Security – Threat Consequences

Threat Consequence: *A security violation that results from a threat action.*

Includes disclosure, deception, disruption, and usurpation. The following sections describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

This document is an excerpt from R. Shirey, Internet Security Glossary, IETF RFC 2828, May 2000. `http://www.ietf.org/rfc/rfc2828.txt`

1 Threat Consequence: Unauthorized Disclosure

A circumstance or event whereby an entity gains access to data for which the entity is not authorized. The following threat actions can cause unauthorized disclosure:

1.1 Threat Action: Exposure

A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:

Deliberate Exposure: Intentional release of sensitive data to an unauthorized entity.

Scavenging: Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Human error*: Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data.

Hardware/software error*: System failure that results in an entity gaining unauthorized knowledge of sensitive data.

1.2 Threat Action: Interception

A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. This includes:

Theft: Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.

Wiretapping (passive): Monitoring and recording data that is flowing between two points in a communication system.

Emanations analysis: Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

1.3 Threat Action: Inference

A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. This includes:

Traffic analysis: Gaining knowledge of data by observing the characteristics of communications that carry the data.

Signals analysis: Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

1.4 Threat Action: Intrusion

A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. This includes:

Trespass: Gaining unauthorized physical access to sensitive data by circumventing a system's protections.

Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Reverse engineering: Acquiring sensitive data by disassembling and analyzing the design of a system component.

Cryptanalysis: Transforming encrypted data into plaintext without having prior knowledge of encryption parameters or processes.

2 Threat Consequence: Deception

A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. The following threat actions can cause deception:

2.1 Threat Action: Masquerade

A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.

Spoof: Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

Malicious logic: In context of masquerade, any hardware, firmware, or software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

2.2 Threat Action: Falsification

A threat action whereby false data deceives an authorized entity.

Substitution: Altering or replacing valid data with false data that serves to deceive an authorized entity.

Insertion: Introducing false data that serves to deceive an authorized entity.

2.3 Threat Action: Repudiation

A threat action whereby an entity deceives another by falsely denying responsibility for an act.

False denial of origin: Action whereby the originator of data denies responsibility for its generation.

False denial of receipt: Action whereby the recipient of data denies receiving and possessing the data.

3 Threat Consequence: Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions. The following threat actions can cause disruption:

3.1 Threat Action: Incapacitation

A threat action that prevents or interrupts system operation by disabling a system component.

Malicious logic: In context of incapacitation, any hardware, firmware, or software intentionally introduced into a system to destroy system functions or resources.

Physical destruction: Deliberate destruction of a system component to interrupt or prevent system operation.

Human error*: Action or inaction that unintentionally disables a system component.

Hardware or software error*: Error that causes failure of a system component and leads to disruption of system operation.

Natural disaster*: Any "act of God" (e.g. fire, flood, earthquake, lightning, or wind) that disables a system component.

3.2 Threat Action: Corruption

A threat action that undesirably alters system operation by adversely modifying system functions or data.

Tamper: In context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.

Malicious logic: In context of corruption, any hardware, firmware, or software (e.g. a computer virus) intentionally introduced into a system to modify system functions or data.

Human error*: Human action or inaction that unintentionally results in the alteration of system functions or data.

Hardware or software error*: Error that results in the alteration of system functions or data.

Natural disaster*: Any "act of God" (e.g. power surge caused by lightning) that alters system functions or data.

3.3 Threat Action: Obstruction

A threat action that interrupts delivery of system services by hindering system operations.

Interference: Disruption of system operations by blocking communications or user data or control information.

Overload: Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

4 Threat Consequence: Usurpation

A circumstance or event that results in control of system services or functions by an unauthorized entity. The following threat actions can cause usurpation:

4.1 Threat Action: Misappropriation

A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.

Theft of service: Unauthorized use of service by an entity.

Theft of functionality: Unauthorized acquisition of actual hardware, software, or firmware of a system component.

Theft of data: Unauthorized acquisition and use of data.

4.2 Threat Action: Misuse

A threat action that causes a system component to perform a function or service that is detrimental to system security.

Tamper: In context of misuse, deliberate alteration of a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

Malicious logic: In context of misuse, any hardware, software, or firmware intentionally introduced into a system to perform or control execution of an unauthorized function or service.

Violation of permissions: Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.