The Economics of Cybersecurity — Lecture 7 Notes

Adam Hastings

February 27, 2024

In this class we will look at three approaches towards measuring cybercrime: One from government, one from industry, and one from academia.

- What is the relationship between cybercrime and cybersecurity?
  - Are they two sides of the same coin? (Not really—Are romance scams really a question of cybersecurity?)

(show Venn Diagram of Cybersecurity, Economics, and Cybercrime. A standard 3-dim Venn diagram!)

Activity: Have students list out some of the attacks mentioned in the papers. Ask students to define them.

Activity: Have students try to rank which attack classes they thought would be highest.

Question: Should the law enforcement community take a proportionate response to cybercrime based on the amount of harm done? Should the security community?

Question: Is anyone familiar with MITRE ATT&CK? How is this different? How is this different from the NVD/CVE system?

Activity: For each attack, list out 1) who the attack targets (individuals, enterprises), and 2) what some reasonable defenses might be.

Question: What do most of the attacks have in common? (social engineering)

Question: What do most security researchers spend their time focused on? (Finding/patching vulnerabilities, researching new attack classes)

Question: What do most of the reasonble defenses against the most common attacks have in common? (Social engineering—we can't rely on technology to save us!).

Security is a social problem with technical elements, not a technical problem with social elements! No amount of research on clever attacks and defenses is going to change this fact.

Does that mean we should give up on technical solutions? No! Many of the social engineering attacks *can* be addressed through technology. E.g. stronger authentication to verify identity (is this really my professor asking for gift cards?), or more in-browser support to detect phishing, e.g.

For example, stopping romance scams seems to fall out of the scope of cybersecurity, but maybe it shouldn't!

(I'm going to ruffle some feathers with this one) Question: Can someone define "hacking"? (Among the hacker crowd, this usually is something close to "exploiting a technological flaw to achieve some goal"). Under this definition, how are romance scams *not* considered hacking? It is exploiting a technological flaw (namely, the lack of strong identification on the Internet) to achieve the goal of scamming people for money.

This brings up a very deep philosophical question: The lack of identification on the Internet is not a bug, it's a feature in most cases. It was a deliberate decision. How can you call it a flaw? (OK I concede, I'm motte-and-baileying this one). My point is that the difference between a technological flaw and a deliberate design decision is more or less a matter of perspective. C doesn't have memory safety. Is that a feature or a bug? Depends who you ask! DRAM cells are very tiny and can be perturbed. Feature or a bug? CPUs speculate unsafely. Feature or a bug? Most web services still use passwords. Feature or a bug? It's a matter of perspective in many cases. The line between them is blurred in many cases.

Problem: The feature-or-bug decision is usually decided by vendors, who may not have security as a top priority.

Activity: For each of the defenses proposed, who ends up paying the cost?

Question: So how do we pick which party to be repsonsible for the cost? (As you can see, this really is a question of balancing costs! Doctrine papers help us here!)

FBI Cybercrime Report 2022

- What are some of the findings in the FBI report that confirmed your suspicions?
- What are some of the findings the FBI report that countered your intuitions or were surprising to you?
- How was this data collected?
- What are some of the threats to the validity of this data?

Sophos State of Ransomware 2023

- Who bothered to look up what Sophos was? Can someone explain?
- What are some of the findings in the FBI report that confirmed your suspicions?
- What are some of the findings the FBI report that countered your intuitions or were surprising to you?
- How was this data collected?
- What are some of the threats to the validity of this data?

Measuring the Changing Cost of Cybercrime

- Who bothered to look up what Sophos was? Can someone explain?
- What are some of the findings in the FBI report that confirmed your suspicions?
- What are some of the findings the FBI report that countered your intuitions or were surprising to you?
- How was this data collected?
- What are some of the threats to the validity of this data?