1.5. HAZARDS

Information hazards are risks that arise from the dissemination or the potential dissemination of true information that may cause harm or enable some agent to cause harm. Relative to their significance, and compared to many direct physical dangers, some types of information hazard are unduly neglected.

Information security hazards can be classified:

1. By information transfer mode as follows:

• *Data hazard:* This is specific data, such as the genetic sequence of a lethal pathogen or a blueprint for

making a thermonuclear weapon, if disseminated, it creates risk.

• *Idea hazard:* It is a general idea, if disseminated, creates risk, even without a data-rich detailed specification.

• *Attention hazard:* The drawing of attention to some particularly potent or relevant ideas or data increases risk, even when these ideas or data are already "known".

• *Template hazard:* The presentation of a template enables distinctive modes of information transfer and thereby creates risk.

• *Signaling hazard:* Verbal and non-verbal actions can indirectly transmit information about some hidden quality of the sender, and such social signaling creates risk.

• *Evocation hazard:* There can be a risk that the particular mode of presentation used to convey some

content can activate undesirable mental states and processes.

NB: Each of these information transfer modes can play a role in creating various kinds of risk.

2. By effect: this categorization produces fine-grained picture of the way in which information can be hazardous. These include:

• *Competitiveness hazard***:** These are risks that, by obtaining information, some competitors become

stronger, thereby weakening the competitive position.

This type of hazard constitutes the following:

– *Enemy hazard*: By obtaining information enemy or potential enemy becomes stronger and this increases the threat he/she poses to an organization.

– *Intellectual property hazard*: A faces the risk that some other firm B will obtain A's intellectual property, thereby weakening A's competitive position.

– *Commitment hazard*: This is risk that the obtainment of some information will weaken one's ability to credibly commit to some course of action.

– *Knowing-too-much hazard*: when one possesses some information she/he becomes a potential target or object of dislike.

• *Normal hazard*: Some social norms depend on a coordination of beliefs or expectations among many

subjects; and a risk is posed by information that could disrupt these expectations for the worst.

They include:

– *Information asymmetry hazard:* When one party to a transaction has the potential to gain information that the others lack resulting to market failure.

– *Unveiling hazard:* The functioning of some markets, and the support for some social policies, depends on the existence of a shared "veil of ignorance"; and the lifting of that veil can undermine those markets and policies.

– ***Recognition hazard:*** Some social fiction depends on some shared knowledge not becoming

common knowledge or not being publicly acknowledged; but public release of information could

ruin the pretense.

• *Ideological hazard:* An idea might, by entering into an ecology populated by other ideas, interact in ways which, in the context of extant institutional and social structures, produce a harmful outcome, even in the absence of any intention to harm.

• *Distraction and temptation hazards:* Information can harm us by distracting us or presenting us

with temptation.

• *Role model hazard:* Individuals can be corrupted and deformed by exposure to bad role models.

• Biasing hazard: When people are biased, they can be led further away from the truth by exposure to

information that triggers or amplifies their biases.

• **De-biasing hazard:** When people biases have individual or social benefits, harm could result from information that erodes these biases.

• Neuro-psychological hazard: Information might have negative effects on people's psyches because of

the particular ways in which their brains are structured, effects that would not arise in more "idealized"

cognitive architectures.

• Information-burying hazard: Irrelevant information can make relevant information harder to find,

thereby increasing search costs for agents with limited computational resources.

• Psychological reaction hazard: Information can reduce well-being by causing sadness, disappointment,or some other psychological effect in the receiver. These include:

– Belief-constituted value hazard: If some component of well-being depends constitutively on epistemic or attention states, then information that alters those states might thereby directly impact

well-being.

– Disappointment hazard: people emotional wellbeing can be adversely affected by the receipt of

bad news.

– Spoiler hazard: Fun that depends on ignorance and suspense is at risk of being destroyed by premature disclosure of truth.

– Mindset hazard: Our basic attitude or mindset might change in undesirable ways as a consequence of exposure to information of certain kinds.

• **Embarrassment hazard:** We may suffer psychological distress or reputation damage as a result of

embarrassing facts about ourselves being disclosed.

• **Information system hazard:** The behavior of some (non-human) information system can be adversely affected by some informational inputs or system interactions. These include:

– Information infrastructure failure hazard: There is a risk that some information system will malfunction, either accidentally or as result of cyber attack; and as a consequence, the owners or users

of the system may be inconvenienced, or third parties whose welfare depends on the system may

be harmed, or the malfunction might propagate through some dependent network, causing a wider

disturbance.

– Inf**ormation infrastructure misuse hazard:** There is a risk that some information system, while functioning according to specifications, will service some harmful purpose and will facilitate the achievement of said purpose by providing useful information infrastructure.

– Robot hazard: There are risks that derive substantially from the physical capabilities of a robotic system.

– Artificial intelligence hazard: There could be computer related risks in which the threat would derive primarily from the cognitive sophistication of the program rather than the specific properties of any actuators to which the system initially has access.

• Development hazard: Progress in some field of knowledge can lead to enhanced technological, organizational, or economic capabilities, which can produce negative consequences (independently of any particular extant competitive context).

1.6. Summary

• Access attacks occur when an attacker gains information that he or she is not authorized to access.

• Snooping, Eavesdropping, and Interception are the three types of Access attacks.

• Modification attacks are attacks against the integrity of information.

• ARP spoofing, MAC duplicating, and DNS spoofing are the three methods of redirecting traffic.

• Denial-of-Service attacks deny legitimate users' access to the system, information, or capabilities.

• Open file sharing, weak passwords, programming flaws, and buffer overflows were exploited by hackers to break into systems.

• In social engineering, the hacker uses human nature and the ability to lie, to access information.

• In Denial-of-Service attacks, legitimate users are denied access to the system, network, information, or applications.

• In Distributed Denial-of-Service attacks, many systems are coordinated to attack a single target.

• The attacker may target the information, applications, the system, or the communications media itself in a DoS attack.

• Repudiation is an attack against the accountability of the information.

REVISION QUESTIONS

Exercise 1. Differentiate between security mechanism and security service.

Example. Discuss the psychological and normal hazard as applied in system security.

Solution: Psychological reaction hazard: Information can reduce well-being by causing sadness, disappointment, or some other psychological effect in the receiver.

These include: Belief constituted value hazard: If some component of well-being depends constitutively on epistemic or attention states, then information that alters those states might thereby directly impact **well-being.**

i) Disappointment hazard: people emotional well being can be adversely affected by the receipt of bad news.

ii) Spoiler hazard: Fun that depends on ignorance and suspense is at risk of being destroyed by premature disclosure of truth.

iii) Mindset hazard: Our basic attitude or mindset might change in undesirable ways as a consequence of exposure to information of certain kinds.

Normal hazard: Some social norms depend on a coordination of beliefs or expectations among many subjects; and a risk is posed by information that could disrupt these expectations for the worse. They include:

Information asymmetry hazard: When one party to a transaction has the potential to gain information that the others lack, a market failure can result.

Unveiling hazard: The functioning of some markets, and the support for some social policies, depends on the existence of a shared "veil of ignorance"; and the lifting of which veil can undermine those markets and policies.

Recognition hazard: Some social fiction depends on some shared knowledge not becoming common knowledge or not being publicly acknowledged; but public release of information could ruin the pretense.

Exercise 2. Describe the modification and access attacks as used in information security.

Solutions to Exercises

EXERCISE 1.

a) Security Mechanism: is a process that is designed to detect, prevent or recover from counter security attack.

b) Security service: This is a process or communication service that enhances the security of the data processing system and the information transfer of an organization. The services are intended to counter security attacks and to make use of one or more security mechanisms to provide the service.

EXERCISE 2.

Modification Attacks: A modification attack is an attempt to modify information that the attacker is not authorized to modify. The attacker may change or delete existing information, or insert new information in a modification attack.

Modifying electronic information is easier than modifying information on paper. Access Attacks: An access attack is an attempt to see information that the attacker is not authorized to see. Snooping is looking through information files to find something interesting. Eavesdropping is when someone listens in on a conversation

that they are not a part of. Interception is an active attack against the information. To access the information on paper, the attacker needs to gain access to that paper. Good site security may prevent an outsider from accessing information on paper, but may not prevent an insider from gaining access.