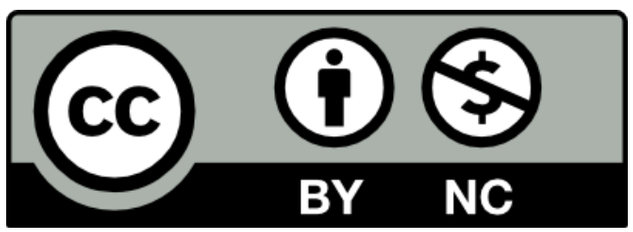
Cybersecurity:
A Systems Problem

Steven M. Bellovin
https://www.cs.columbia.edu/~smb



Protecting a Web Site

- You want to buy something online
- You enter your credit card number
- How do we protect it from being stolen from the Web?

(Photos by the author except as noted)

Security Questions

- What are you trying to protect?

- From whom?

  - Different attackers have different powers

  - They also have different goals

  - *What are you trying to protect <u>from whom</u>?*

- This is the first security question to ask

Getting the Threat Model Wrong

- What if you don't understand what the enemy wants?
- What if you get the enemy's abilities wrong?
- You'll protect the wrong thing or your defenses will be inadequate

(Photo source unknown)

Ordinary Thieves

- They want money or something easily convertible to money
  - Credit card numbers are good
  - Defense secrets are bad—they can't easily monetize them
- They know how to hack
- They don't have 007-grade skills or devices; they aren't foreign intelligence agencies!
  - *They're ordinary criminals with some technical skills*

Stealing Card Numbers in Transit

- Can the attacker monitor your conversation?
- Can they steal things in mid-flight?

Encrypt the Communication!

- Ordinary thieves can’t break encryption

- Internet encryption isn’t perfect—but again, we’re not dealing with intelligence agencies

Hack Into the Site?

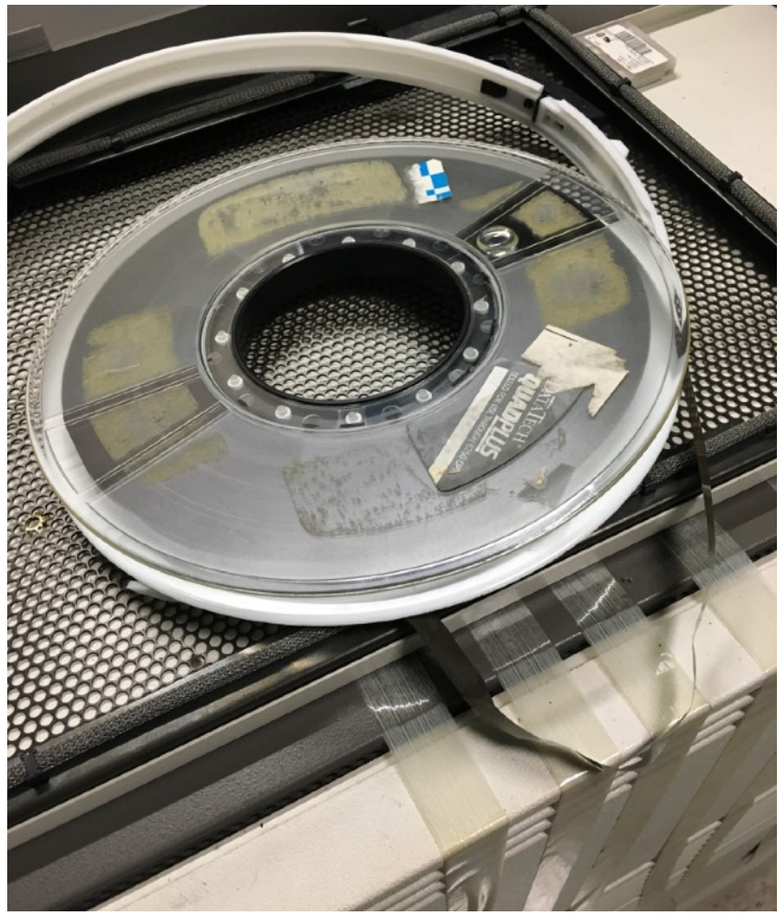
- Web sites have to have credit card numbers to bill you
- Many store them
- Can the attacker hack into a site and get your credit card number that way?

It’s Not Just a Website

- All modern web sites use databases, often on separate computers

- If the web site is programmed incorrectly, an attacker can go *through* the web server to attack the database

- One of those databases might hold your credit card number



Site Defenses

- Harden the site
- Many defenses, including firewalls

Phishing Attacks

- Can the attacker get your password?
- Guessing your password?
- “Phishing”—trick you into entering your password into a fake version of the web site

Defenses

- Strong passwords

- Two-factor authentication

Think About It

- No one defense will suffice
- You have to protect *all* parts of the system
- Defenders have to *think* about the *entire* system, and not just one or two pieces
- *Security is a systems problem*

Skills

- Cryptology, for the encryption
- Human factors, to protect against phishing
- Networking, to build firewalls
- Programming
- Many more, including system administration and operation
- *A systems perspective*

Questions?