Security Defense Strategy Basics

Joseph E. Cannon, PhD

Professor of Computer and Information Sciences

Harrisburg University of Science and Technology

Only two things in the water after dark.

Gators and gator food.

Old Florida Saying

Information Security Defense Strategy Basics

Abstract

As more and more people become *wired*, an increasing number of people need to understand the basics of information security in a networked world. This presentation was developed with the information systems manager in mind and explains the concepts needed to understand Computer and Network Security. The presentation goes on to consider risk management, network threats, firewalls, and more special-purpose secure networking devices. This presentation is designed to make all managers aware of the full spectrum of threats and vulnerabilities in information systems. The participant will recognize that information security is more than just technical solutions but is a defense strategy that balances Technology, Policy, Practice, Awareness, and Training. Each participant will come to understand that information security is a complicated subject, which historically was only tackled by well-trained and experienced experts.

What is Security?

- The quality or state of being secure to be free from danger.

- What is Computer Security?
  - Answer depends upon the perspective of the person you’re asking.
    - The Network Administrator has a different perspective than an end user or a security professional.
  - “A computer is secure if you can depend on it and its software to behave as you expect.” [Garfinkel, Spafford]

What is Computer Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information.

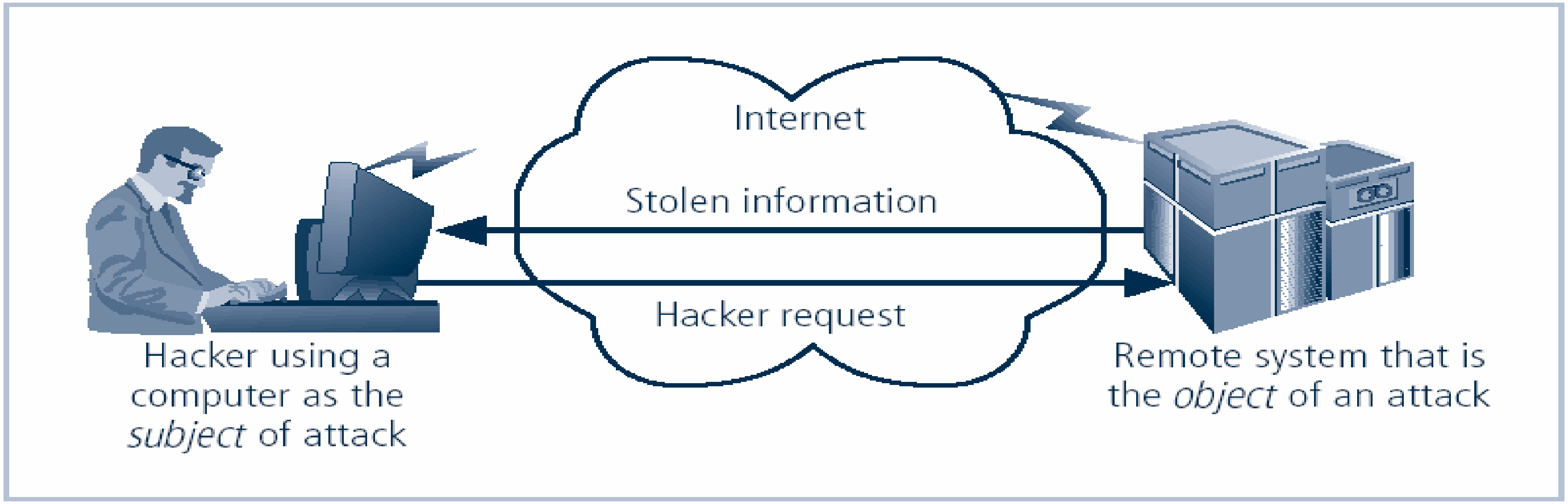

Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

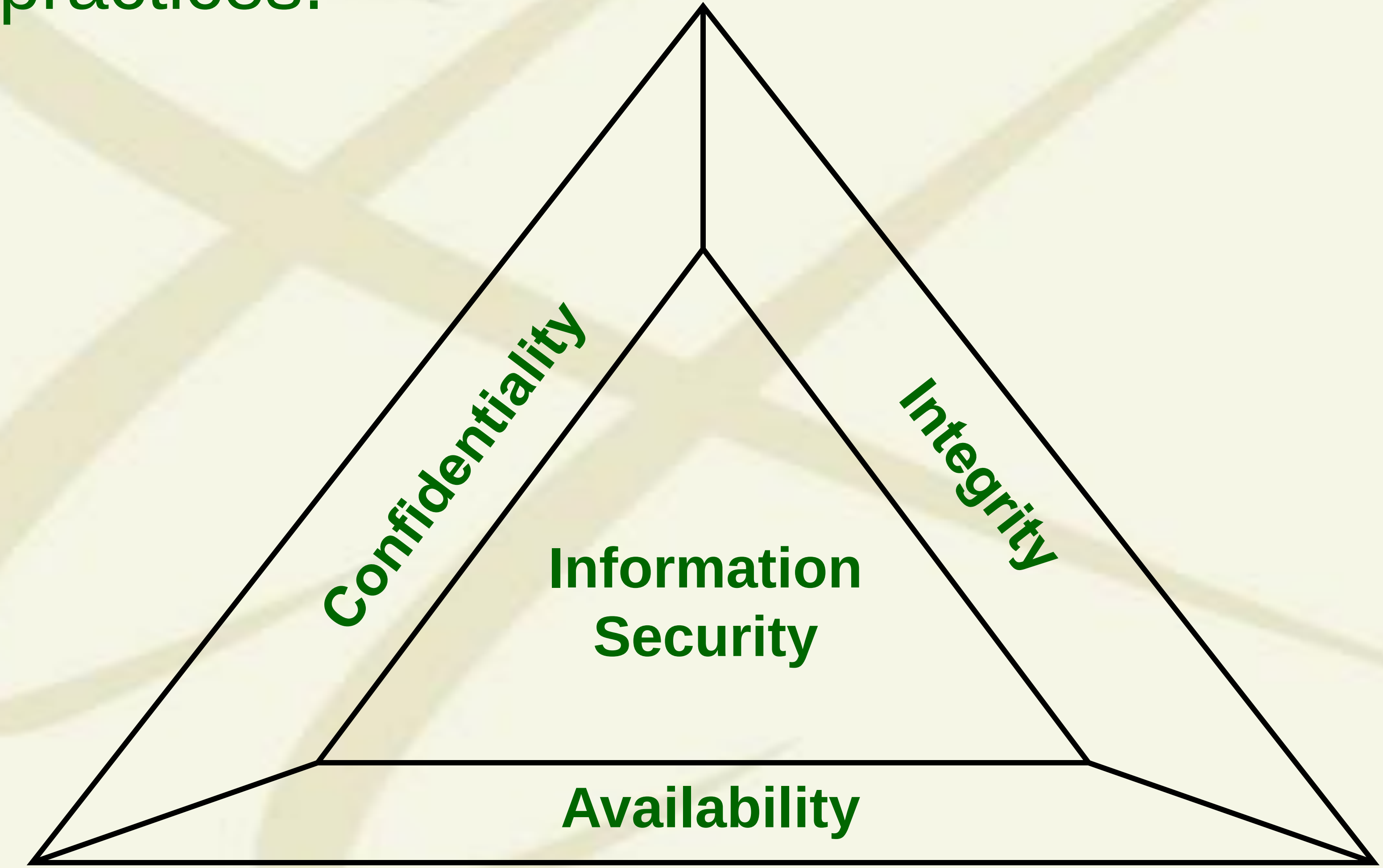
FIGURE 1-6 Computer as the Subject and Object of an Attack

Security Vulnerabilities

- “People are the weakest link. You can have the best technology: firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” – Kevin Mitnick
  - Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity.
- Perfect security is impossible
  - ***Lock computer in a safe and don’t use it***
  - ***Or, accept some risk***

Computer Security Basics[1]

- **CIA** Triad - Goals for implementing security practices.

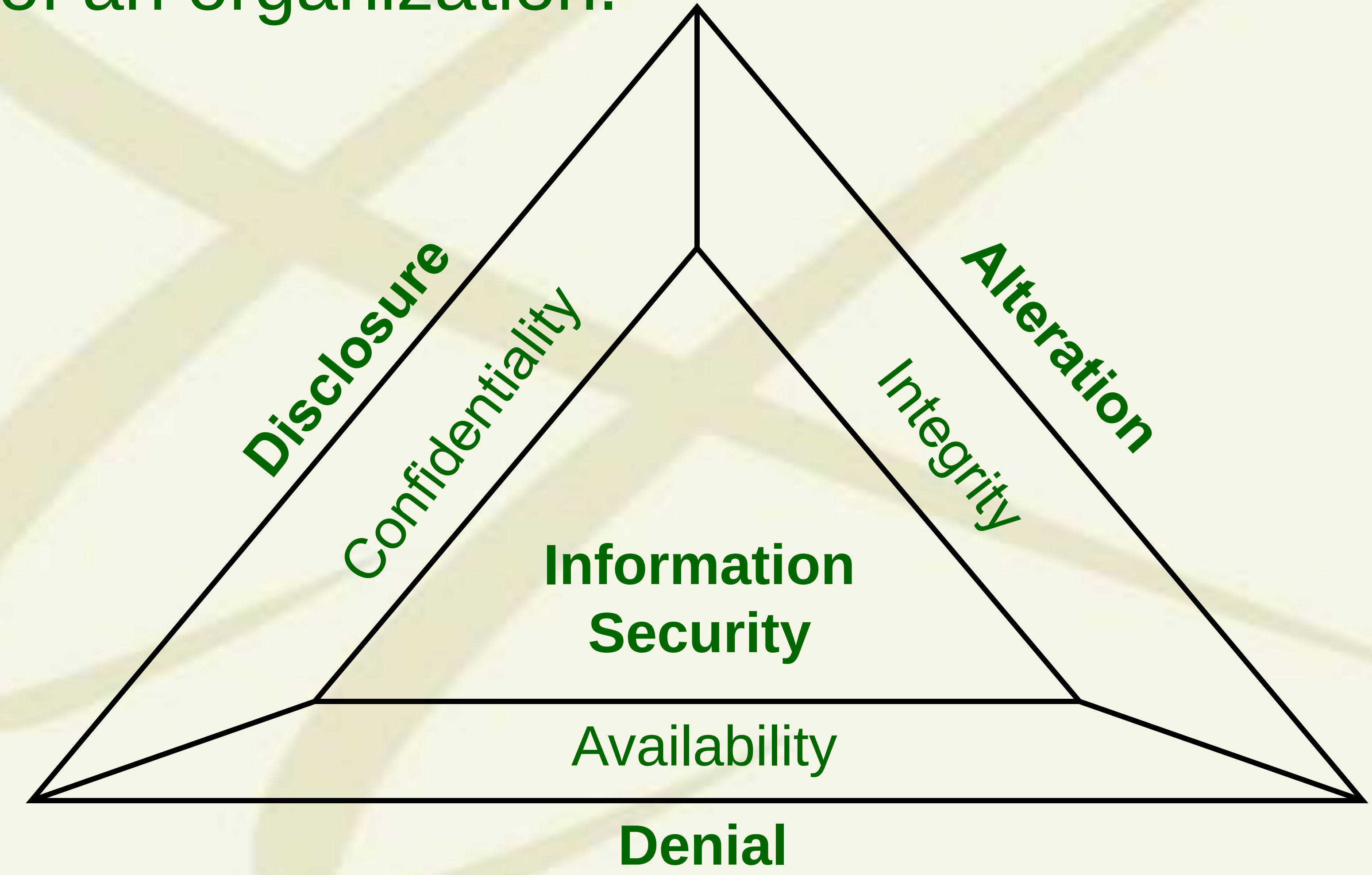


CIA Triad

- **C**onfidentiality
  - Confidential information should not be accessible to unauthorized users.
- **I**ntegrity
  - Data may only be modified through an authorized mechanism.
- **A**vailability
  - Authorized users should be able to access data for legitimate purposes as necessary.

Computer Security Basics

- **DAD** Triad - Goals for defeating the security of an organization.



DAD Triad

- **D**isclosure
  - Unauthorized individuals gain access to confidential information.
- **A**lteration
  - Data is modified through some unauthorized mechanism.
- **D**enial
  - Authorized users cannot gain access to a system for legitimate purposes.
- **DAD** activities may be malicious or accidental.

Threats to Security

- Hacker
  - Anyone who attempts to penetrate the security of an information system, regardless of intent.
  - Early definition included anyone very proficient in computer use.
- Malicious code object
  - Virus, worm, Trojan horse
  - A computer program that carries out malicious actions when run on a system.
- Malicious insider
  - Someone from within the organization that attempts to go beyond the rights and permissions that they legitimately hold.
  - Security professionals and system administrators are particularly dangerous.

Risk Analysis

- Actions involved in risk analysis:
  - Determine which assets are most valuable
  - Identify risks to assets
  - Determine the likelihood of each risk occurring
  - Take action to manage the risk
- First steps of risk analysis process:
  - Identify the information assets in the organization hardware, software, and data
  - Assign value to those assets using a valuation method
  - Assigning value to assets is the foundation for decisions about cost/benefit tradeoffs

Risk Analysis

- Second step in risk analysis process:
  - Two major classifications of risk assessment techniques
    - Qualitative
    - Quantitative
  - Vulnerability
    - An internal weakness in a system that may potentially be exploited
    - Not having antivirus software is an example
  - Threat
    - A set of external circumstances that may allow a vulnerability to be exploited
    - The existence of a particular virus for example
  - Risk
    - occurs when a threat and a corresponding vulnerability both exist

Identifying and Assessing Risk

- Qualitative Risk Assessment
  - Focuses on analyzing intangible properties of an asset rather than monetary value.
  - Prioritizes risks to aid in the assignment of security resources.
  - Relatively easy to conduct

Identifying and Assessing Risk

- Quantitative Risk Assessment
  - Assigns dollar values to each risk based on measures such as asset value, exposure factor, annualized rate of occurrence, single loss expectancy, and annualized loss expectancy.
  - Uses potential loss amount to decide if it is worth implementing a security measure.

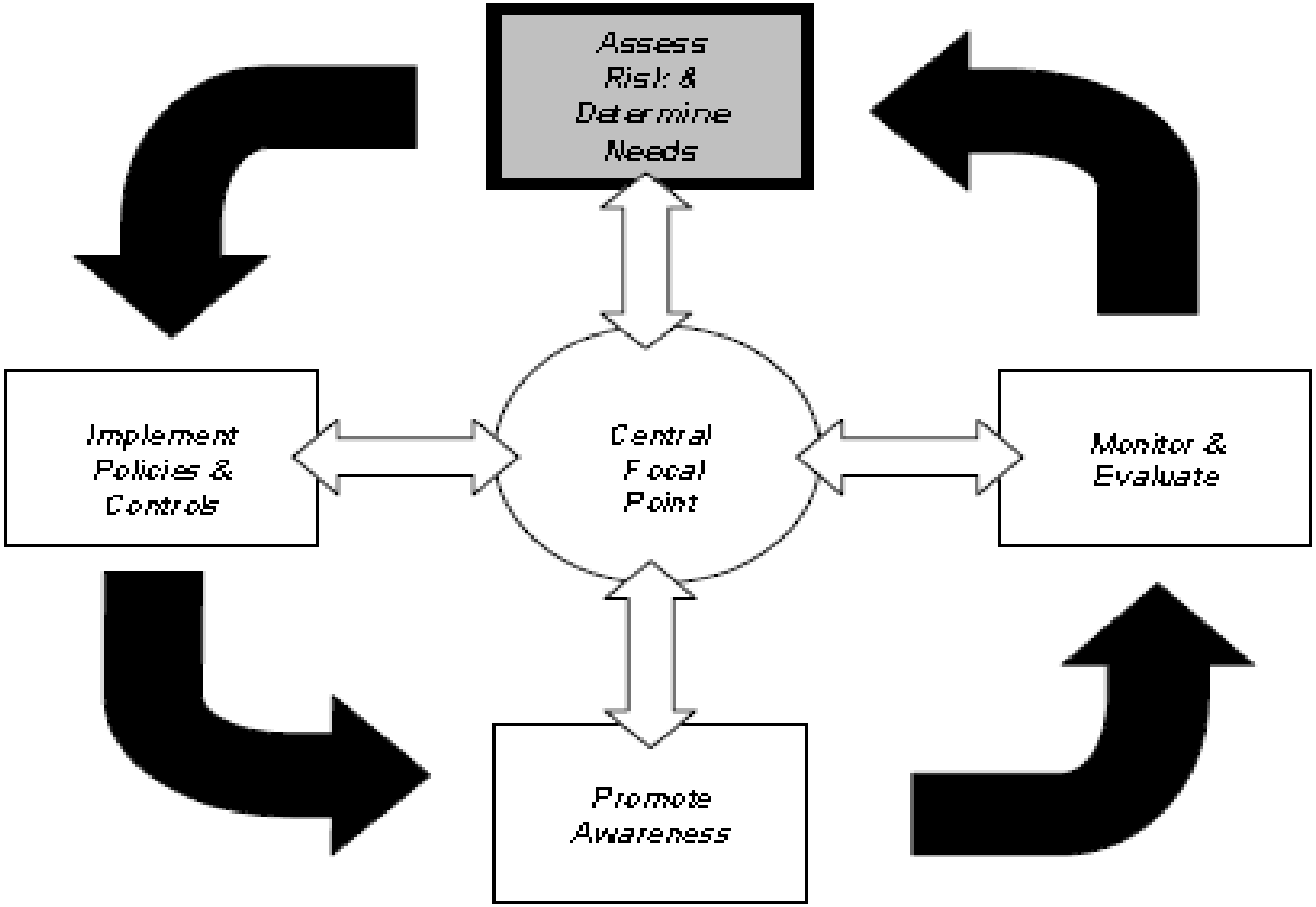
Managing Risks

- Risk Avoidance
  - Used when a risk overwhelms the benefits gained from having a particular mechanism available.
  - Avoid any possibility of risk by disabling the mechanism that is vulnerable.
  - Disabling e-mail is an example of risk avoidance.
- Risk Mitigation
  - Used when a threat poses a great risk to a system.
  - Takes preventative measures to reduce the risk.
  - A firewall is an example of risk mitigation.

Managing Risk

- Risk Acceptance
  - Do nothing to prevent or avoid the risk.
  - Useful when risk or potential damage is small.
- Risk Transference
  - Ensure that someone else is liable if damage occurs.
  - Buy insurance for example.
- Combinations of the above techniques are often used.

Figure 1: Risk Management Cycle



Basic Elements of the Risk Assessment Process [2]

Considering Security Tradeoffs

- Security can be looked at as a tradeoff between risks and benefits.
  - Cost of implementing the security mechanism and the amount of damage it may prevent.
  - Tradeoff considerations are security, user convenience, business goals, and expenses.

Considering Security Tradeoffs

- An important tradeoff involves user convenience
  - Between difficulty of use and willingness of users.
  - If users won’t use a system because of cumbersome security mechanisms, there is no benefit to having security.
  - If users go out of their way to circumvent security, the system may be even more vulnerable.

Policy and Education

- Cornerstone of a security effort is to
  - Implement proper policies
  - Educate users about those policies
- Information security policies should be
  - Flexible enough not to require frequent rewrites
  - Comprehensive enough to ensure coverage of situations
  - Available to all members of the organization
  - Readable and understandable

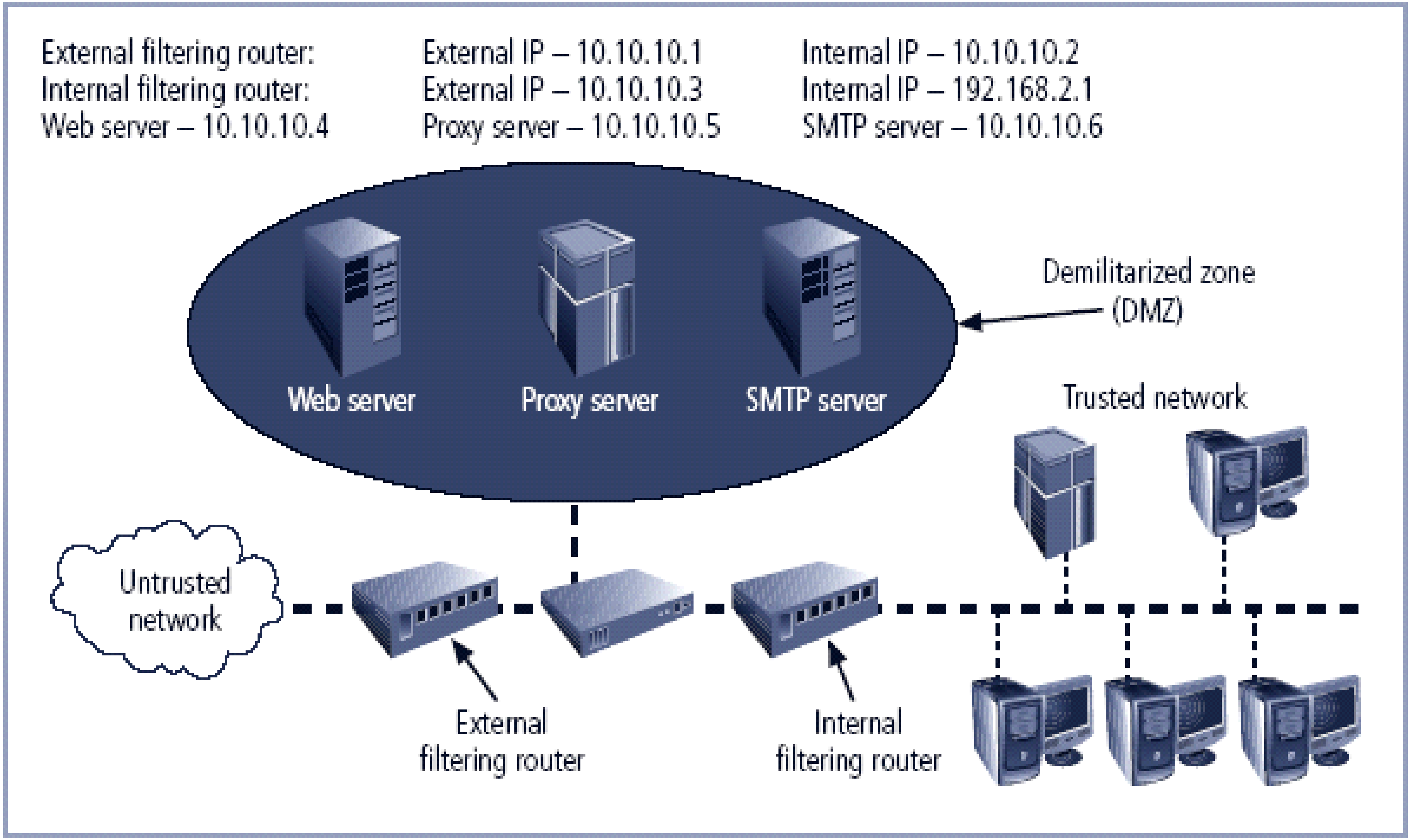
Common Security Policies

- Separation of Privileges:
  - No single person should have enough authority to cause a critical event to happen.
  - Tradeoff between security gained and manpower required to achieve it.
- Least Privilege:
  - An individual should have only the minimum level of access controls necessary to carry out job functions.
  - A common violation of this principle occurs because of administrator inattention.
    - Users are placed in groups that are too broad.
  - Another common violation occurs because of privilege creep.
    - Users are granted new privileges when they change roles without reviewing existing privileges.

Common Security Policies

- Defense in Depth
  - Defenses should be layered.
  - Layers begin with points of access to a network and continue with cascading security at bottleneck points.
- Security through Obscurity
  - In early days of computing, administrators depended upon secrecy about the security that was in place.
  - No longer very effective in most cases because so much information is freely available.

Defense in Depth



External filtering router:	External IP – 10.10.10.1	Internal IP – 10.10.10.2
Internal filtering router:	External IP – 10.10.10.3	Internal IP – 192.168.2.1
Web server – 10.10.10.4	Proxy server – 10.10.10.5	SMTP server – 10.10.10.6

FIGURE 6-14 Example Network Configuration[1]

Security Policies

- Goal is to have clearly defined security objectives:
  - Design specific controls
  - Keep users informed of expected behavior
- A security policy should be a written document.
  - Available to all users of an organizational information system.
- Security policies range from single documents to multiple documents for specialized use or for specific groups of users.

Acceptable Use Policy

- Defines allowable uses of an organization’s information resources.
- Must be specific enough to guide user activity but flexible enough to cover unanticipated situations
- Should answer key questions
  - What activities are acceptable?
  - What activities are not acceptable?
  - Where can users get more information as needed?
  - What to do if violations are suspected or have occurred?

Confidentiality Policy

- Outlines procedures used to safeguard sensitive information.
- Should cover all means of information dissemination including telephone, print, verbal, and computer.
- Questions include
  - What data is confidential and how should it be handled?
  - How is confidential information released?
  - What happens if information is released in violation of the policy?
- Employees may be asked to sign nondisclosure agreements.

Wireless Device Policy

- Includes mobile phones, PDAs, palm computers.
- Users often bring personal devices to the workplace.
- Policy should define
  - Types of equipment that can be purchased by the organization.
  - Type of personal equipment that may be brought into the facility.
  - Permissible activities.
  - Approval authorities for exceptions.

Education

- Includes education and training programs for affected employees.
- Users should be aware of their responsibilities with regard to policies.
- Two types of training
  - Initial training is a one-time program early in an employee’s tenure with company
  - Refresher training should be done periodically to
    - Remind employees of their responsibilities
    - Provide employees with updates of policies and technologies that affect their responsibilities

Enforcement and Maintenance

- Policies should define responsibilities for
  - Reporting violations.
  - Procedures when violations occur.
- Policies should be strictly enforced.
- Policy changes occur as companies and technologies change.
- Policies should contain provisions for modification through maintenance procedures.
  - Common to have periodic reviews mandated.

Personnel Security

- People are the weakest link in a security system.
- Perform background investigations
  - Should include criminal record checks, reference evaluations.
- Monitor employee activity
  - Can include monitoring Internet activity, surveillance cameras, telephone recording.
- Exit procedures for employees leaving the company.
  - Remind employees of any nondisclosure agreements.

Authentication

- Authentication is validation of a client’s identity.
- Four general ways in which authentication is carried out:
  - What a client knows
  - What a client has
  - Who a client is
  - What a client produces

Effectiveness of Biometrics

- Biometric technologies evaluated on three basic criteria:
  - False reject rate
  - False accept rate
  - Crossover error rate (CER)
- Balance must be struck between how acceptable security system is to users and its effectiveness in maintaining security.
  - Many biometric systems that are highly reliable and effective are considered intrusive.
  - As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of biometric controls, don’t implement them.

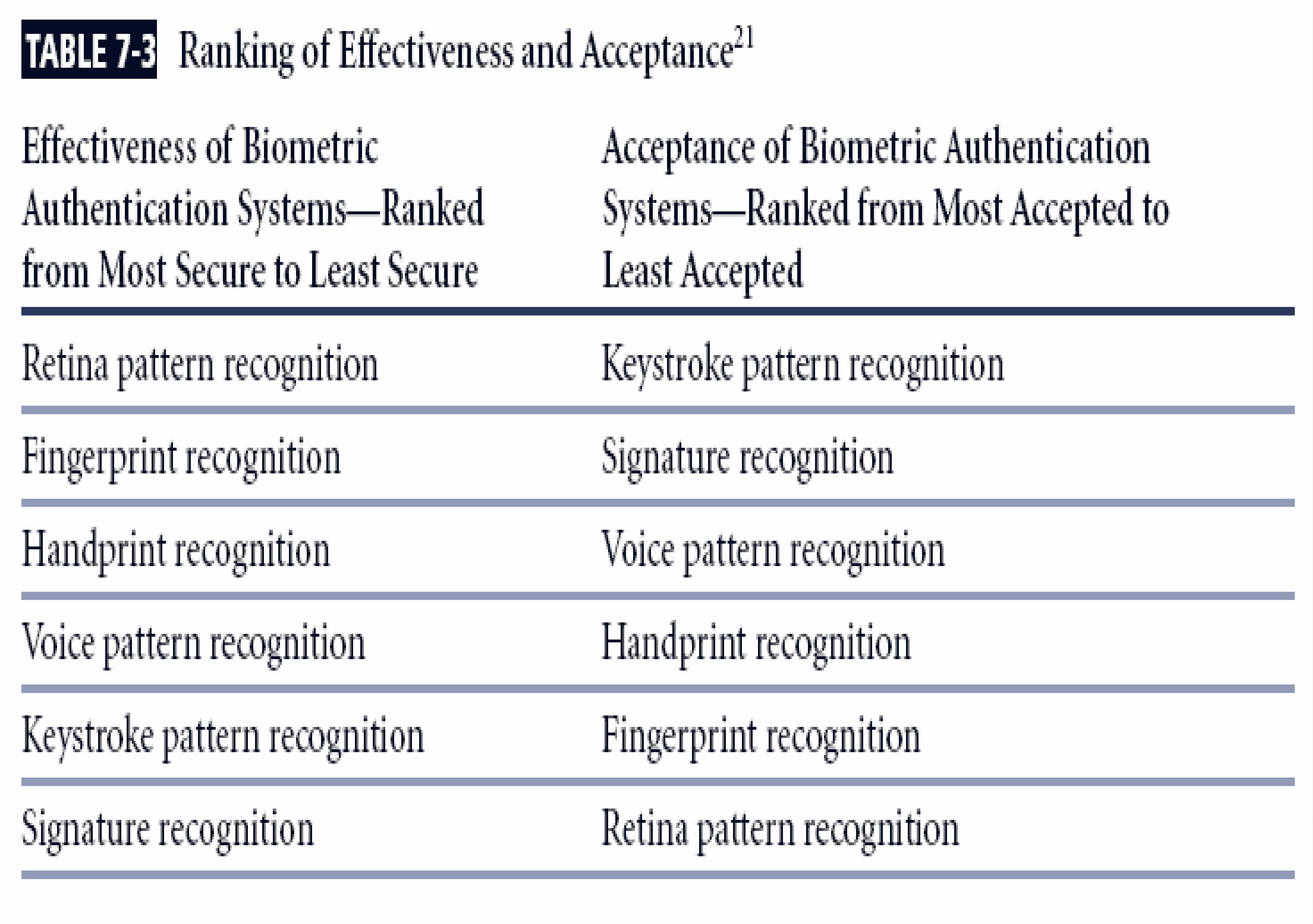


TABLE 7-3 Ranking of Effectiveness and Acceptance[21]

Effectiveness of Biometric Authentication Systems—Ranked from Most Secure to Least Secure	Acceptance of Biometric Authentication Systems—Ranked from Most Accepted to Least Accepted
Retina pattern recognition	Keystroke pattern recognition
Fingerprint recognition	Signature recognition
Handprint recognition	Voice pattern recognition
Voice pattern recognition	Handprint recognition
Keystroke pattern recognition	Fingerprint recognition
Signature recognition	Retina pattern recognition

Some Web Articles

- ***Flash on College Web Sites***
- ***Why Can't Johnny Develop Secure Software?***
- ***Wanted: Young cyber experts to defend Internet***
- ***Fighting back against web attacks***

10 Web Articles on Security

- AIRLINE SECURITY: THE TECHNICAL TASK OF CONNECTING DOTS http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222200692
- As attacks increase, U.S. struggles to recruit computer security experts http://www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122203789.html
- Carnegie Mellon Researcher Says Privacy Concerns Could Limit Benefits from Real-Time Data Analysis http://www.cmu.edu/news/archive/2009/December/dec17_privacydataanalysis.shtml
- Cell phone Encryption Code Is Divulged http://www.nytimes.com/2009/12/29/technology/29hack.html?pagewanted=1&_r=1
- How could Santa know if you've been good or bad? http://www.csiro.au/news/Automated-Expression-Recognition-Technology.html
- HP researchers try to tell you who your friends are http://www.mercurynews.com/breaking-news/ci_13971965?nclick_check=1
- In Shift, U.S. Talks to Russia on Internet Security http://www.nytimes.com/2009/12/13/science/13cyber.html
- Motion-sensing phones that predict your every move http://www.newscientist.com/article/mg20427385.900-motionsensing-phones-that-predict-your-every-move.html
- Moving Video to "Captcha" Robot Hackers http://www.aftau.org/site/News2?page=NewsArticle&id=11321
- Securing the Information Highway http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway

References

1. Principles of Information Security, 3rd Edition
2. Information Security Risk Assessment GAO

   Practices of Leading Organizations

   A Supplement to GAO's May 1998 Executive Guide on Information Security Management