Corporate Vital Defense Strategy: A framework for Information Assurance

Bel G. Raggad, Ph.D.

School of Computer Science and Information Systems

Pleasantville, NY 10570

braggad@pace.edu

CVDS: Vital Defense strategy:

1. Defend enclave;
2. Defend the Data Processing (DP) environment;
3. Defend infrastructure support.

How to defend the corporate enclave as required in the CVDS?

<u>CIAFT</u>: **structure and sufficient design information for**:

1. the protection of network access originating at the enclave;
2. the protection of remote access conducted by traveling users and remote users; and
3. the protection of interoperability across security levels.

*****Defending the enclave also includes defending external connections as required by the CVDS**.

How to defend DP as required in the CVDS?

Protecting:
-end-user workstations,
-servers, applications, and
-operating systems.
CIATF: explicit information details of how security requirements of divers DP elements are designed.
DP Resources:identified, analyzed before their security solutions designed and implemented.
End-user applications: secure emailing, secure web browsing, file protection, and mission specific applications.

How to defend the infrastructure support as required in the CVDS?

➢Defending DP, its networks, and its enclave is useless if the infrastructure support is not secure.

➢Two major areas should be planned:

- KIM/PKI (key management infrastructure/public key infrastructure), and
- D&R (detection and respond).

*** technologies, services, and processes used to manage public key certificates and symmetric cryptography.

Classes of attacks:

Attacks are better organized in terms of:

- the identity of the entity carrying the attack,
- their effects on system owners, and
- the models employed in the attacks.

Identities of entities carrying the attacks:

Whitten, Bentley, and Barlow (1996):

Five possible acting entities:

- an activity,
- a person,
- network resources,
- a technology, and
- a data resource

Security disruptions resulting from attacks:

Cohen (1995):

Three main groups:

- **information corruption (C),**
- **information leakage (L),**
- **information denial (D).**

Attack models:

Models: **combine people, data, knowledge, hardware, software, and other resources in order to achieve a specific objective, usually to cause harm to system owners**.

Four categories:

- Probe models,
- Infrastructure models,
- Authorized access models, and
- Factory models.

Probe attack models

- ➢Passive attacks that are designed to identify opportunities that can be explored to cause harm to system owners.

- ➢A probe model takes the form of any other method conformant with the attack opportunity the attacker is exploring .

Infrastructure attack models:

➢Attacks that are designed to induce entities to cause harm to system owners, by affecting an infrastructure attribute.

▪Generic as introducing ,malicious code, copy traveling data, an attempt to break a security feature; or

▪core as attacking a network backbone.

Factory attack models:

- Designed to induce an entity to indirectly cause harm to system owners by carrying the modification or the substitution of hardware or software at the factory, or during the distribution process.

How to develop a security information system?

Three dimensions:

- **attack model;**
- **security disruption produced; and**
- **the entity induced to cause the attack.**

That is:

Model x Disruption x Entity 60 Systems

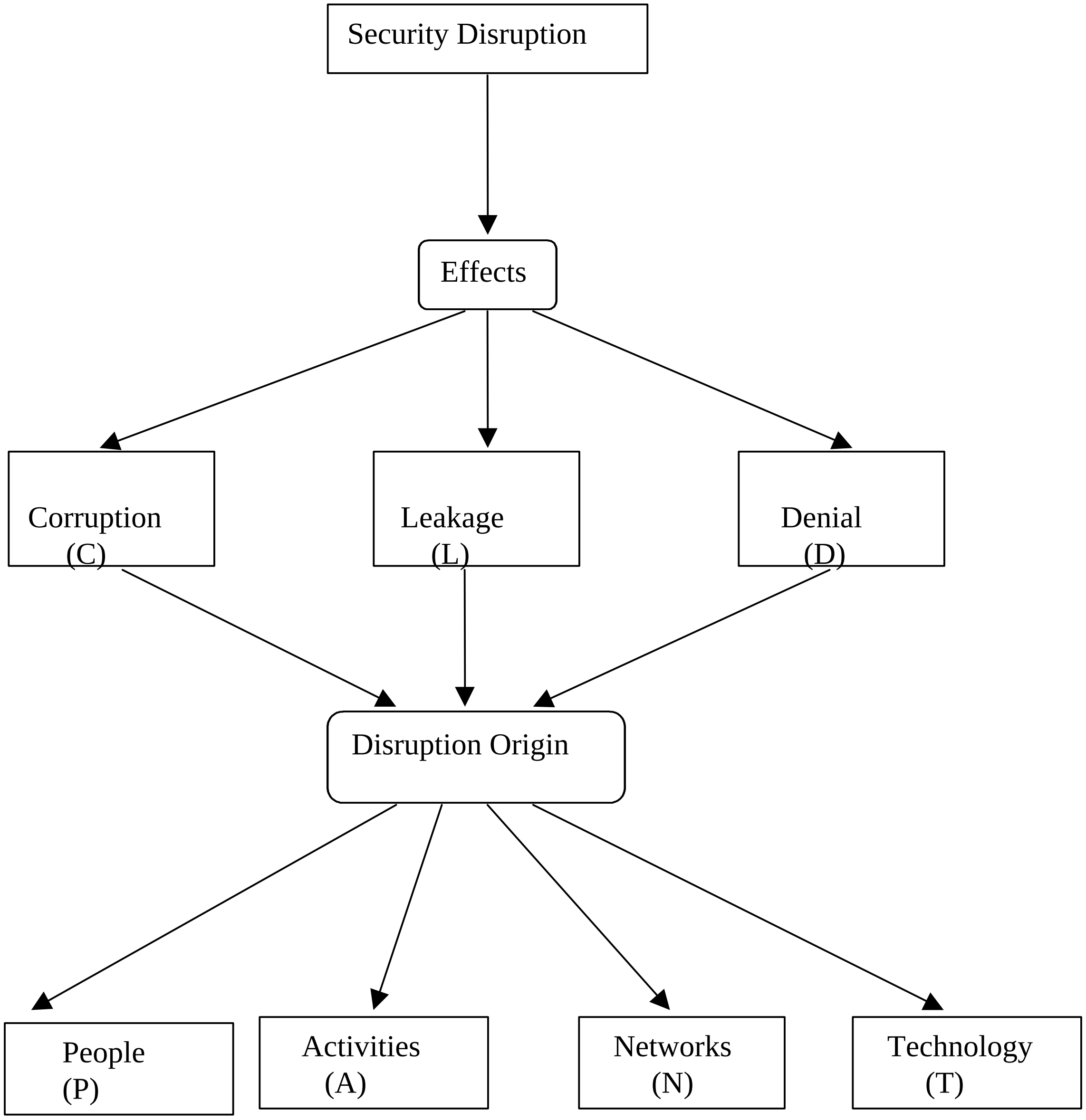

Figure 1: Security disruption classes defined by (Effect, Origin) pairs

Conclusion:

<u>60 default functional security information systems, defined in terms of</u>

- DoD’s attack models (probe; infrastructure; factory; and authorized-access models),
- Whitten, Bentlry, and Barlow’s entities (data; people, activities, technology; and networks) induced to cause the attack, and
- 3) Cohen’s security disruptions (information leakage; information corruption; and service denial) produced.

Automatic information security solutions can be developed. Some of the automatic security solutions are already provided as a part of the IDS literature.