Week 13

SECURITY AUDITING

LEGAL AND ETHICAL ASPECTS

Chapter 18

Security Auditing

Security audit An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises.

Security Audit Trail A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

By Definition

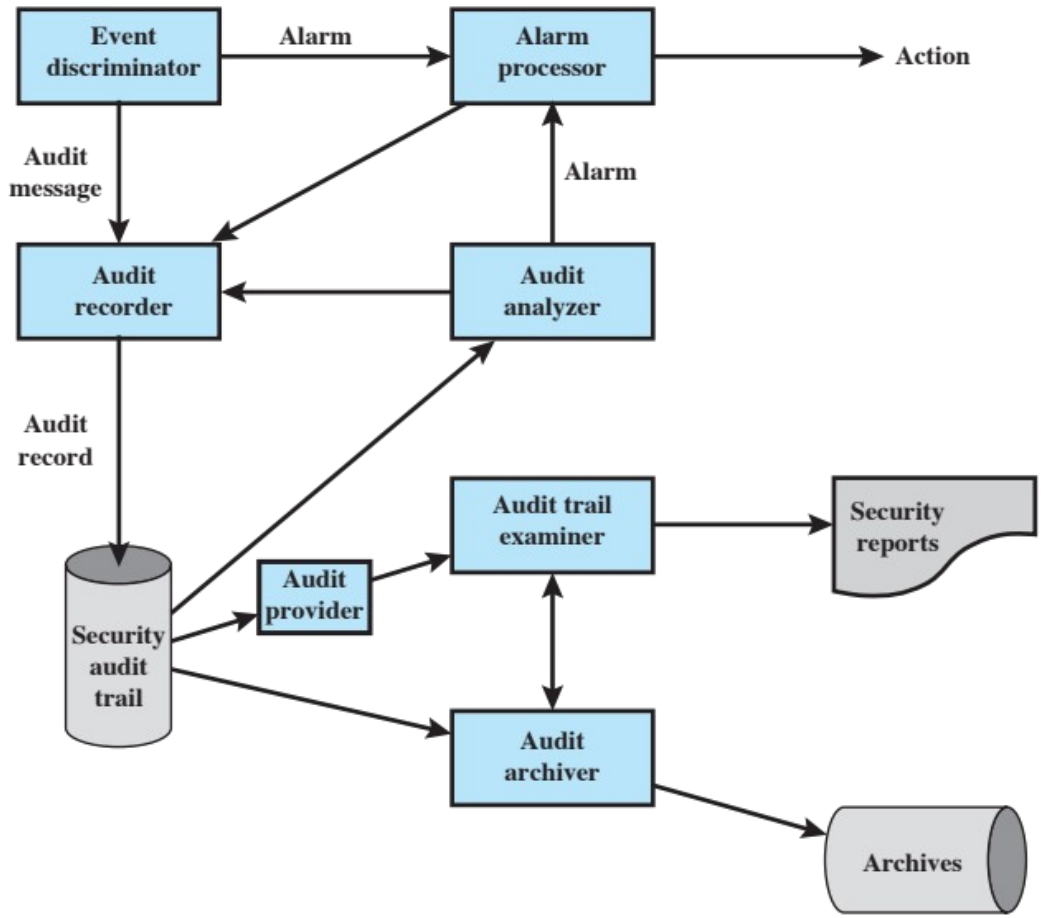


Figure 18.1 Security Audit and Alarms Model (X.816)

Security Audit and Alarm Models

Definition of an EVENT

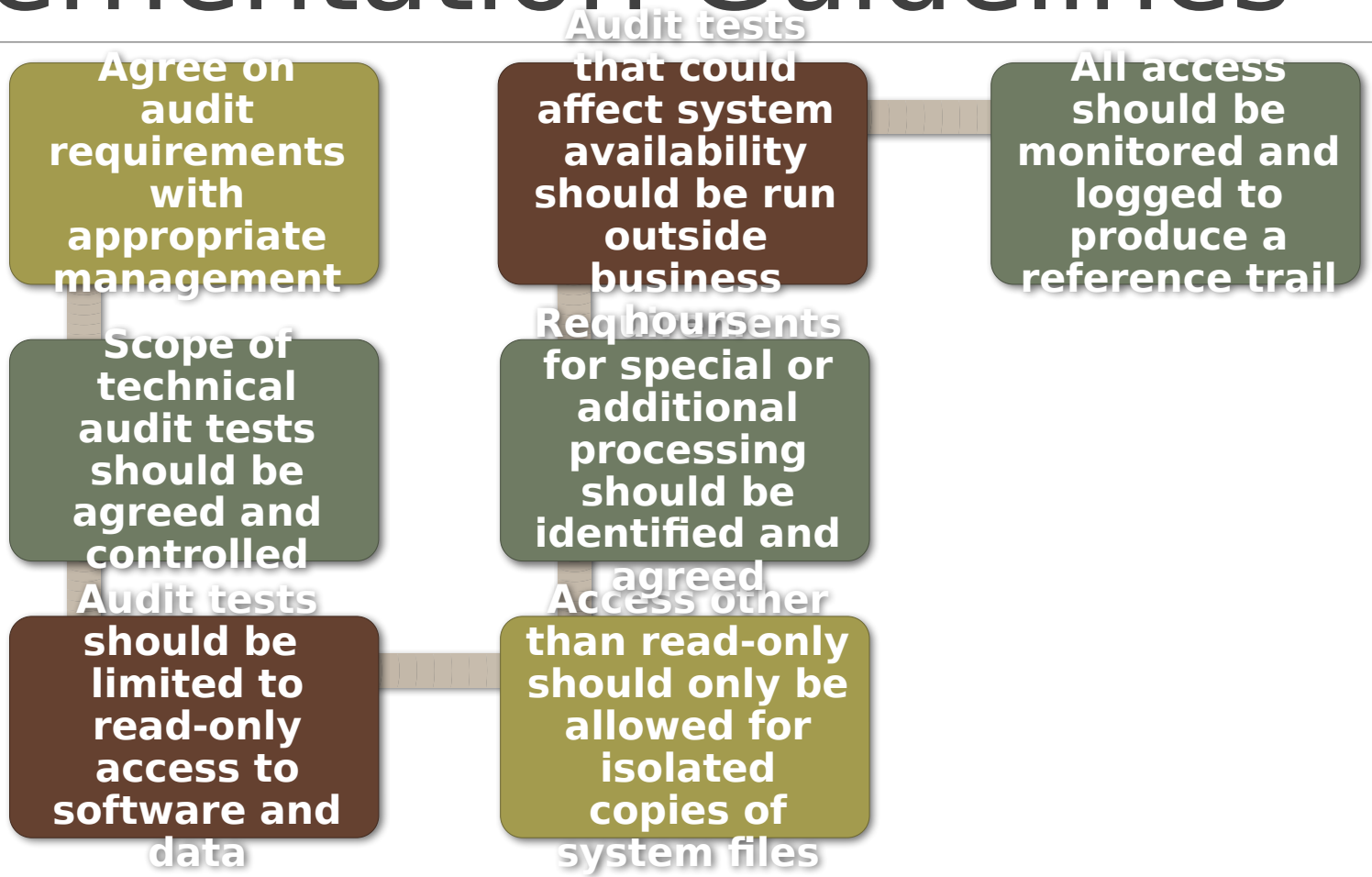
Common criteria suggests:

- Must define the set of events that are subject to audit
- Introduction of objects
- Deletion of objects
- Distribution or revocation of access rights or capabilities
- Changes to subject or object security attributes
- Policy checks performed by the security software
- Use of access rights to bypass a policy check
- Use of identification and authentication functions
- Security-related actions taken by an operator/user
- Import/export of data from/to removable media

Detecting Events

- Appropriate hooks must be available in the application and system software to enable event detection
- Monitoring software needs to be added to the system and to appropriate places to capture relevant activity
- An event recording function is needed, which includes the need to provide for a secure storage resistant to tampering or deletion
- Event and audit trail analysis software, tools, and interfaces may be used to analyze collected data as well as for investigating data trends and anomalies
- There is an additional requirement for the security of the auditing function
- Auditing system should have a minimal effect on functionality

Implementation Guidelines



What to Collect

- Events related to the use of the auditing software
- Events related to the security mechanisms on the system
- Events that are collected for use by the various security detection and prevention mechanisms
- Events related to system management and operation
- Operating system access
- Application access for selected applications
- Remote access

Security related events related to a specific connection
– Connection requests
– Connection confirmed
– Disconnection requests
– Disconnection confirmed
– Statistics appertaining to the connection

Security related events related to the use of security services
– Security service requests
– Security mechanisms usage
– Security alarms

Security related events related to management
– Management operations
– Management notifications

The list of auditable events should include at least
– Deny access
– Authenticate
– Change attribute
– Create object
– Delete object
– Modify object
– Use privilege

In terms of the individual security services, the following security-related events are important
– Authentication: verify success
– Authentication: verify fail
– Access control: decide access success
– Access control: decide access fail
– Non-repudiation: non-repudiable origination of message
– Non-repudiation: non-repudiable receipt of message
– Non-repudiation: unsuccessful repudiation of event
– Non-repudiation: successful repudiation of event
– Integrity: use of shield
– Integrity: use of unshield
– Integrity: validate success
– Integrity: validate fail
– Confidentiality: use of hide
– Confidentiality: use of reveal
– Audit: select event for auditing
– Audit: deselect event for auditing
– Audit: change audit event selection criteria

Auditable Items

```
Jan 27  17:14:04   host1  login: ROOT LOGIN console
Jan 27  17:15:04   host1  shutdown: reboot by root
Jan 27  17:18:38   host1  login: ROOT LOGIN console
Jan 27  17:19:37   host1  reboot: rebooted by root
Jan 28  09:46:53   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28  09:47:35   host1  shutdown: reboot by user1
Jan 28  09:53:24   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12  08:53:22   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17  08:57:50   host1  date: set by user1
Feb 17  13:22:52   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
```

(a) Sample system log file showing authentication messages

```
Apr 9 11:20:22   host1   AA06370:  from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23   host1   AA06370:  to=<user1@host1>, delay=00:00:02,stat=Sent
Apr 9 11:59:51   host1   AA06436:  from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52   host1   AA06436:  to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52   host1   AA06441:  from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53   host1   AA06441:  to=<user1@host1>, delay=00:00:01, stat=Sent
```

(b) Application-level audit record for a mail delivery system

```
rcp        user1   ttyp0    0.02 secs Fri Apr 8 16:02
ls         user1   ttyp0    0.14 secs Fri Apr 8 16:01
clear      user1   ttyp0    0.05 secs Fri Apr 8 16:01
rpcinfo    user1   ttyp0    0.20 secs Fri Apr 8 16:01
nroff      user2   ttyp2    0.75 secs Fri Apr 8 16:00
sh         user2   ttyp2    0.02 secs Fri Apr 8 16:00
mv         user2   ttyp2    0.02 secs Fri Apr 8 16:00
sh         user2   ttyp2    0.03 secs Fri Apr 8 16:00
col        user2   ttyp2    0.09 secs Fri Apr 8 16:00
man        user2   ttyp2    0.14 secs Fri Apr 8 15:57
```

(c) User log showing a chronological list of commands executed by users

Figure 18.4 Examples of Audit Trails

Audit Trail Examples

Physical Access Audit Trails

Generated by equipment that controls physical access

- Card-key systems, alarm systems

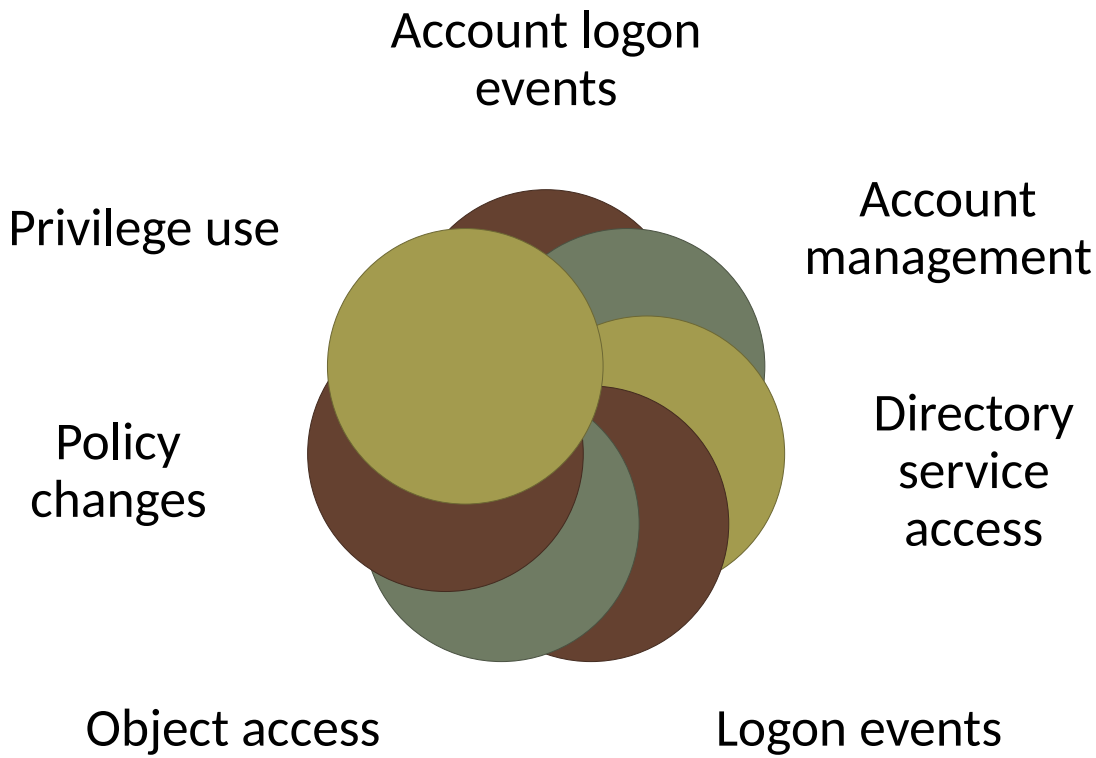
Sent to central host for analysis and storage

Data of interest:

- Date/time/location/user of access attempt
- Both valid and invalid access attempts
- Attempts to add/modify/delete physical access privileges
- May send violation messages to personnel

Protecting Audit Trail Data

Windows Event Categories



Audit Trail Analysis

Analysis programs and procedures vary widely

Must understand context of log entries

- Relevant information may reside in other entries in the same logs, other logs, and nonlog sources

Audit file formats contain mix of plain text and codes

- Must decipher manually/automatically

Ideally regularly review entries to gain understanding of baseline

Types of Audit Trail Analysis

Audit trails can be used in multiple ways

- This depends in part on when done

Possibilities include:

- Audit trail review after an event
  - Triggered by event to diagnose cause and remediate
  - Focuses on the audit trail entries that are relevant to the specific event
- Periodic review of audit trail data
  - Review bulk data to identify problems and behavior
- Real-time audit analysis
  - Part of an intrusion detection function

Audit Review

Audit review capability provides administrator with information from selected audit records

- Actions of one or more users
- Actions on a specific object or resource
- All or a specified set of audited exceptions
- Actions on a specific system/security attribute

May be filtered by time/source/frequency

Used to provide system activity baseline

Level of security related activity

Approaches to Data Analysis

Basic alerting

- Indicate interesting type of event has occurred

Baselining

- Define normal versus unusual events/patterns
- Compare with new data to detect changes
- Thresholding is the identification of data that exceed a particular baseline value

Windowing

- Detection of events within a given set of parameters

Correlation

- Seeks relationships among events

SIEM Systems

Software is a centralized logging software package similar to, but much more complex than, syslog

Provide a centralized, uniform audit trail storage facility and a suite of audit data analysis programs

There are two general configuration approaches:

- Agentless
  - SIEM server receives data from the individual log generating hosts without needing to have any special software installed on those hosts
- Agent-based
  - An agent program is installed on the log generating host to perform event filtering and aggregation and log normalization for a particular type of log, and then transmit the normalized log data to a SIEM server, usually on a real-time or near-real-time basis for analysis and storage

https://www.youtube.com/watch?v=ZuLazPgFtBE

Chapter 19

Legal and Ethical Aspects

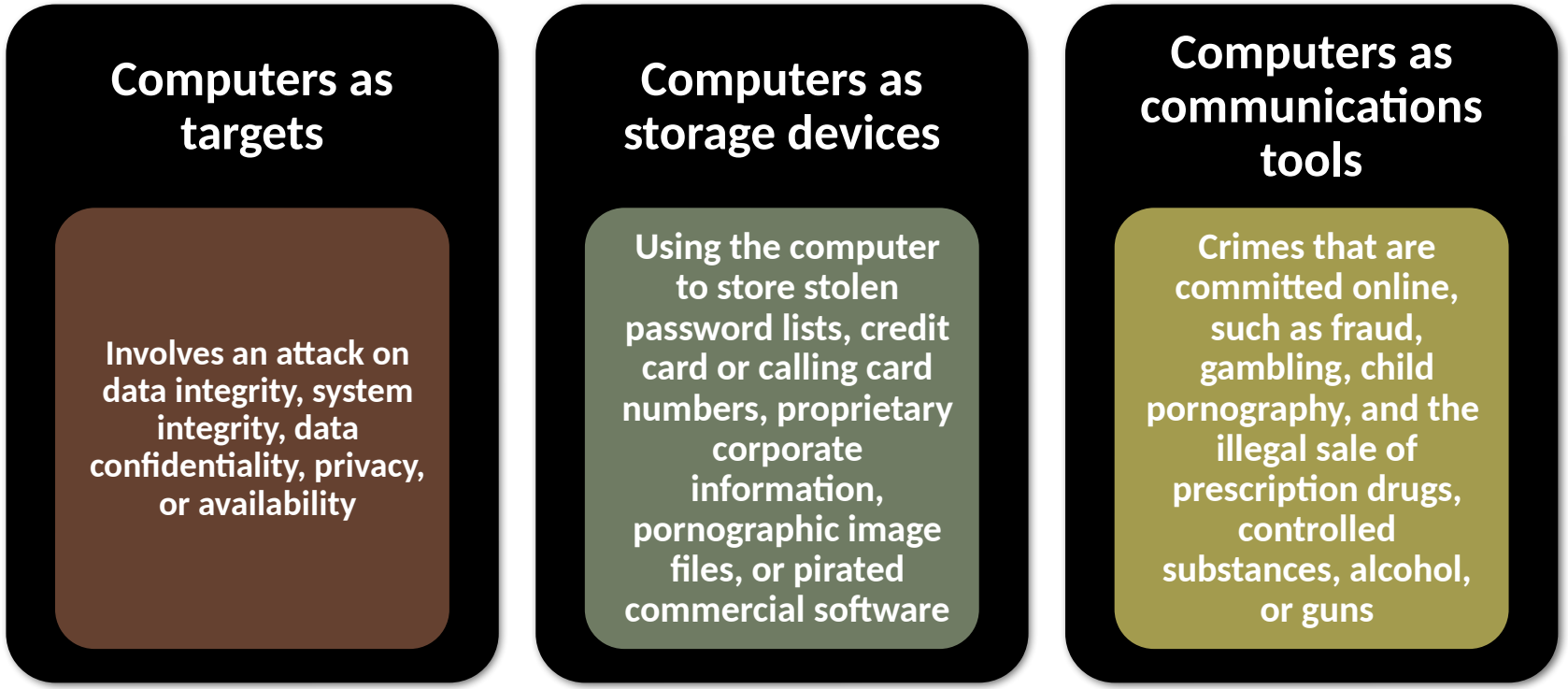
Cybercrime

"Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity."

--From the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

Types of Computer Crime

The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:



Article 2 Illegal access

The access to the whole or any part of a computer system without right.

Article 3 Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices

a The production, sale, procurement for use, import, distribution or otherwise making available of:

- **i** A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
- **ii** A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and

b The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

a Any input, alteration, deletion or suppression of computer data;

b Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Cybercrimes Cited in the Convention on Cybercrime (1/2)

Cybercrimes Cited in the Convention on Cybercrime (2/2)

Article 9 Offenses related to child pornography

a Producing child pornography for the purpose of its distribution through a computer system;
b Offering or making available child pornography through a computer system;
c Distributing or transmitting child pornography through a computer system;
d Procuring child pornography through a computer system for oneself or for another person;
e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

CERT 2007 (E-Crime Watch Survey Results)

	Committed (net %)	Insider (%)	Outsider (%)	Source Unknown (%)
Virus, worms or other malicious code	74	18	46	26
Unauthorized access to/use of information, systems or networks	55	25	30	10
Illegal generation of spam e-mail	53	6	38	17
Spyware (not including adware)	52	13	33	18
Denial of service attacks	49	9	32	14
Fraud (credit card fraud, etc.)	46	19	28	5
Phishing (someone posing as your company online in an attempt to gain personal data from your subscribers or employees)	46	5	35	12
Theft of other (proprietary) info including customer records, financial records, etc.	40	23	16	6
Theft of intellectual property	35	24	12	6
Intentional exposure of private or sensitive information	35	17	12	9
Identity theft of customer	33	13	19	6
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks	30	14	14	6
Zombie machines on organization's network/bots/use of network by BotNets	30	6	19	10
Web site defacement	24	4	14	7
Extortion	16	5	9	4
Other	17	6	8	7

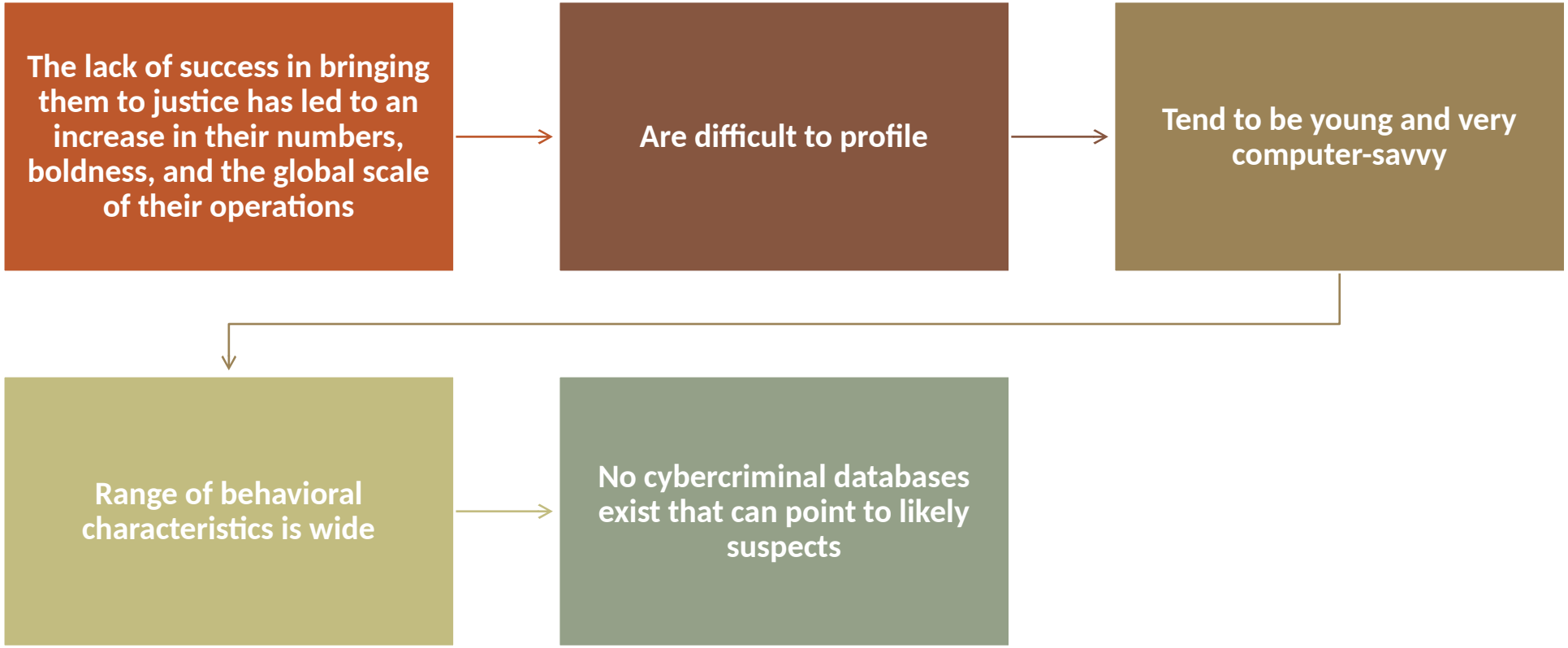
Law Enforcement Challenges

The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution

Law enforcement agency difficulties:

- Lack of investigators knowledgeable and experienced in dealing with this kind of crime
- Required technology may be beyond their budget
- The global nature of cybercrime
- Lack of collaboration and cooperation with remote law enforcement agencies
- Convention on Cybercrime introduces a common terminology for crimes and a framework for harmonizing laws globally

Cybercriminals



Cybercrime Victims

Working with Law Enforcement

Executive management and security administrators need to look upon law enforcement as a resource and tool

Management needs to:

- Understand the criminal investigation process
- Understand the inputs that investigators need
- Understand the ways in which the victim can contribute positively to the investigation

Property Infringement

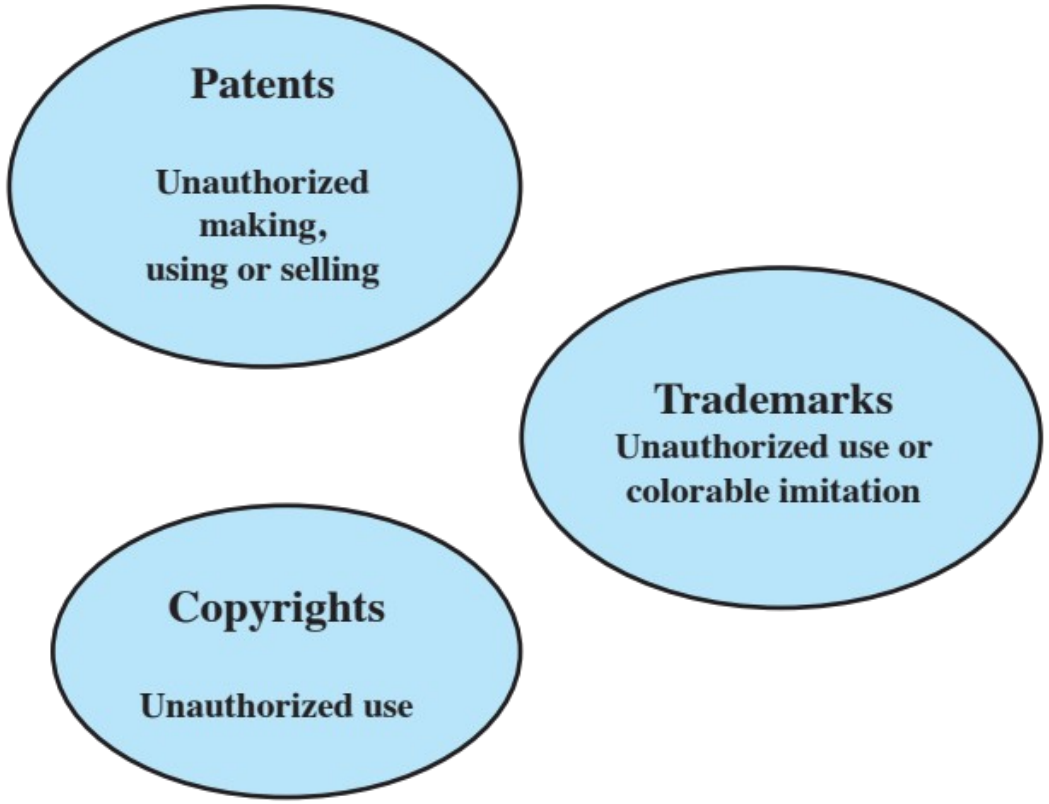


Figure 19.1 Intellectual Property Infringement

Copyright

Protects tangible or fixed expression of an idea but not the idea itself

Creator can claim and file copyright at a national government copyright office if:

- Proposed work is original
- Creator has put original idea in concrete form

Copyright Rights

Copyright owner has these exclusive rights, protected against infringement:

- Reproduction right
- Modification right
- Distribution right
- Public-performance right
- Public-display right

- Examples include:
  - Literary works
  - Musical works
  - Dramatic works
  - Pantomimes and choreographic works
  - Pictorial, graphic, and sculptural works
  - Motion pictures and other audiovisual works
  - Sound recordings
  - Architectural works
  - Software-related works

Patent

Grant a property right to the inventor

“The right to exclude others from making, using, offering for sale, or selling” the invention in the United States or “importing” the invention into the United States

Types:

Utility	Design	Plant
• Any new and useful process, machine, article of manufacture, or composition of matter	• New, original, and ornamental design for an article of manufacture	• Discovers and asexually reproduces any distinct and new variety of plant

Trademark

A word, name, symbol, or device

Used in trade with goods

Indicates source of goods

Distinguishes them from goods of others

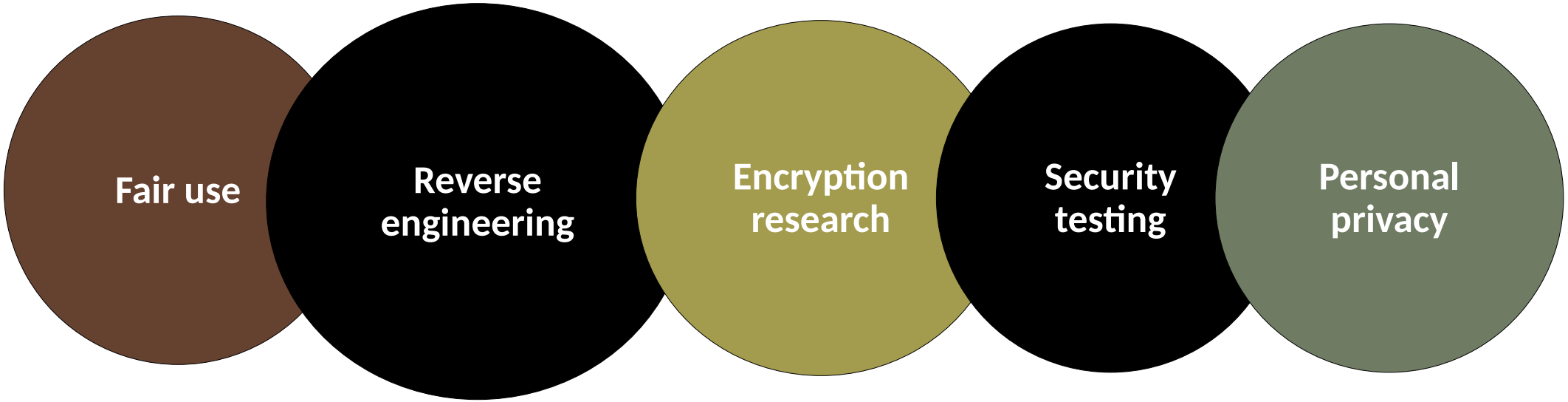
Trademark rights may be used to:

- Prevent others from using a confusingly similar mark
- But not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark

IP (Intellectual Property) related to Network and Computer Security

Software	Databases	Digital content	Algorithms
• Programs produced by vendors of commercial software • Shareware • Proprietary software created by an organization for internal use • Software produced by individuals	• Data that is collected and organized in such a fashion that it has potential commercial value	• Includes audio and video files, multimedia courseware, Web site content, and any other original digital work	• An example of a patentable algorithm is the RSA public-key cryptosystem

DMCA Exceptions



Privacy Data Surveillance

The demands of big business, government and law enforcement have created new threats to personal privacy

- Scientific and medical research data collection for analysis
- Law enforcement data surveillance
- Private organizations profiling
- This creates tension between enabling beneficial outcomes is areas including scientific research, public health, national security, law enforcement and efficient use of resources, while still respecting an individual's right to privacy

Another areas of particular concern is the rapid rise in the use of public social media sites

- These sites gather, analyze, and share large amounts of data on individuals and their interactions with other individuals and organizations
- Many people willingly upload large amounts of personal information, including photos and status updates
- This data could potentially be used by current and future employers, insurance companies, private investigators, and others, in their interactions with the individual

Data Privacy (GDPR)

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.

2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.

4. **Accuracy** — You must keep personal data accurate and up to date.

5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.

6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).

7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Ethical Issues

Many potential misuses and abuses of information and electronic communication that create privacy and security problems

Basic ethical principles developed by civilizations apply

- Unique considerations surrounding computers and information systems
- Scale of activities not possible before
- Creation of new types of entities for which no agreed ethical rules have previously been formed

Ethics:

"A system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions."

Ethical Issues related to Computers and Information Systems

Some ethical issues from computer use:

- Repositories and processors of information
- Producers of new forms and types of assets
- Instruments of acts
- Symbols of intimidation and deception

Those who understand, exploit technology, and have access permission, have power over these

Professional/Ethical Responsibilities

Concern with balancing professional responsibilities with ethical or moral responsibilities

Types of ethical areas a computing or IT professional may face:

- Ethical duty as a professional may come into conflict with loyalty to employer
- “Blowing the whistle”
- Expose a situation that can harm the public or a company’s customers
- Potential conflict of interest

Organizations have a duty to provide alternative, less extreme opportunities for the employee

- In-house ombudsperson coupled with a commitment not to penalize employees for exposing problems

Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Codes of Conduct

- Ethics are not precise laws or sets of facts
- Many areas may present ethical ambiguity
- Many professional societies have adopted ethical codes of conduct which can:

1. Be a positive stimulus and instill confidence
2. Be educational
3. Provide a measure of support
4. Be a means of deterrence and discipline
5. Enhance the profession's public image

Example of Code of Conduct (IEEE)

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.7 IEEE Code of Ethics