Cybersecurity Policy & Law

Engineering Secure Software

Last Revised: November 17, 2020
“Attack is simply easier than defense. Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere.”

Ross Anderson (2001): Why Information Security is Hard; An Economic Perspective
Why Should Software Engineers Care?

● Cybersecurity and data protection policies/laws are designed to **protect assets** and serve as general **security requirements**

● Assets
  ○ Personally Identifiable Information (PII) → medical/student records, address, DOB, SSN, etc.
  ○ Classified Information

● Security Requirements
  ○ HIPAA → Medical records
  ○ FERPA → Student records
  ○ GDPR → Privacy
A Brief History

- Computer Fraud and Abuse Act (CFAA) of 1984
  - “Whoever... having knowingly accessed a computer without authorization or exceeding authorized access...”
  - Purposefully vague
  - How do you define authorization and access?
A Brief History

- Computer Fraud and Abuse Act (CFAA) of 1984
  - “Whoever... having knowingly accessed a computer without authorization or exceeding authorized access...”
  - Purposefully vague
  - How do you define authorization and access?

- United States v. Morris (1990)
  - CS grad student at Cornell → developing worm virus
  - Spread the worm by finding vulnerabilities in mail and user directory software → spread faster than expected
  - $200-$53,000 worth of damage for each infected host/network
  - Used mail/directory services in an unintended way → unauthorized access
“Morris’s conduct here falls well within the area of unauthorized access. Morris did not use either of those... features in any way related to their intended function. He did not send or read mail nor discover information about other users... he found holes in both programs that permitted him a special and unauthorized access route into other computers.”

United States v. Morris (1990)
A Brief History

- Digital Millennium and Copyright Act (DMCA) of 1996
  - Criminalizes unauthorized sharing of copyrighted material over the Internet → this is not a piracy class

- This is not a Net Neutrality class
  - Stop Online Piracy Act (SOPA) in 2011
  - PROTECT IP Act (PIPA) in 2011
  - Anti-Counterfeiting Trade Agreement (ACTA) of 2011
  - Cyber Intelligence Sharing and Protection Act (CISPA) in 2011

- This is not a philosophy class
  - WikiLeaks
  - Edward Snowden
Economics of Computer Security

- Relatively simple to determine financial loss of IP
  - e.g. if someone pirates a $20 movie, there was a $20 loss

- How do you determine the value of loss for intangible or private information?
  - e.g. reputation, availability, PII

- 750K U.S. jobs lost to intellectual property theft circa 2018
  - 9% of unemployed population

- $200-250 Billion lost annually (in the U.S.) to IP infringement
  - More than the combined loss of all movies, music, software, and video games in 2005
Economics of Computer Security

- Most metrics are terrible
  - Incomplete surveys of companies
  - Companies lying to protect their reputation

- Dean (2015)
  - Sony breach: $15-35M -- 0.9-2% of Sony’s total projected sales
  - Target breach: $105M -- 0.1% of total annual sales
  - Home Depot breach: $28M -- 0.01% of total annual sales

- *Is there a Cost to Privacy Breaches? (2006)*
  - Revenue decreases when announced, but bounces back quickly

- *NY Times (2014)*
  - Target’s profit dropped 46% compared to the previous year
Economics of Computer Security

- Cyberinsurance!
  - Yes, that’s a thing
  - Very high premiums
  - Max coverage of about $300 million

- But if the metrics are bad, how do cyberinsurance companies know what to charge you?
  - What about exploits that hit many companies simultaneously?

- Wolff (2014)
  - We need better understanding of the causes, consequences, and mitigations for vulnerabilities
Encryption Policies

  - Encryption device that secured voice and data messages
  - Had a built in back door to “allow Federal, State, and local law enforcement officials” to bypass encryption
  - Lots of vulnerabilities

- After Snowden (2013), Google and Apple said they would implement encryption on their smartphones that even they could not break
Encryption Policies

- FBI/Apple Encryption Dispute (2015/2016)
  - 2015 San Bernardino, CA terrorist attack (mass shooting, attempted bombing)
  - All Writs Act (1789): FBI ordered Apple to “use its existing capabilities to extract data” from locked iPhones
  - For iOS 8+, Apple could not possibly break the encryption with existing technology and computing resources
  - Courts ruled that the All Writs Act could not be used to compel Apple to unlock an iPhone
Consumer Protections

- Federal Trade Commission Act
  - “Unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”
  - Mostly applies to false advertising

- Google Buzz
  - “not misrepresent in any manner... the extent to which [it] maintains and protects the privacy and confidentiality...” of data
  - “obtain express affirmative consent from the ... user ... prior to any new or additional sharing ... of the ... user’s identified information with any third party”
  - “maintain a comprehensive privacy program”
  - “obtain initial and biennial assessments and reports from a qualified, objective, independent third-party professional”
Consumer Protections

- Wyndham Data Breaches
  - 2008: Hackers brute-forced admin credentials and obtained PII for 500K accounts → unencrypted
  - 2009: Hackers obtained unencrypted credit card info for 50K accounts using malware installed in the previous breach
  - FTC: Wyndham failed to use firewalls and encryption, and failed to mitigate well-known vulnerabilities
  - Because Wyndham didn’t do anything to secure their assets, they were being unlawful and were completely liable
Consumer Protections

- Terms & Conditions, End User License Agreements
  - Designed to protect the user and the company
- Information Sharing Policies
- Data Breaches
  - Notification laws (all but Alabama, South Dakota)
- Cyber Intelligence Sharing and Protection Act (CISPA) → Cybersecurity Information Sharing Act (CISA)
What is a Data Protection Policy?

- A policy and/or law that governs/protects the sharing of sensitive data
- Principles, rules, and/or guidelines that organizations must follow to protect personal information or sensitive data
  - Records management and retention
  - Acceptable use of IT systems
  - Confidentiality
  - Information security
  - Risk management
- Personally Identifiable Information (PII)
HIPAA

- HIPAA: Health Insurance Portability and Accountability Act
  - Enacted 1996 in the United States
  - Governs how PII is handled by the healthcare and insurance industries must be protected from fraud/theft

- Title II: Policies/procedures for maintaining privacy/security of PII in the healthcare industry
  - Programs for controlling fraud and abuse
  - Privacy Rule: regulates use/disclosure of Protected Health Information (PHI)
HIPAA

- Individuals must have access to their PHI
  - Provider must disclose information within 30 days of request
  - Exclusions: psychotherapy notes, information gathered to defend against a lawsuit
  - Individuals can request disclosure to a third-party

- Security Rule:
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
HIPAA Violation Examples

- Your doctor’s office does not give you a privacy notice to inform you how your PHI will be used/disclosed
- A medical agency (e.g. hospital, doctor’s office) takes more than 60 days to inform customers of a data breach
- A pharmacist shares information about his ex-boyfriend’s medical conditions
- A medical clinic hired a third-party vendor to convert X-Rays to digital form, but didn’t sign a security agreement (BAA)
- An unauthorized person gains physical access to a data center where medical records are stored
FERPA

- FERPA: Family Educational Rights and Privacy Act
  - 1974 federal law in the United States
  - Governs access to educational information/records by public entities (e.g. potential employers, foreign governments, mom)
- Gives parents access to their child’s education records (if the child is under 18)
  - Children/adults 18+ must consent to disclose education records
FERPA Violation Examples

- Your high school posts final exam grades next to your name on a bulletin board
- RIT shares your grades with your parents without consent
- RIT throws away old paper student records without shredding them
- RIT shares your transcript with Cornell without consent
- RIT shares your behavioral record with unauthorized employees (e.g. custodians, dining staff)
FERPA: The Musical

- [https://twitter.com/FERPAtheMusical](https://twitter.com/FERPAtheMusical)

*To the tune of "Let It Go" from Frozen*:
FERPA Hold, FERPA Hold,
Not in the directory anymore
FERPA Hold, FERPA Hold,
No more info to disclose
I don't care what they're going to say
Let the requests rage on
No release without consent anyway

To the tune of "Call Me Maybe" by Carly Rae Jepsen:
Hey, I just met you,
And this is crazy,
Don't share my data*,
That's kinda shady*

*Without consent or legitimate educational interest*

*To the tune of "Everything is Awesome" from Lego Movie:
Everything is FERPA.
Everything is FERPA when you're a registrar.
Everything is FERPA, unless it's GDPR.*
Outside of the United States

- GDPR: General Data Protection Regulation
  - Data protection law in the European Union (EU) and the European Economic Area (EEA)
  - Gives individuals control over their personal data
  - Requires “appropriate technical and organizational measures” to be implemented
  - Business processes dealing with personal data “must be designed and built” with safeguards to protect data
  - Data collection must be clearly disclosed and explained
  - Data breaches must be reported within 72 hours (up to €20M fine)
Takeaways

- Cybersecurity policies/laws serve as security requirements for protecting user data
- CFAA → exploiting vulnerabilities is illegal in the U.S.
- Not doing *anything* to secure your software is illegal
- Companies must disclose how they protect your data
- Your ethical responsibility as a Software Engineer is to seek out and mitigate vulnerabilities in your product