ECS655U: Security Engineering

Week 11: Security Management

Dr Arman Khouzani

March 22, 2019

EECS, QMUL

Security Management

Security Assessment

Nomenclature (terminologies) related to security assessment: Security Asset, Threat, Vulnerability, Risk.

- **Asset:** Anything that has a value (or can cause loss if compromised) and needs to be protected, e.g., employees/customers, infrastructure, intellectual property, data, services, reputation, etc.

Security Assessment

Security Asset, Threat, Vulnerability, Risk.

- **Threat:** Any potential for occurrence of a violation of security (leading to a violation of security service, e.g. obtaining/viewing confidential data, altering the data/service, or destroying data/service or making it inaccessible, etc).
  - An **Attack** is a threat that is carried out (by an **Attacker**, using **exploits**)
  - **Exploit**: software/commands that take advantage of vulnerabilities to enable an **attack**.
  - A **Threat Agent** is an entity that poses a threat, i.e., can carry out an attack.

Security Assessment

Examples of Threat-Agent types:

- *Anonymous Attacker*
  - script-kiddies: typically non-targeted attacks
  - hackers for hire: typically targeted attacks
  - nation-states: capable of launching "*advanced persistent threat (APT)*"
- *Trusted Attacker* (a.k.a *Malicious Tenants*)
- *Insider Threat*

Security Assessment

Examples of Attacks:

- *Traffic Eavesdropping*
- *Malicious Intermediary* — a.k.a. *Main-In-The-Middle* (MITM)
- *Denial-of-Service*
- *Distributed-Denial-of-Service (DDoS)*
- *Exploiting Insufficient Authorization/Weak Authentication*
- *Virtualisation Attack* (VM/sandbox Escaping)
- *Malicious Payload Attack*

Security Assessment

Security Asset, Threat, Vulnerability, Risk.

- **Vulnerability:** A **weakness** (gap/bug, etc) that can be exploited by an attacker to perform its attack.

Examples of vulnerabilities:

- Buffer Overflow, Buffer Overrun, Stack Overflow
- Weak Crypto-Suites, Flawed Implementation of cryptographic Primitives, Flawed Implementation of cryptographic Protocols, Flawed Key Management, Weak Password Policy
- Hard-coded Credentials, Race Condition, Weak input validation/sanitisation
- Unused Open Ports/Services, Side Channels, ...

Security Assessment

Security Asset, Threat, Vulnerability, Risk.

- **(Security) Risk:** The expected loss/harm/damage that can be brought about as a result of security attacks.

Security Assessment

So the security risk of an organisation depends on:

- The **asset profile** of an organization.
- Its **vulnerability profile** (list of known vulnerabilities in the organization, and their seriousness, ease of discovery, ease of exploitation, success rate, etc).
- The **impact** of each vulnerability: the expected losses/damages if the vulnerability is successfully exploited.
- The organization's **threat profile** (what type of threat agents the organization will be the target of).

Security Controls

Security Controls, Mechanisms, Policy, Plan.

- **Security Controls** Counter-measures used to prevent the exploitation of a vulnerability, or decrease its probability of successful exploitation, or mitigate its impact upon a successful exploitation (a security response).
- **Security Mechanisms** The technologies, tools and procedures that perform Security Controls (often used interchangeably with **Security Controls**).

Security Plan

Security Controls, Mechanisms, Policy, Plan.

- **Security Policy** A set of security rules and regulations (what is allowed/disallowed). Security policy is enforced through security controls.
- **Security Plan** Description of the implementation of your Information Security Policy (the list of security controls to be implemented & detail of implementation, e.g. intensity level, etc.)

Top Security Controls

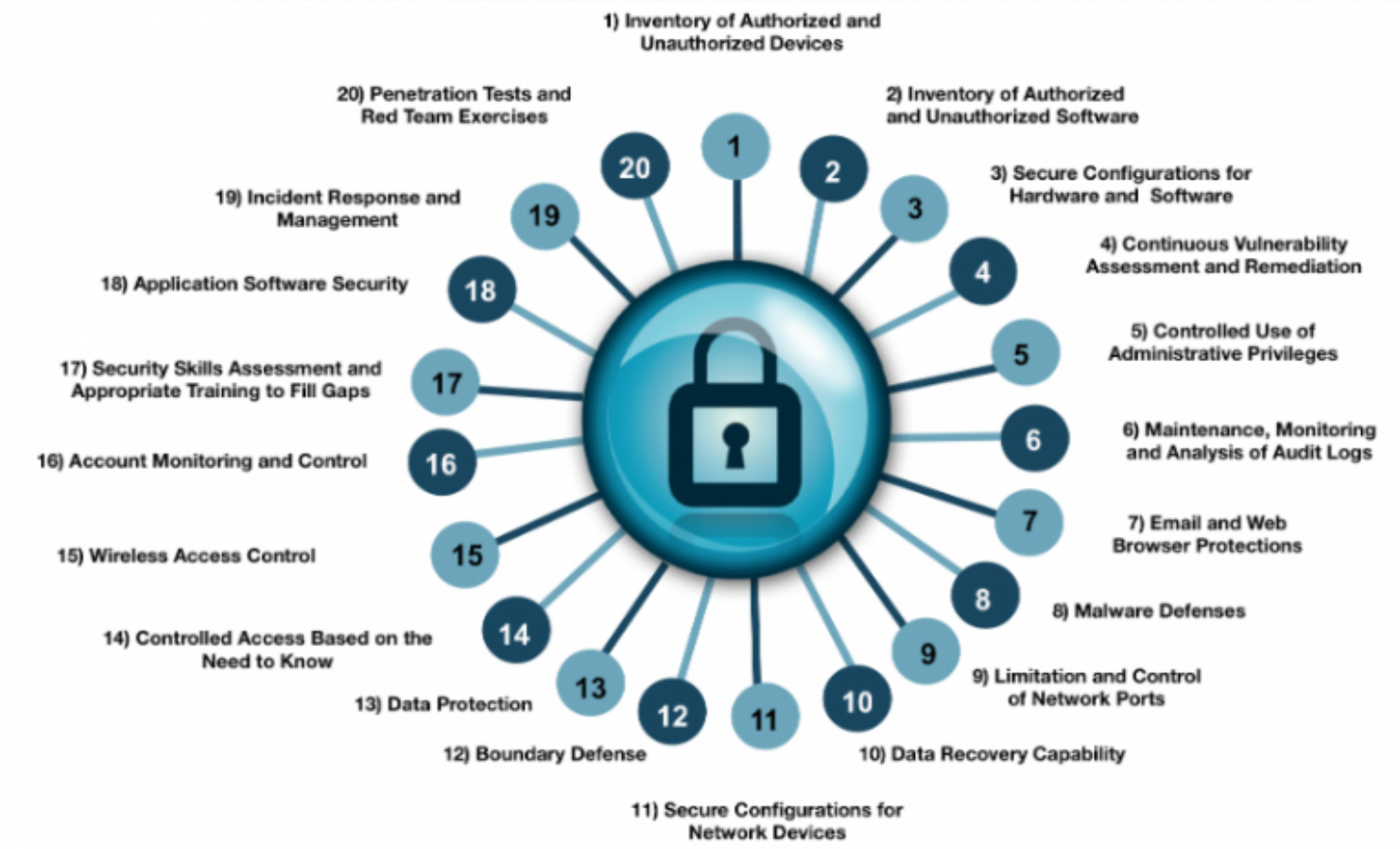

Figure 1: Top-20 Critical Security Controls by SANS (no need to memorize!) (http://www.sans.org/critical-security-controls/)

Security Controls

Hardening is the process of stripping unnecessary software/privileges from a system to limit potential vulnerabilities that can be exploited by attackers (i.e., reducing its “attack surface”).

- Examples of hardening: removing redundant programs, closing unnecessary server ports, disabling unused services, internal root accounts and guest access, etc.

Security Controls: Categories

Prevention, Detection, Response/Recovery

Security Principles

KISS, Defence in Depth, Obscurity is Not Security, Security is Economics, Least Privileges, Separation of Responsibilities, Total Mediation, Avoid Security Theatre, Human Factor