CS 5430

Beyond Attacks

Prof. Clarkson
Spring 2017

Attacks!

Beyond attacks

Attacks
are perpetrated by
threats
that inflict
harm
by exploiting
vulnerabilities
which are controlled by
countermeasures.

Harm

A negative consequence to a system asset

- Assets:
  - physical objects (e.g., money)
  - intangible objects (e.g., bank account balance)
- In computer systems:
  - information is typically the main asset
  - hardware and software could be assets
  - people are not typically considered to be assets

Stakeholders

- Anything of value to a stakeholder in system could be an asset
  - direct value: damage affects asset itself
  - indirect value: damage affects something else, e.g. reputation
- An object is not an asset if it doesn't have value to some stakeholder
- A principal isn't a stakeholder if it doesn't value some system object
  - We won't consider a generic "attacker" to be a stakeholder

Harm

Kinds of harm:

- Damage to confidentiality (e.g., interception)
- Damage to integrity (e.g., modification, fabrication)
- Damage to availability (e.g., interruption)

BISTRO

CLARKSON

Ex: BISTRO CLARKSON

- New restaurant in Collegetown
- Contracts with opentable.com to make online reservations possible
- What confidentiality, integrity, and availability harms does Bistro Clarkson risk by contracting with opentable.com?

Threat

A principal that has potential to cause harm to assets

- Adversary or attacker: a human threat, motivated and capable
- Sometimes humans aren't malicious: accidents happen
- Sometimes non-humans cause harm: floods, earthquakes, power outage, hardware failure

Threats

[S1, based on U.S. Defense Science Board]

- Inquisitive people, unintentional blunders
- Hackers driven by technical challenges
- Disgruntled employees or customers seeking revenge
- Criminals interested in personal financial gain, stealing services, or industrial espionage
- Organized crime with the intent of hiding something or financial gain
- Organized terrorist groups attempting to influence policy by isolated attacks
- Foreign espionage agents seeking to exploit information for economic, political, or military purposes
- Tactical countermeasures intended to disrupt specific weapons or command structures
- Multifaceted tactical information warfare applied in a broad orchestrated manner to disrupt a major military missions
- Large organized groups or nation-states intent on overthrowing a government

Vulnerability

An unintended aspect of a system (design, implementation, or configuration) that can cause the system to do something it shouldn't, or fail to do something it should

- E.g., buffer overflows, code injection, cross-site scripting, missing authentication or access control, misconfiguration
- National databases: CVE, NVD
- Ignoring vulnerabilities is risky
  - Too often: "no one would/could ever exploit that"
  - *Weakest link* phenomenon
- Assumptions are vulnerabilities
  - Timing, failure modes, message delivery, input format, etc.

Trust

- Trust is an essential assumption, hence vulnerability
- A trusted component is assumed to satisfy a security policy
- A trustworthy component additionally is accompanied by evidence that it satisfies the policy
  - A lot of what we study seeks to transform trust into trustworthiness
  - That is, relocating trust
  - It's a game of Whack-A-Mole

Attack

The act of causing harm by exploiting a vulnerability

- E.g, sending a well-crafted HTTP request to a server with a parsing vulnerability, which incorrectly launches a root shell in response
- E.g., calling up an employee, asking for their password, using it to login and exfiltrate information

- Real world attacks:
  - Data breaches
  - News

Ex: BISTRO CLARKSON

- New restaurant in Collegetown
- Contracts with opentable.com to make online reservations possible
- What confidentiality, integrity, and availability harms does Bistro Clarkson risk by contracting with opentable.com?
- What vulnerabilities might threats exploit to cause harm to Bistro Clarkson?

Countermeasure

A defense that protects against attacks by neutralizing either the threat or vulnerability involved

Strategy:

- Prevent: block attack or close vulnerability
- Deter: make attack harder but not impossible
- Deflect: make other targets more attractive
- Mitigate: make harm less severe
- Detect: as it happens or after the fact
- Recover: undo harm

Classes of countermeasures

- Physical: something tangible (walls, locks, guards)
- Procedural: protocols for how people act (laws, regulations, policies, contracts)
- Technical: hardware and software (cryptography, access control, passwords, intrusion detection systems, …)

Classes of technical countermeasures

- Isolation: restrict communication between components (virtual machines, sandboxes, processes, firewalls)
- Monitoring: a program analyzes execution and blocks bad things from happening (reference monitor, intrusion detection system)
- Recovery: detect and reverse effects of harm (transactions, backups, key changes)

Ex: BISTRO CLARKSON

- New restaurant in Collegetown
- Contracts with opentable.com to make online reservations possible
- What confidentiality, integrity, and availability harms does Bistro Clarkson risk by contracting with opentable.com?
- What vulnerabilities might threats exploit to cause harm to Bistro Clarkson?
- What countermeasures could be employed to control those vulnerabilities?

Beyond attacks

Attacks
are perpetrated by
threats
that inflict
harm
by exploiting
vulnerabilities
which are controlled by
countermeasures.

Upcoming events

- [Wed] A1 out; consulting hours start

"Nobody ever defended anything successfully, there is only attack and attack and attack some more."
– George S. Patton