Advanced Security and Cryptography

Dr. Ramesh Gadde

M.Sc., M.Tech, Ph.D., LMISTE, MCSI

Department of Computer Science and Engineering
School of Electrical & Computer Engineering
EiT- Mekelle University

Text book and Reference

- Text book
  1. Charles P Pfleager, Security in Computing,Prentice Hall, 2006, ISBN 0-13-239077-9.
  2. Man Young Rhee, Internet Security, Cryptographic Principles, Algorithms and Protocol, John Wiley, 2003, ISBN 0-470-85285-2.
  3. Ynag Xiao, Xuemin Shem, Ding Zhu Du, Wireless Network Security, Springer Publishing, 2007, ISBN 0-387-33112-3.

Text book and Reference

- Text book

4. William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005, ISBN 0-13-187316-4.
5. Chatlie Kaufman, Radia Perlman, Network Security-Private Communication in Public World, Prentice Hall of India, 2002, ISBN: 81 - 203-2213-4.
6. Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, ISBN 0-471 -38922-6.

Text book and Reference

- Text book
    7. Bruce Schneier: Secrets & Lies: Digital Security in a Networked World, ISBN 0-471-25311.
    8. Robert C. Seacord: Secure Coding in C and C++. Addison Wesley, September, 2005. ISBN 0-321 -33572-4.
    9. Walter Ciciora, James Farmer, David Large and Michael Adams(Dec 8, 2003), Modern Cable Television Technology, Second Edition (The Morgan Kaufmann Series in networking).
    10. Patricia A. Morreale and KornelTerplan(Nov 22, 2000),The CRC Handbook of Modern Telecommunications.

Mode of Assessment

- Attendance & Seminar : 10%
- Lab Experiments : 5%
- Paper Writing :15%
- Mid-term Exam: 20%
- Final Exam: 50%

Advanced Security and Cryptography

Chapter - 1

Overview

1.1 BACK GROUND

Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers.

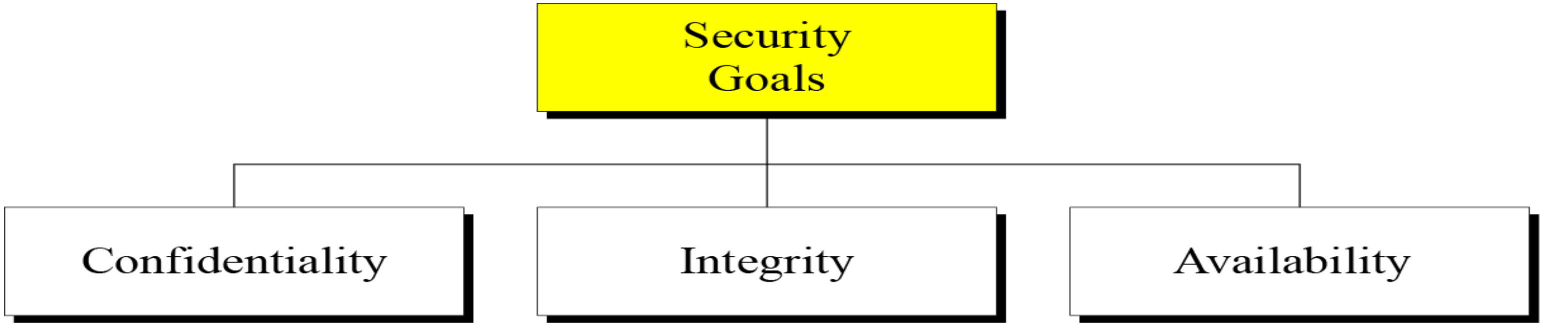
Network Security - measures to protect data during their transmission.

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure.

Understanding Network Security

- Network security
  - Process by which digital information assets are protected
- Goals
  - Maintain integrity
  - Protect confidentiality
  - Assure availability



Secured Communication Model

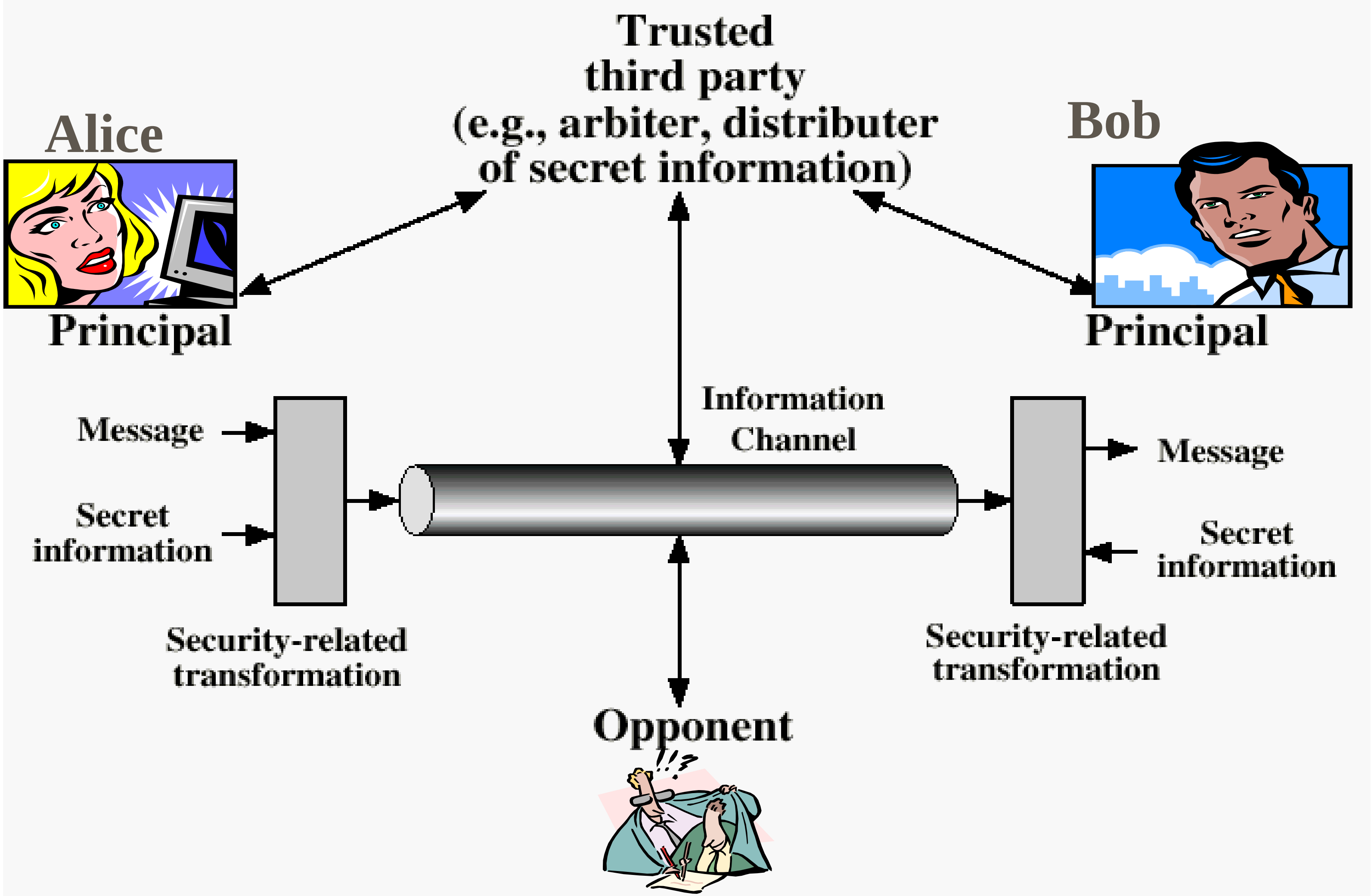
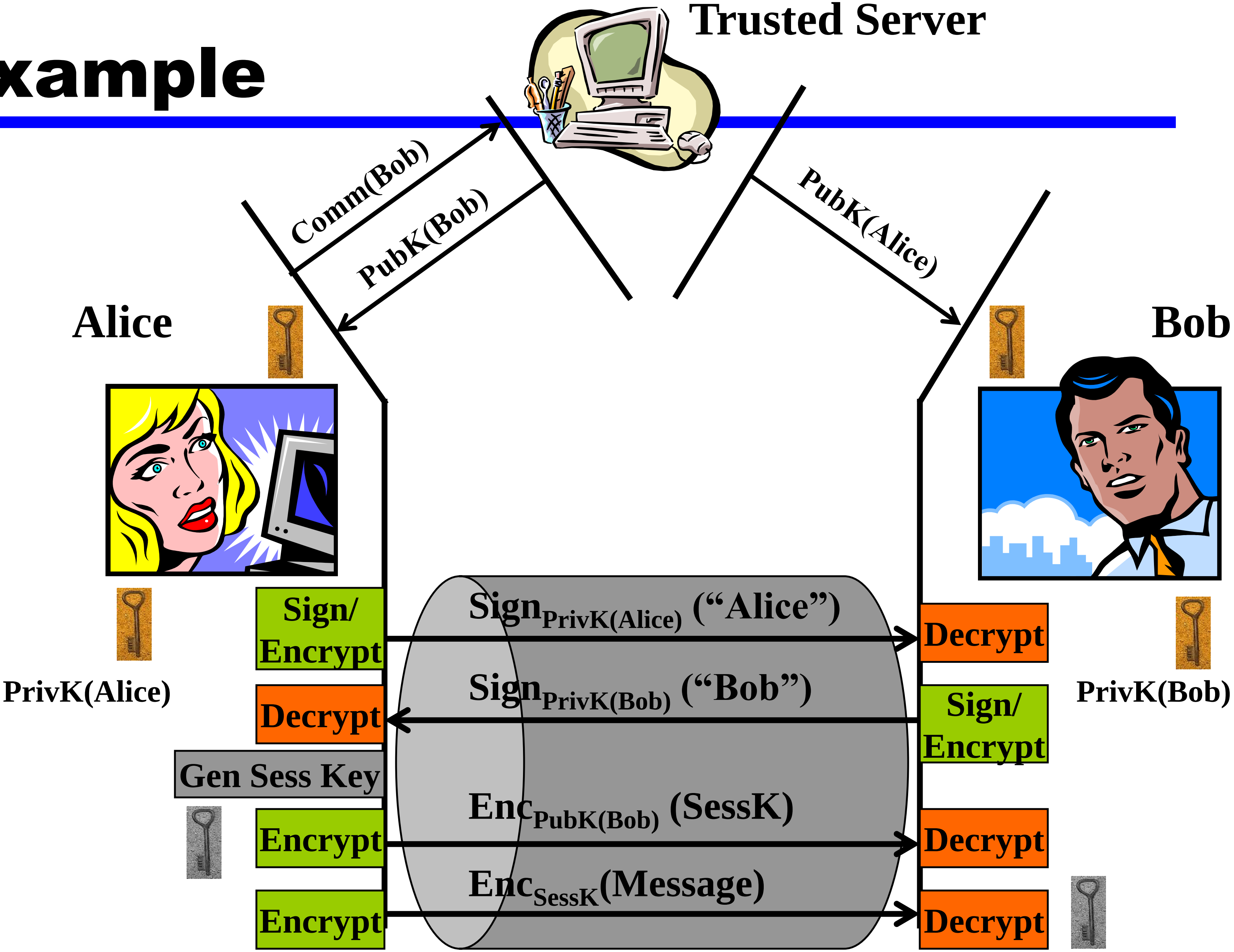


Figure 1.3 Model for Network Security

Example



Trusted Server

Comm(Bob)

PubK(Bob)

PubK(Alice)

Alice

Bob

PrivK(Alice)

PrivK(Bob)

Sign/ Encrypt

Sign$_{\text{PrivK(Alice)}}$ ("Alice")

Decrypt

Decrypt

Sign$_{\text{PrivK(Bob)}}$ ("Bob")

Sign/ Encrypt

Gen Sess Key

Encrypt

Enc$_{\text{PubK(Bob)}}$ (SessK)

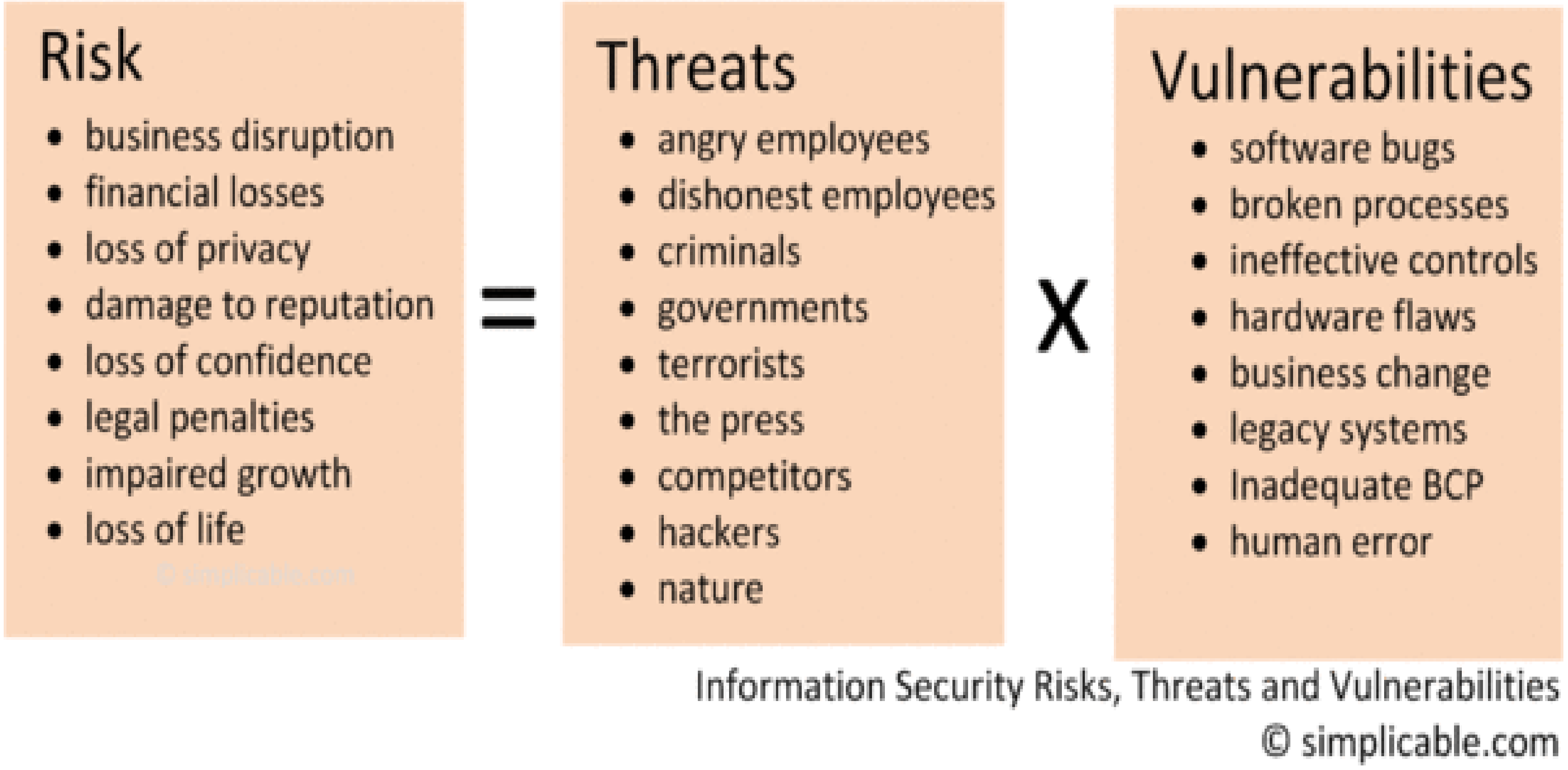
Decrypt

Encrypt

Enc$_{\text{SessK}}$(Message)

Decrypt

Risk = Threats x Vulnerabilities



Risk

- business disruption
- financial losses
- loss of privacy
- damage to reputation
- loss of confidence
- legal penalties
- impaired growth
- loss of life

=

Threats

- angry employees
- dishonest employees
- criminals
- governments
- terrorists
- the press
- competitors
- hackers
- nature

X

Vulnerabilities

- software bugs
- broken processes
- ineffective controls
- hardware flaws
- business change
- legacy systems
- Inadequate BCP
- human error

Information Security Risks, Threats and Vulnerabilities

1.2 Security Vulnerabilities

- “Some weakness of a system that could allow security to be allowed.”
- Types of vulnerabilities
  - Physical vulnerabilities
  - Natural vulnerabilities
  - Hardware/software vulnerabilities
  - Media vulnerabilities (e.g., stolen/damaged disk/tapes)
  - Emanation vulnerabilities---due to radiation
  - Communication vulnerabilities
  - Human vulnerabilities

How do the vulnerabilities manifest?

- The different types of vulnerabilities manifest themselves via several misuses:
  - External misuse---visual spying, misrepresenting, physical scavenging
  - Hardware misuse---logical scavenging, eavesdropping, interference, physical attack, physical removal
  - Masquerading---impersonation, piggybacking attack, spoofing attacks, network weaving
  - Pest programs---Trojan horse attacks, logic bombs, malevolent worms, virus attacks
  - Bypasses---Trapdoor attacks, authorization attacks (e.g., password cracking)
  - Active misuse---basic active attack, incremental attack, denial of service
  - Passive misuse---browsing, interference, aggregation, covert channels

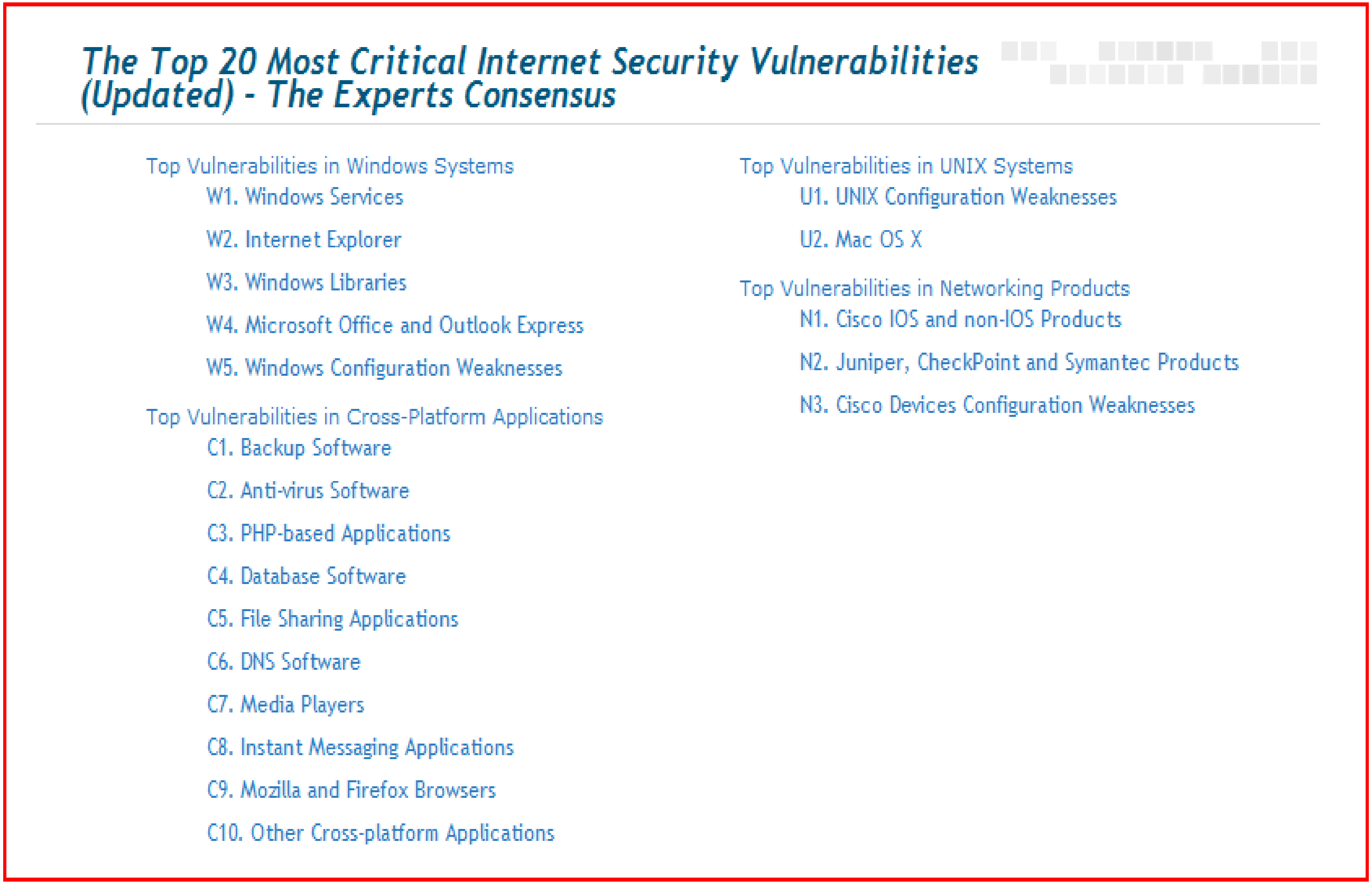
Examples of Information Security Vulnerabilities

- Ref: http://simplicable.com/new/the-big-list-of-information-security-vulnerabilities
- Information security vulnerabilities are weaknesses that expose an organization to risk.
- **Through employees**: Social interaction, Customer interaction, Discussing work in public locations, Taking data out of the office (paper, mobile phones, laptops), Emailing documents and data, Mailing and faxing documents, Installing unauthorized software and apps, Removing or disabling security tools, Letting unauthorized persons into the office (tailgating) , Opening spam emails, Connecting personal devices to company networks, Writing down passwords and sensitive data, Losing security devices such as id cards, Lack of information security awareness, Keying data
- **Through former employees---**Former employees working for competitors, Former employees retaining company data, Former employees discussing company matters
- **Though Technology---**Social networking, File sharing, Rapid technological changes, Legacy systems, Storing data on mobile devices such as mobile phones, Internet browsers
- **Through hardware---**. Susceptibility to dust, heat and humidity, Hardware design flaws, Out of date hardware, Misconfiguration of hardware

Examples of Information Security Vulnerabilities (Cont.)

- **Through software---**Insufficient testing, Lack of audit trail, Software bugs and design faults, Unchecked user input, Software that fails to consider human factors, Software complexity (bloatware), Software as a service (relinquishing control of data), Software vendors that go out of business or change ownership
- **Through Network---**Unprotected network communications, Open physical connections, IPs and ports, Insecure network architecture, Unused user ids, Excessive privileges, Unnecessary jobs and scripts executing , Wifi networks
- **Through IT Management---**Insufficient IT capacity , Missed security patches, Insufficient incident and problem management, Configuration errors and missed security notices , System operation errors, Lack of regular audits, Improper waste disposal, Insufficient change management, Business process flaws, Inadequate business rules, Inadequate business controls, Processes that fail to consider human factors, Overconfidence in security audits, Lack of risk analysis, Rapid business change, Inadequate continuity planning Lax recruiting processes
- **Partners and suppliers---**Disruption of telecom services, Disruption of utility services such as electric, gas, water, Hardware failure, Software failure, Lost mail and courier packages, Supply disruptions, Sharing confidential data with partners and suppliers

SANS Top 20 Security Vulnerabilities



The Top 20 Most Critical Internet Security Vulnerabilities (Updated) - The Experts Consensus

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

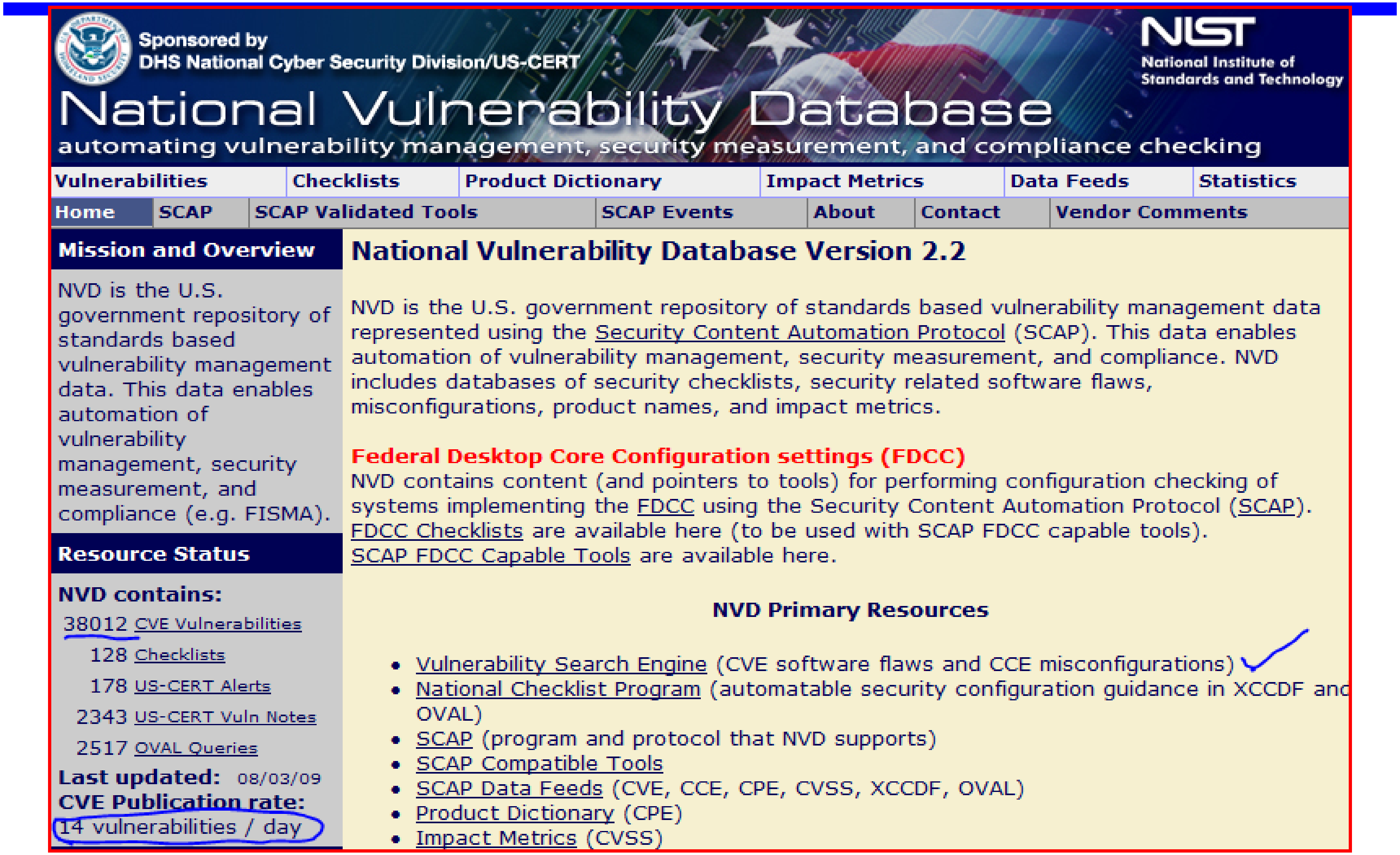
- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players
- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

Top Vulnerabilities in UNIX Systems

- U1. UNIX Configuration Weaknesses
- U2. Mac OS X

Top Vulnerabilities in Networking Products

- N1. Cisco IOS and non-IOS Products
- N2. Juniper, CheckPoint and Symantec Products
- N3. Cisco Devices Configuration Weaknesses



Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

38012	CVE Vulnerabilities
128	Checklists
178	US-CERT Alerts
2343	US-CERT Vuln Notes
2517	OVAL Queries

Last updated: 08/03/09

CVE Publication rate:

14 vulnerabilities / day

National Vulnerability Database Version 2.2

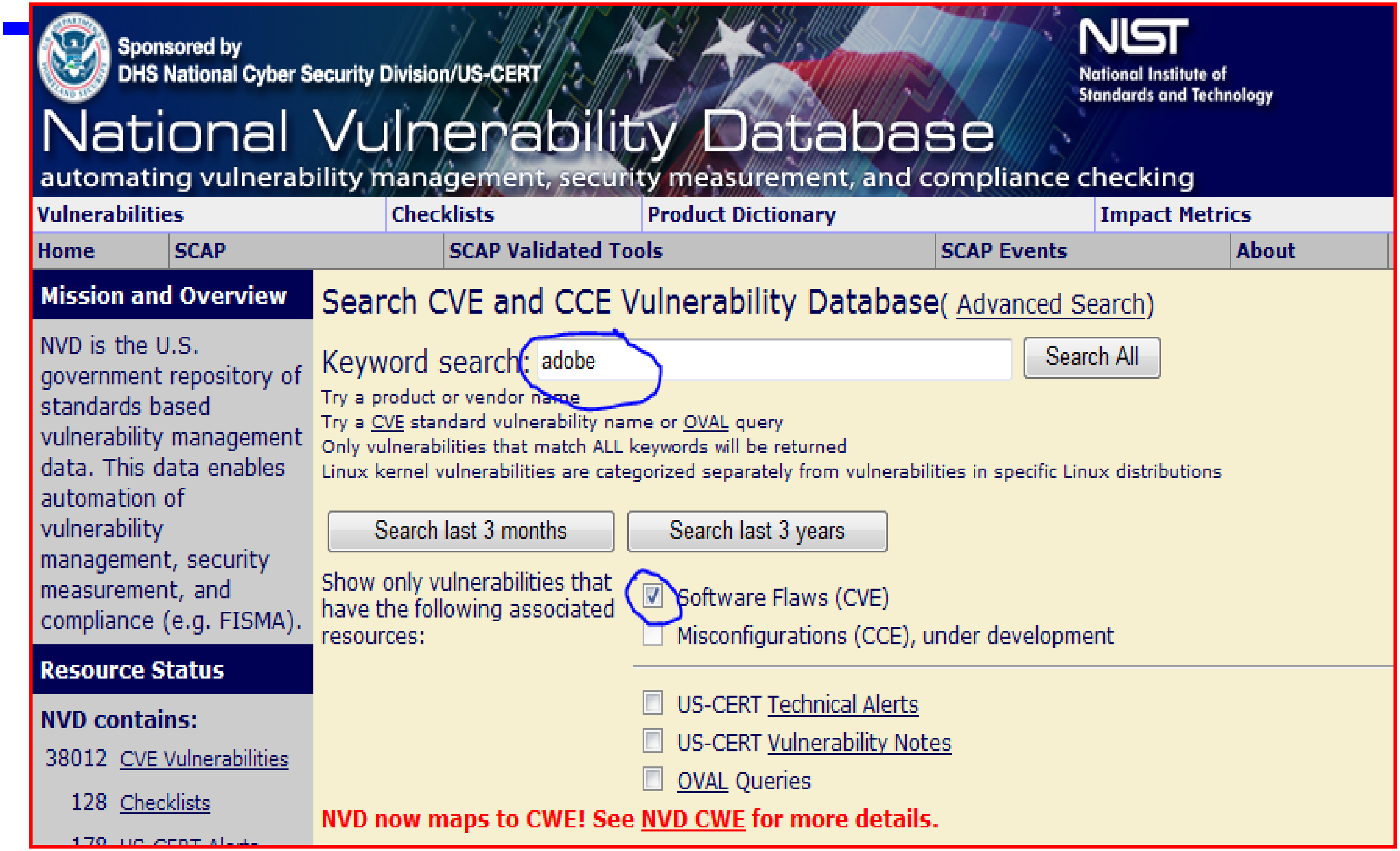
NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations) ✓
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)



National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

38012	CVE Vulnerabilities
128	Checklists
178	US-CERT Alerts

Search CVE and CCE Vulnerability Database(Advanced Search)

Keyword search: adobe

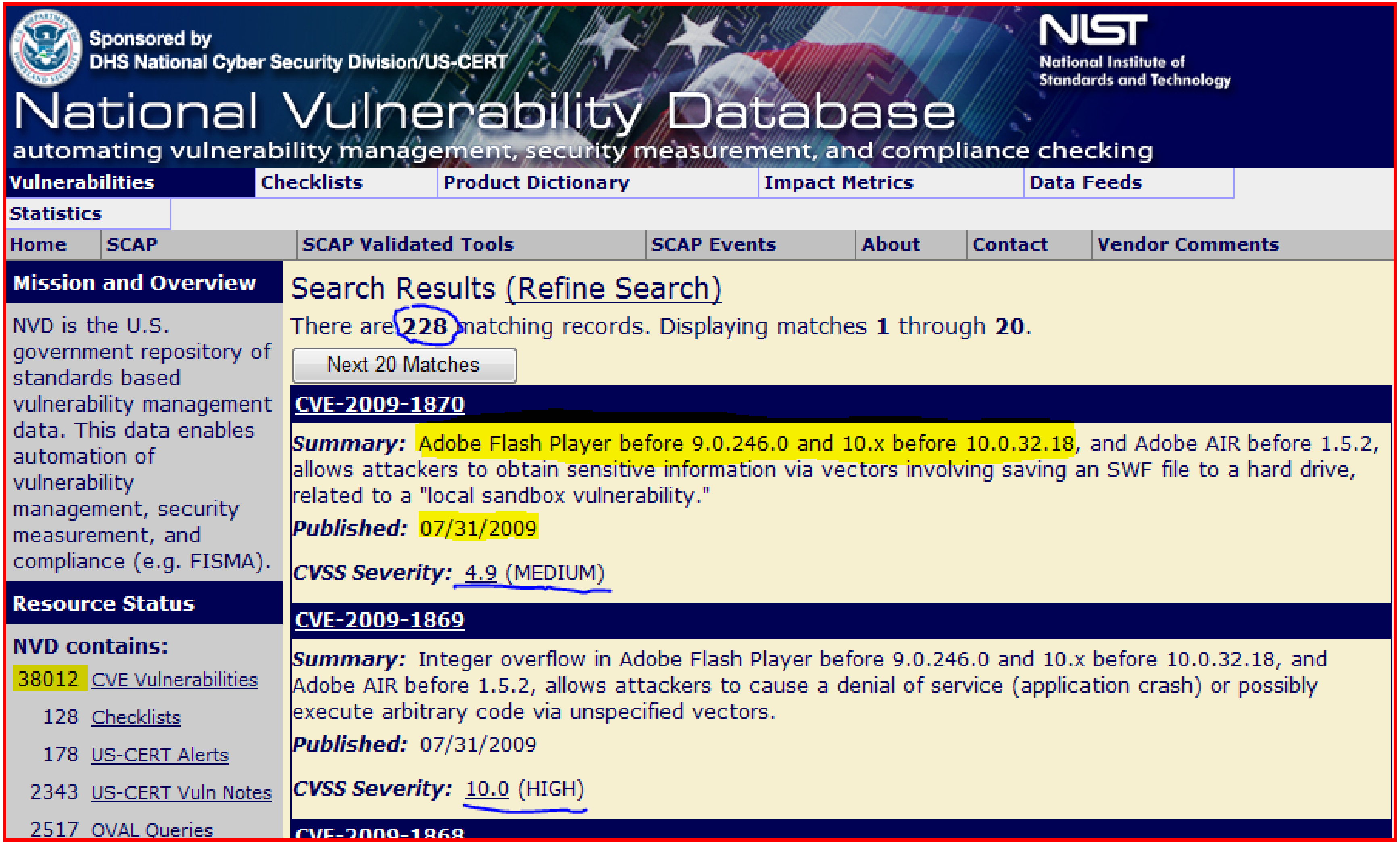
Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:

☑ Software Flaws (CVE)
□ Misconfigurations (CCE), under development

□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

NVD now maps to CWE! See NVD CWE for more details.



Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

38012	CVE Vulnerabilities
128	Checklists
178	US-CERT Alerts
2343	US-CERT Vuln Notes
2517	OVAL Queries

Search Results (Refine Search)

There are **228** matching records. Displaying matches **1** through **20**.

CVE-2009-1870

Summary: Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to obtain sensitive information via vectors involving saving an SWF file to a hard drive, related to a "local sandbox vulnerability."

Published: 07/31/2009

CVSS Severity: 4.9 (MEDIUM)

CVE-2009-1869

Summary: Integer overflow in Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors.

Published: 07/31/2009

CVSS Severity: 10.0 (HIGH)

CVE-2009-1868

Other Vulnerabilities

- Code Mistakes
- Untrained Users
- Insecure Configuration Settings

Code Mistakes

- Federal Student Aid has had Code Mistakes
  - Implement Prevention in Code
  - Thoroughly Test
  - Use Tools

Untrained Users

- Security ignorance compromises data
- Provide the training
- Rules of Behavior
- Annual refresher training

Insecure Configuration Settings

- NIST, DISA, CIS vs. Business Needs
- Builds
- System Upgrades
- Vulnerability Scans

- Note: Federal Student Aid Secure Configuration Guides are based off the NIST checklist located at http://checklists.nist.gov

1.3 Security Threats

- Identity theft
- Privacy concerns
- Wireless access

To Offset Security Threats

- Integrity
  - Assurance that data is not altered or destroyed in an unauthorized manner
- Confidentiality
  - Protection of data from unauthorized disclosure to a third party
- Availability
  - Continuous operation of computing systems

Security Ramifications: Costs of Intrusion

- Causes of network security threats
  - Technology weaknesses
  - Configuration weaknesses
  - Policy weaknesses
  - Human error

Technology Weaknesses

- TCP/IP
- Operating systems
- Network equipment

Configuration Weaknesses

- Unsecured accounts
- System accounts with easily guessed passwords
- Misconfigured Internet services
- Unsecured default settings
- Misconfigured network equipment
- Trojan horse programs
- Vandals
- Viruses

Policy Weaknesses

- Lack of a written security policy
- Politics
- High turnover
- Concise access controls not applied
- Software and hardware installation and changes do not follow policy
- Proper security
- Nonexistent disaster recovery plan

Human Error

- Accident
- Ignorance
- Workload
- Dishonesty
- Impersonation
- Disgruntled employees
- Snoops
- Denial-of-service attacks

Security Attacks (Stallings)

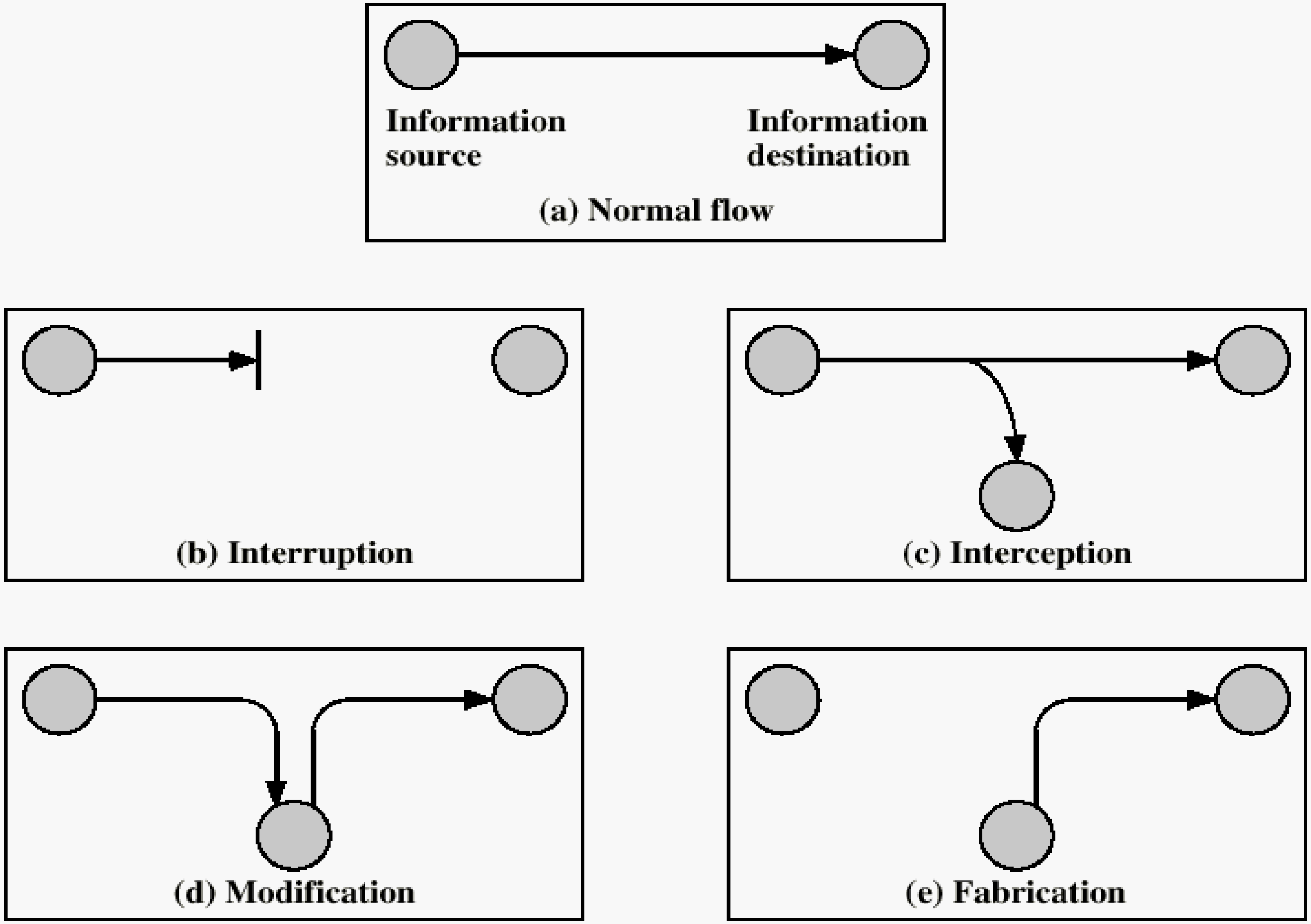
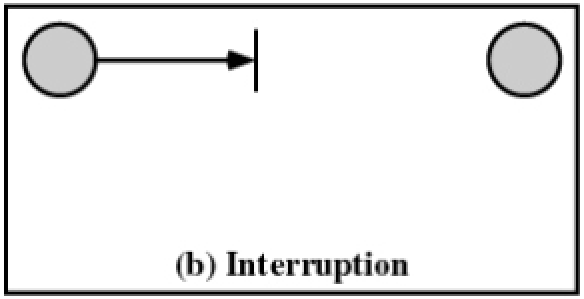


Figure 1.1 Security Threats

Types of Threats

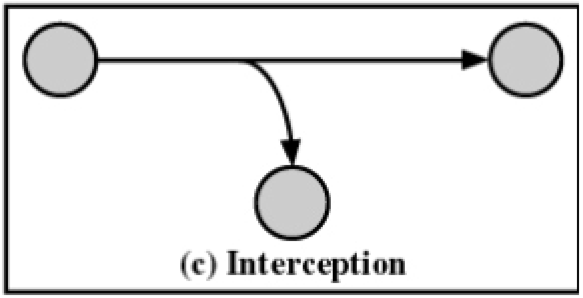
- Interruption
  - An asset of the system is destroyed of becomes unavailable or unusable
  - Attack on availability
  - Destruction of hardware
  - Cutting of a communication line
  - Disabling the file management system



(b) Interruption

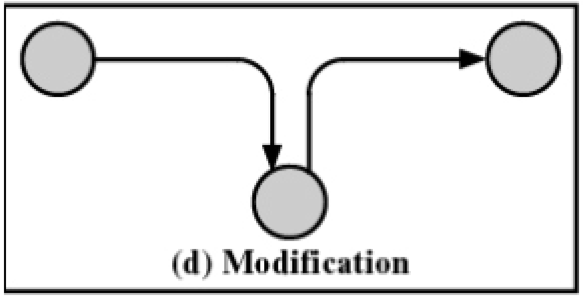
Types of Threats

- Interception
  - —An unauthorized party gains access to an asset
  - —Attack on confidentiality
  - —Wiretapping to capture data in a network
  - —Illicit copying of files or programs



Types of Threats

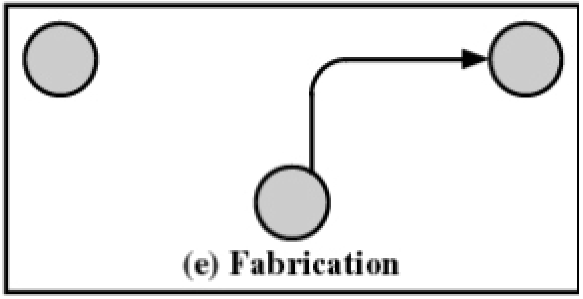
- Modification
  - —An unauthorized party not only gains access but tampers with an asset
  - —Attack on integrity
  - —Changing values in a data file
  - —Altering a program so that it performs differently
  - —Modifying the content of messages being transmitted in a network



(d) Modification

Types of Threats

- Fabrication
  - An unauthorized party inserts counterfeit objects into the system
  - Attack on authenticity
  - Insertion of spurious messages in a network
  - Addition of records to a file



Examples of Attacks

- Attacks can be Active, e.g., intrusion, or Passive, e.g, eavesdropping

- Examples of attacks:
  - Intrusion
  - Eavesdropping
  - Impersonation
  - Viruses / Worms
  - Denial of service
  - Man-in-the-middle
  - Reflection attack
  - Replay attack
  - Password cracking
  - Data/code modification
  - Fraudulent attribution
  - Repudiation

1.4 Security Policies

Goals of Network Security

- Achieve the state where any action that is not expressly permitted is prohibited
  - Eliminate theft
  - Determine authentication
  - Identify assumptions
  - Control secrets

Creating a Secure Network Strategy

- Address both internal and external threats
- Define policies and procedures
- Reduce risk across perimeter security, the Internet, intranets, and LANs

Creating a Secure Network Strategy

- Human factors
- Know your weaknesses
- Limit access
- Achieve security through persistence
  - Develop change management process
- Remember physical security
- Perimeter security
  - Control access to critical network applications, data, and services

Creating a Secure Network Strategy

- Firewalls
  - Prevent unauthorized access to or from private network
  - Create protective layer between network and outside world
  - Replicate network at point of entry in order to receive and transmit authorized data
  - Have built-in filters
  - Log attempted intrusions and create reports

Creating a Secure Network Strategy

- Web and file servers
- Access control
  - Ensures that only legitimate traffic is allowed into or out of the network
    - Passwords
    - PINs
    - Smartcards

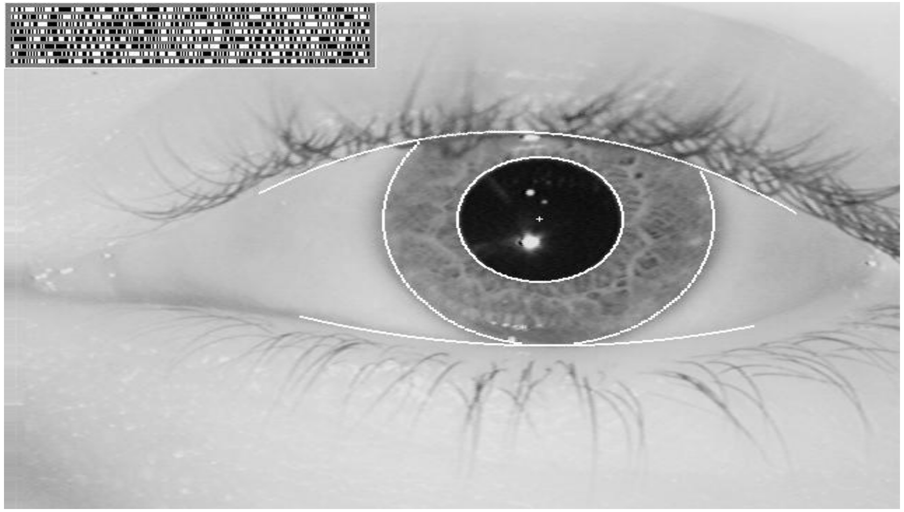
Creating a Secure Network Strategy

- Change management
  - Document changes to *all* areas of IT infrastructure
- Encryption
  - Ensures messages cannot be intercepted or read by anyone other than the intended person(s)

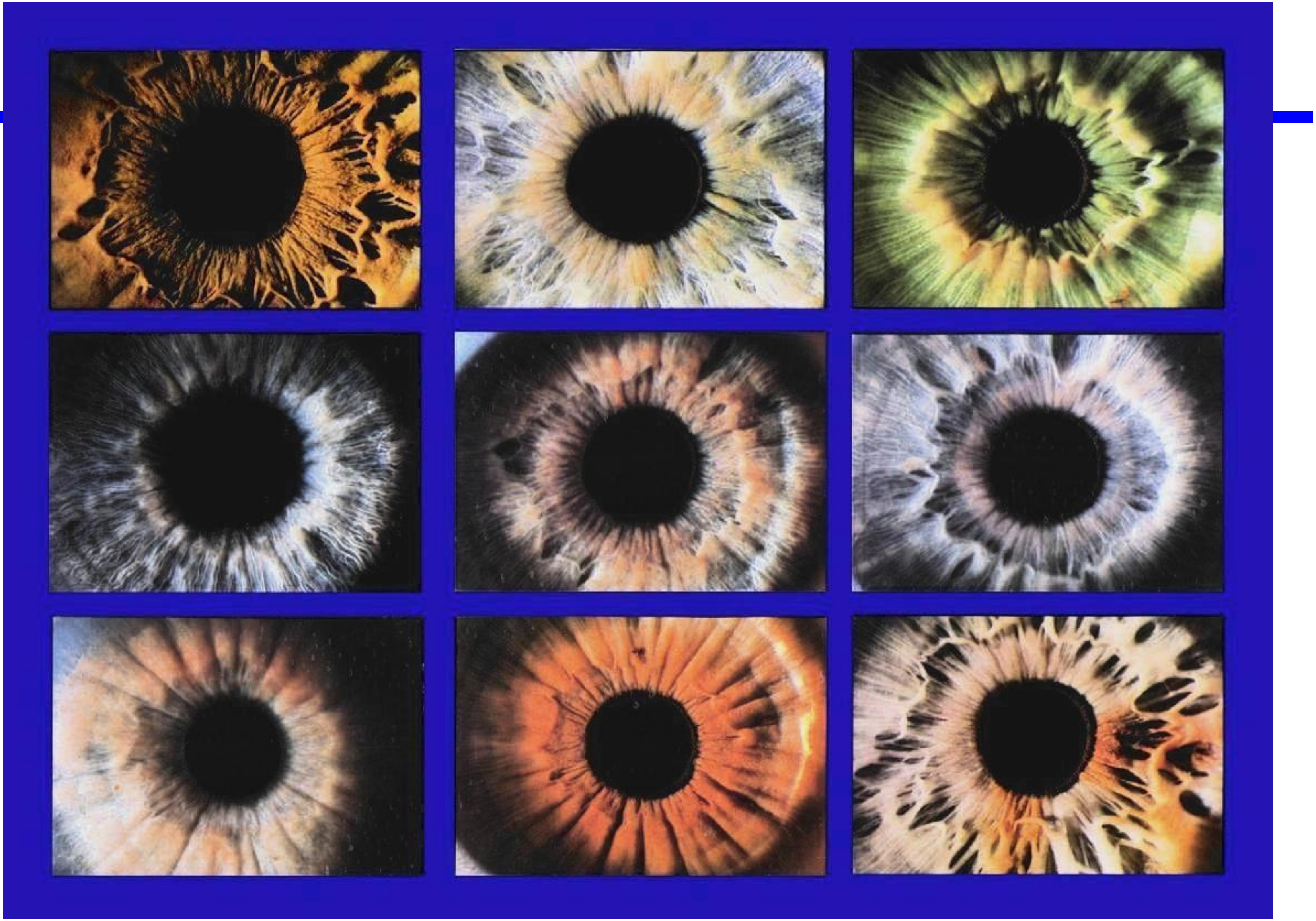
Creating a Secure Network Strategy

- Intrusion detection system (IDS)
  - Provides 24/7 network surveillance
  - Analyzes packet data streams within the network
  - Searches for unauthorized activity

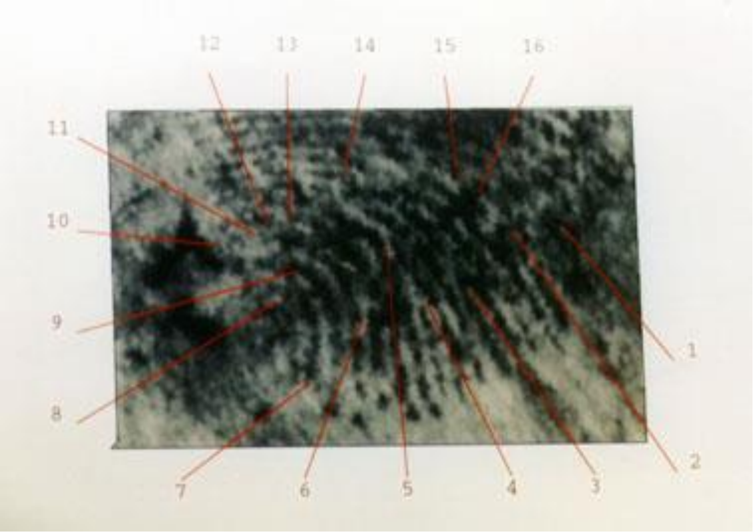
CAPTCHAs

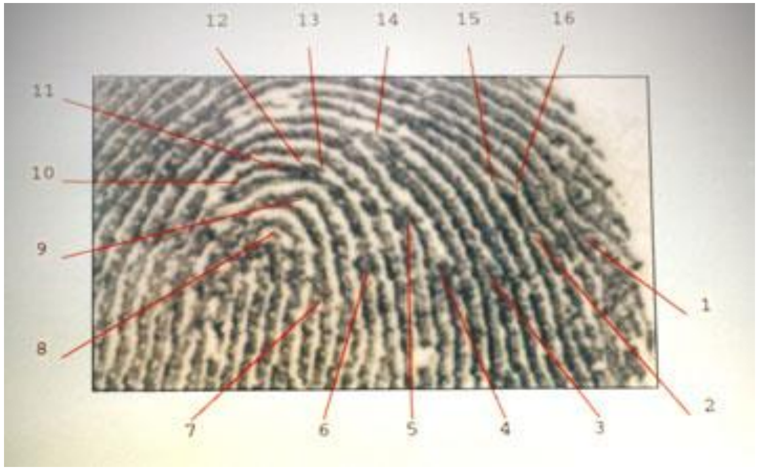


Biometrics

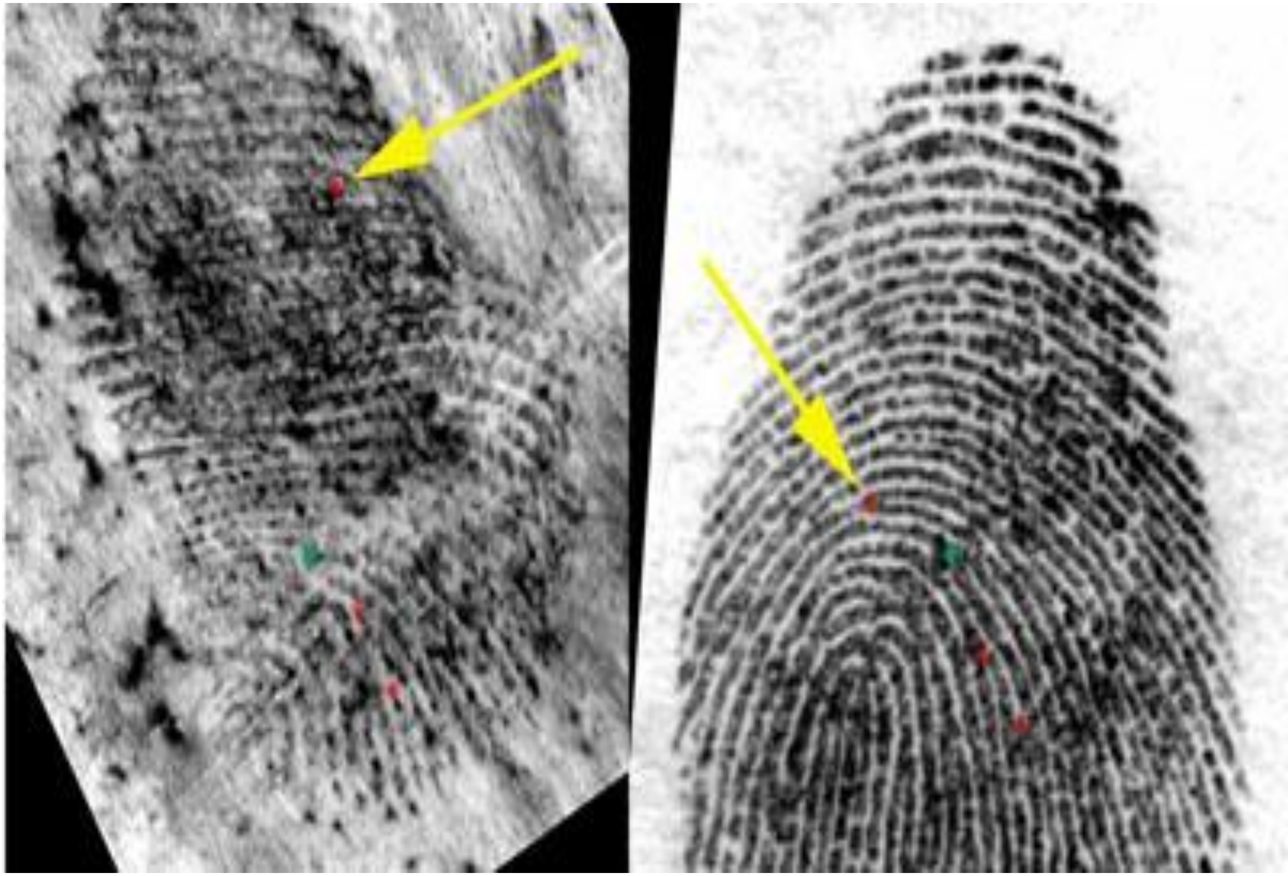


The McKie Case





Actual McKie Case Photos

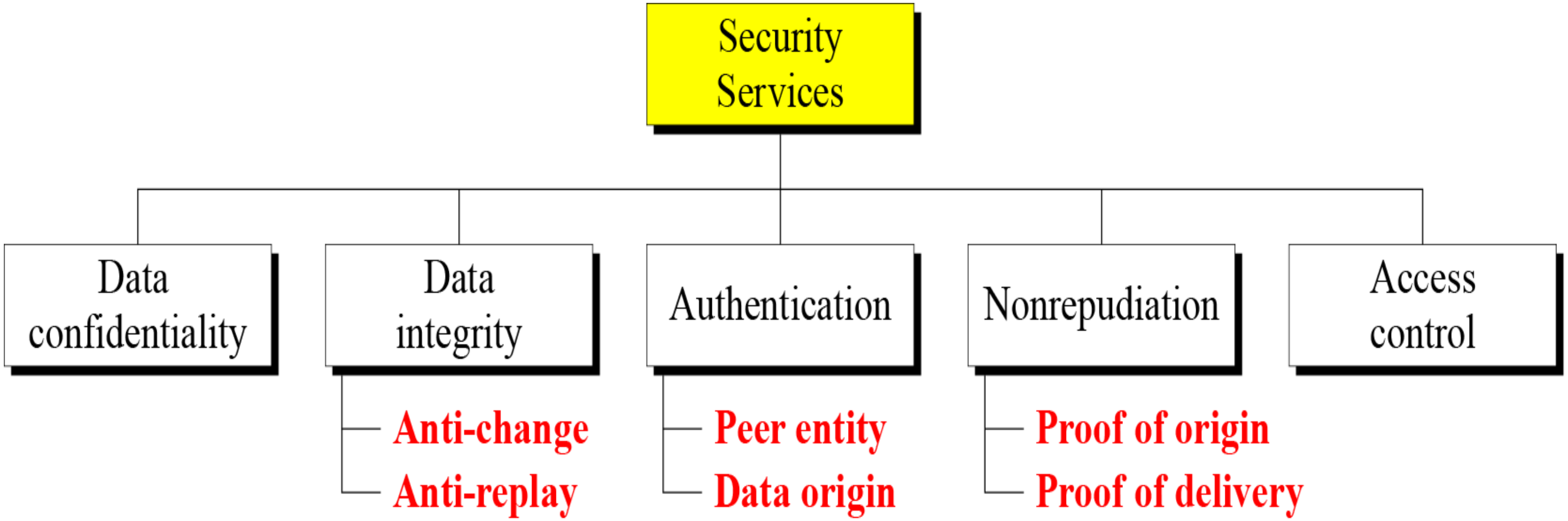


X.800 Security Services

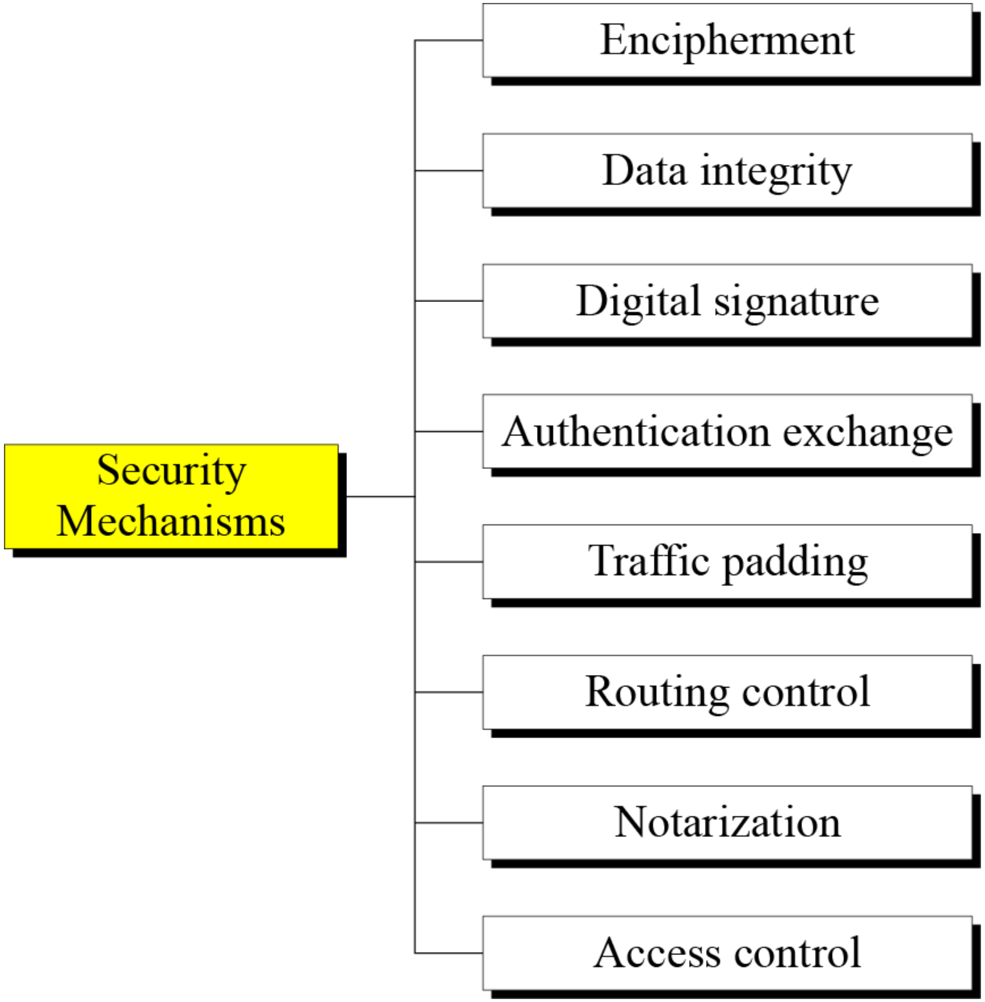
- **Authentication**: Identify peers, Source authentication for data
- **Access Control**: Who can access to what
- **Data Confidentiality**: Connection, Connectionless (system), Traffic, Privacy
- **Data Integrity**: With or without recovery
- **Non-repudiation** : Origin, Destination, Both
- **Availability**: A service on its own, or a property of other services

SECURITY SERVICES

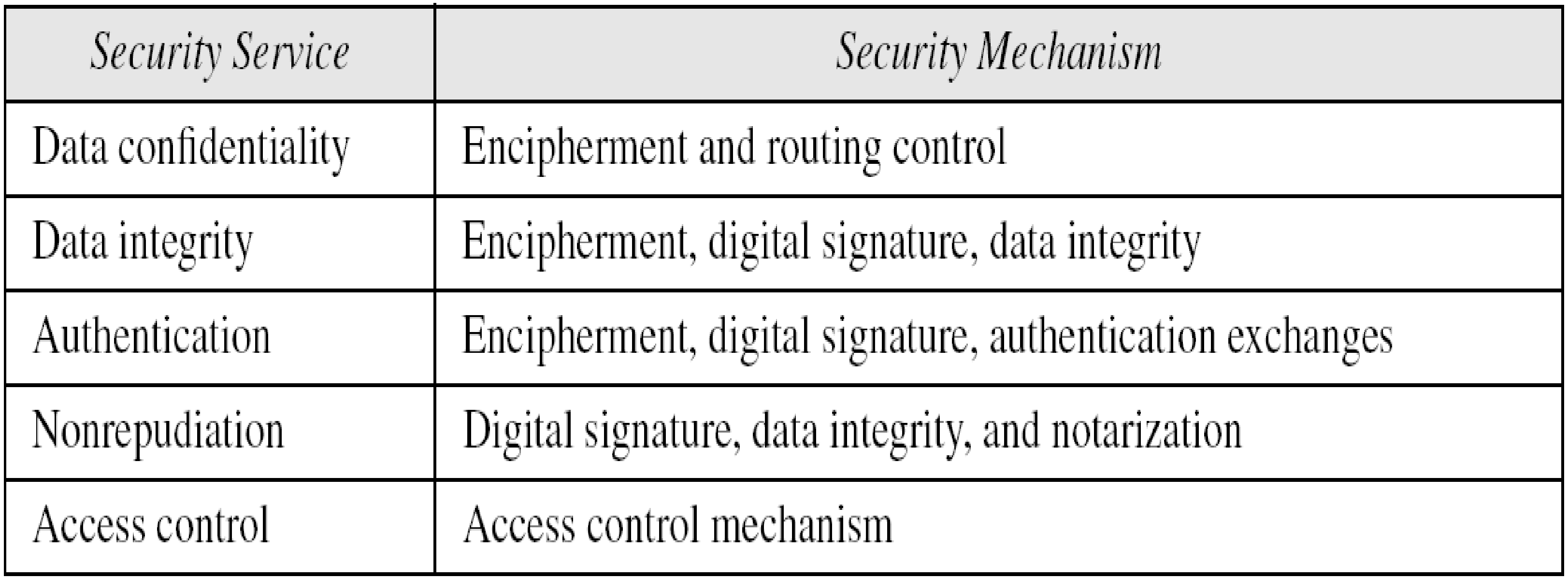
ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..



SECURITY MECHANISMS



Relation between Security Services and Mechanisms



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism