, “no unauthorized modification, deletion” on data (data integrity)
  - System performs as intended without any unauthorized manipulations (system integrity)

ASPECTS OF COMPUTER SECURITY

- Availability
  - services should be accessible when needed and without extra delay
- Accountability
  - audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
  - How can we do that?
    - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
    - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.
- Dependability
  - Can we trust the system as a whole?

ATTACK SURFACES

- An attack surface consists of the reachable and exploitable vulnerabilities in a system
- Examples:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available in a firewall
  - Code that processes incoming data, email, XML, office documents, etc.
  - Interfaces and Web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack

ATTACK SURFACE CATEGORIES

- Network attack surface
  - Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
    - E.g. DoS, intruders exploiting network protocol vulnerabilities
- Software attack surface
  - Refers to vulnerabilities in application, utility, or operating system code
- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders
  - E.g. social engineering, insider traitors

FUNDAMENTAL DILEMMA OF SECURITY

- **“Security unaware users have specific security requirements but no security expertise.”**
  - from D. Gollmann
  - Solution: level of security is given in predefined classes specified in some common criteria
    - Orange book (Trusted Computer System Evaluation Criteria) is such a criteria

FUNDAMENTAL TRADEOFF

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

“If security is an add-on that people have to do something special to get, then most of the time they will not get it”

Martin Hellman,

co-inventor of Public Key Cryptography

GOOD ENOUGH SECURITY

"Everything should be as secure as necessary, but not securer"

Ravi Sandhu, "Good Enough Security", IEEE Internet Computing, January/February 2003, pp. 66- 68.

- Read the full article at

  http://dx.doi.org/10.1109/MIC.2003.1167341

SOME OTHER SECURITY FACTS

- Not as simple as it might first appear to the novice
- Must consider all potential attacks when designing a system
- Generally yields complex and counterintuitive systems
- Battle of intelligent strategies between attacker and admin
- Requires regular monitoring
- Not considered as a beneficial investment until a security failure occurs
  - Actually security investments must be considered as insurance against attacks
- too often an afterthought
  - Not only from investment point of view, but also from design point of view