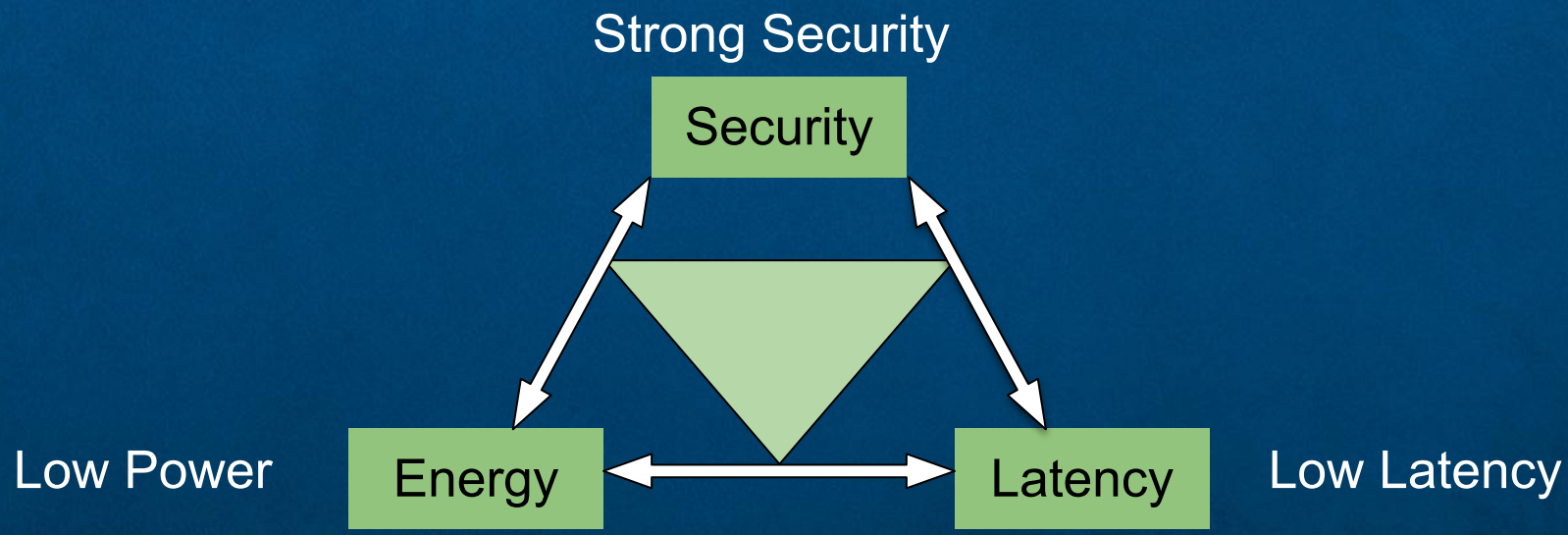
Week 3

Defense in Depth and Risk Response

BYU IDAHO

RESOURCE VS SECURITY CONSTRAINT

In cryptography there is a constraint between resources and security. Security is the most important part of the constraint but it must be balanced between energy consumption (the battery level of a device) and latency (the time it takes to encrypt or decrypt data); this creates an inverted triangle relationship. This concept also applies to software, applications, and even your physical security.



BYU IDAHO

SECURITY VS. CONVENIENCE SCALE

When it comes to cyber security there is a causal relationship between the convenience of a system or device and the security of that system or device. As one side of the scale goes up the other goes down. This concept also applies to software, applications, and even your physical security.

DEFENSE IN DEPTH

Defense-in-depth (DiD): a strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited; also known as Layered Security.

Physical Security: physical protections for computers, data, and assets (digital or physical) from intrusion or theft by a threat actor.

Digital Security: virtual (digital) protections for computers, data, and other digital assets from intrusion or theft by a threat actor.

DEFENSE IN DEPTH: PHYSICAL

Cable Lock: a special cable that locks directly to a device and back to a stationary object;officially known as the Universal Notebook Security Cable.

Door Locks: a lock on an interior or exterior door requiring a key or combination of some kind to open or unlock.

Fencing: a barrier enclosing or bordering an area designed to limit access to authorized entry points.

Lighting: interior and primarily exterior lighting designed to act as a deterrent to any potential threat actor.

DEFENSE IN DEPTH: PHYSICAL

Motion Detection: the process of detecting a change in the position of an object relative to its surroundings or a change in the surroundings relative to an object.

Privacy Screen (Filter): a thin piece of plastic placed over your monitor or display panel in order to prevent other individuals from absorbing confidential information.

Safe: a secure lockable box used for securing valuable objects against theft and/or damage.

Video Surveillance: monitoring activity in an area or building using cameras; the cameras may or may not be recording, internet connected, or on a closed circuit.

DEFENSE IN DEPTH: DIGITAL

Antivirus (AV): software designed to detect, prevent, and destroy computer viruses.

Firewall: a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Malware Scanner: software that deep scans a device to detect, prevent, and destroy a malware infection.

DEFENSE IN DEPTH: PHYSICAL & DIGITAL

Obscurity: security designed and deployed to be unknown, inconspicuous, or unimportant to a threat actor.

Physical Security: physical protections for computers, data, and assets (digital or physical) from intrusion or theft by a threat actor.

Vendor Diversity: the practice of implementing security controls and software from different vendors to increase security.

Least Privilege: the principle that users and systems must be able to access only the information and resources necessary for their legitimate purposes.

DEFENSE IN DEPTH: PHYSICAL & DIGITAL

Key Management: managing the generation, creation, exchanging, storing, using, and replacing of virtual or physical keys.

Security Simplicity: security policies, procedures, and implementations are easy to understand and follow.

Untrained User: a user who is unfamiliar with a system, device, policy, or procedure; untrained user is obviously not a great security defense, but a trained user is!

RISK RESPONSE

Acceptance: risk is acknowledged and no steps taken to avoid it.

Avoidance: risk is identified and a decision is made not to engage in an activity.

Mitigation: risk is identified and attempts are made to make it less serious.

Transference: risk is transferred to someone else; insurance.

REFERENCES

Blue Vespa Scooter [PNG]. Png Find, Aug. 2019, https://www.pngfind.com/mpng/hbbTbx_scooter-png-vespa-png-transparent-png.

Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.). Boston, MA: Cengage.

Justice Icon [PNG]. Ulm, Germany: Pixabay. Free for commercial use, no attribution required.