Cyber Terminology Discussion

Dr. Carol Woody
Christopher Alberts
Charles Wallen

April 26, 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0348

Cyber Terminology Discussion

Security and Resilience

Multiple Definitions for Security and Resilience

There are no universally adopted definitions of security and resilience.

For example, the NIST online glossary[1] lists multiple definitions for each of the following terms:

- Security (9)
- Cybersecurity (5)
- Resilience (10)
- Cyber resilience (2)

This presentation examines one definition for each of the above terms.

1. https://csrc.nist.gov/glossary

Security and Resilience: Definitions -1

Security

- A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [NIST 800-53, Rev 5]

Cybersecurity

- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
  [NIST 800-53, Rev 5]

Security and Resilience: Definitions -2

Resilience

- The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs. [NIST 800-53, Rev 5]

Cyber Resiliency

- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. [NIST 800-160, Vol 2, Rev 1]

Security versus Resilience -1

Security / Cybersecurity

- Establish and maintain protective measures
- Prevent damage
- Protect systems and networks
- Restore services after disruption
- Ensure availability, integrity, authentication, confidentiality, and nonrepudiation

Resilience / Cyber Resiliency

- Operate under and adapt to adverse conditions or stress
- Operate in a degraded or debilitated state
- Maintain essential operational capabilities
- Recover to an effective operational posture in a time frame consistent with mission needs

Security versus Resilience -2

For most definitions

- Security and resilience have some degree of overlap.
- Security includes some unique aspects not included in resilience.
- Resilience includes some unique aspects not included in security.

The definitions for security and resilience are not mutually exclusive.

Viewing Security and Resilience though a Risk Lens

Security and resilience are abstract concepts.

Risk management is an essential practice for both security and resilience.

When discussing risk management, you need to address the following:

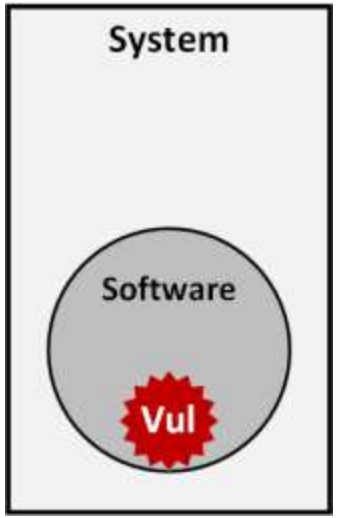
- Vulnerability
- Threat
- Risk

By doing this, we can make abstract concepts (i.e., security and resilience) more tangible.

Note: We have now introduced more definitions into the mix.

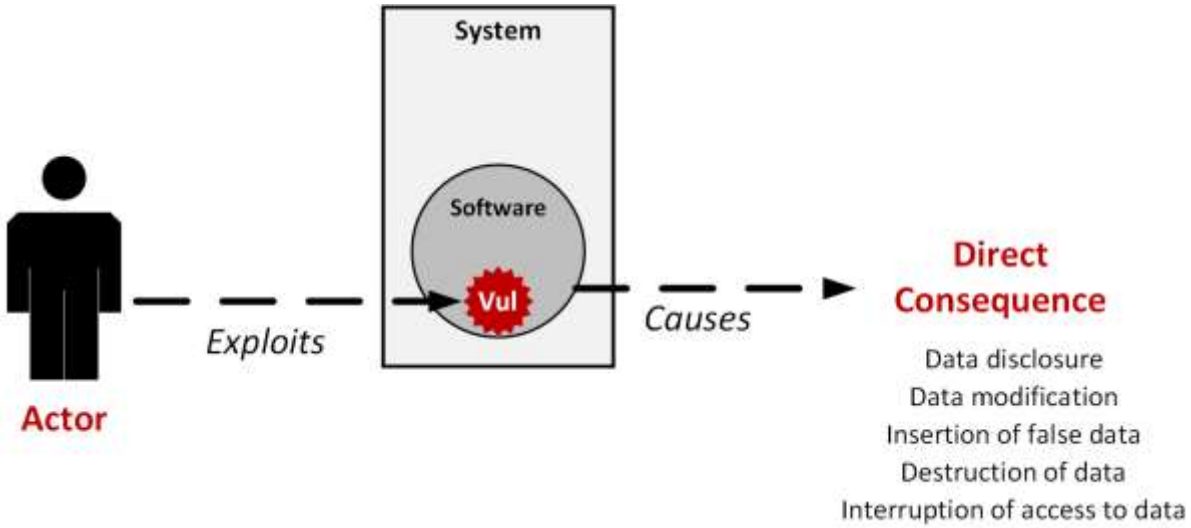
Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
[NIST 800-53, Rev 5]



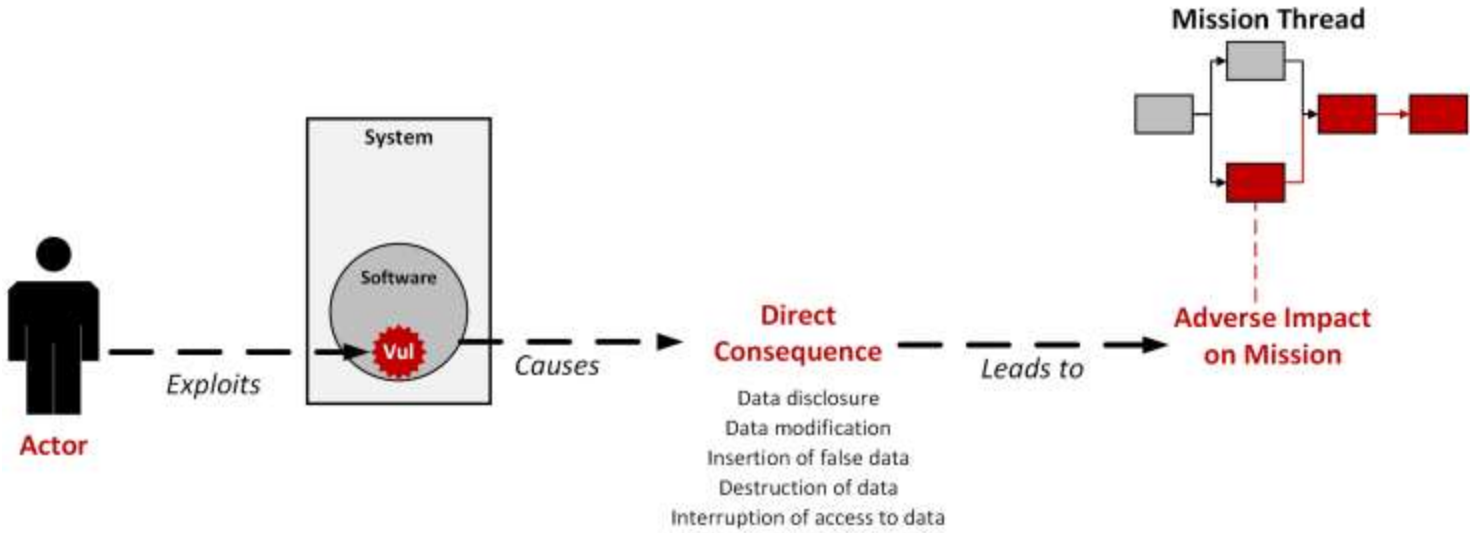
Threat

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST 800-53, Rev 5]



Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [NIST 800-53, Rev 5]



Risk Mitigation Strategies

Risk Mitigation

- Prioritizing, evaluating, and implementing the appropriate risk-reducing controls / countermeasures recommended from the risk management process. [NIST 800-53, Rev 5]

The following strategies are considered during risk mitigation:

- Recognize or monitor
- Resist or protect
- Respond
- Recover

Based on our experience, risk mitigation strategies typically include a mix of security and resilience controls.

Summary

There is no universally adopted cyber terminology.

People use different “dialects” when discussing cyber concepts and issues.

- Always look for miscommunication due to terminology mismatches.
- Understand which guidelines or standards people are using.
- Be prepared to take the lead on being the “translator” for your audience.

Try moving from abstract concepts to concrete data when possible.

Diagraming, analysis, and modeling techniques can

- Bypass terminology mismatches
- Help develop a common understanding

Research topic: Apply logical argumentation to refine definitions.

References

[NIST 800-53, Rev 5] National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53 Revision 1. National Institute of Standards and Technology. 2020.

[NIST 800-160, Vol 2, Rev 1] National Institute of Standards and Technology. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Volume 2 Revision 5. National Institute of Standards and Technology. 2021.