Principles of Information Security and Privacy (PISM) – CS607

MTech I - Lecture 1,2 (18 Aug 2022)

Dhiren Patel, SVNIT Surat

(Disclaimer: All due respect to Apple and Google)

Ack: Bruce Schneier (Essays)

Ref: https://www.schneier.com/essays/privacy/

CS 607 (Aug – Dec 2022)

- Course Name: Principles of Information Security and Privacy
- Course code: CS607
- Scheme: 3-0-2 (Credits 4)
- Exam scheme: 100-0-50 (total 150)
- Google Classroom code: ypir733
- Teachers: Dhiren Patel, Himanshu Patel and visiting faculty

Course Objectives

Course Objective	
1	To UNDERSTAND the basic principles of Information Security & Privacy management.
2	To UNDERSTAND the basic concepts of the technical components involved in implementing of the security & privacy.
3	To UNDERSTAND that ensuring information security & privacy in a modern organization is a problem for the management to solve and not one that the technology alone can address.
4	To ANALYZE the important economic and commercial consequences of devising security and privacy solutions in an enterprise or the lack thereof.

Syllabus

Introduction	**(04 Hours)**
Introduction to Information Security and Privacy: Review of the essential terminologies, basic concepts of security and privacy. Relation or lack thereof between the Information Security, Network Security, Systems Security and the Cyber Security. Key principles of Information Security in terms of Security mechanisms, security attributes and the security attacks. Role of National Security Systems (CNSS) and CERTIN. The McCumber Cube for Security. Introduction to the Security Systems Development Life Cycle and the difference between the Software Security and the Security Software. Classical Security Models.	
Security Threats and Security Attacks	**(02 Hours)**
Taxonomy of Security attacks. Illustrations of typical attacks. Cyber security threats. The basic terminologies viz. threats, defects, vulnerabilities, exploits, attacks, bugs.	

Syllabus

Introduction to Information Privacy	**(06 Hours)**
The importance of Data privacy; Privacy rules; Data Protection – Organization Roles. Approaches to protect sensitive data. Personally, Identifiable Information and Sensitive Data. Data Privacy and Protection Responsibilities. Consequences of Privacy Unawareness. Overview of Global Data Privacy Laws. The DSCI Privacy Framework for global privacy best practices and frameworks.	
SECURITY TECHNOLOGY – I	**(06 Hours)**
Security Mechanisms: The Symmetric and Asymmetric Key Cryptography, Ciphers: Cryptographic Algorithms and the Cryptosystems, Mechanisms for Data Integrity and Entity Authentication, Access Control mechanisms.	

Syllabus

SECURITY TECHNOLOGY – II	**(06 Hours)**
Cryptographic Tools: The Public-Key-Infrastructure (PKI), Digital Signatures, Digital Certificates, Hybrid Cryptographic Systems, Steganography. The Public Key Cryptography (PKC) limitations and looking beyond the PKC.	
Security Technology – III	**(06 Hours)**
Protocols for Secure Communications: HTTPS, TLS for Secure Internet Communication, S/MIME, PEM, PGP for Secure Email, the SET, TLS, and HTTPS for Securing Web Transactions, WEP and WPA for Secure Wireless Communications, Securing TCP/IP with IPSec PGP.	
Security Technology – IV	**(06 Hours)**
Firewalls: Processing Modes, Categorized by Generations, by Structure, Architectures, Selecting the right firewall, Configuring and Managing Firewalls. Remote Access, the concept of Virtual Private Networks.	

Syllabus

Security Technology – V	**(06 Hours)**
Intrusion Detection and Prevention Systems: Why use IDPSs, Types, IDPSs Detection Methods, IDPS Response Behaviour, IDPS Approaches. Strenghts and Limitations. Deployment and Implementation of IDPSs. Measuring the effectiveness of IDPSs. Honeypots, Honeynets and Padded Cell Systems. Network Reconnaissance: Network Scanning and Analysis.	
other topics	**(02 Hours)**

Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements Will Be Changed Every Year and Will Be Notified on Website.)	**(28 Hours)**
(Total Contact Time: 42 Hours + 28 Hours = 70 Hours)	

Course Outcomes

Course Outcomes **At the end of the course, students will be able to**	
CO1	Examine and apply the fundamental techniques of computer security.
CO2	Examine and apply and identify potential security issues and the associated risks.
CO3	Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society.
CO4	Demonstrate foundation knowledge of information security/assurance within the organization.
CO5	Plan for the future and design a solution based on user requirements. Explain business continuity, backup and disaster recovery. Understand troubleshooting and quality consumer support.

Security (of Digital data/asset/account)

- a key—or an account, or anything similar—can be in one of four states:
- **safe** Only the user has access,
  loss No one has access,
  leak Both the user and the adversary have access, or
  theft Only the adversary has access
- Once you know these states, you can assign probabilities of transitioning from one state to another (someone hacks your account and locks you out, you forgot your own password, etc.) and then build optimal security and reliability to deal with it.

Cost of Security

- Money to buy Program/Tool
- Computing (and Network connectivity) to run it all time
- Safe Memory to house it
- Human resources to configure, monitor, revoke
- Self health check (Resilience)
- Criticality of data (and value it protect) on which we are applying Security controls

Privacy
Looking back: Q and 3A (2006)

Q: “If you aren’t doing anything wrong, what do you have to hide?”

1. “If I’m not doing anything wrong, then you have no cause to watch me.”
2. “Because the government gets to define what’s wrong, and they keep changing the definition.”
3. “Because you might do something wrong with my information.”

Privacy

- privacy is about hiding a wrong. It’s not.
- Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect.

Two proverbs and Importance of Privacy

- “Who watches the watchers?”
- “Absolute power corrupts absolutely.”
- Watch someone long enough, and you’ll find something to arrest—or just blackmail—with.
- Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political enemies
- Privacy protects us from abuses by those in power, even if we’re doing nothing wrong at the time of surveillance.

Privacy Concerns

- We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need.
- You watch convicted criminals, not free citizens.
- if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness.
- We lose our individuality, because everything we do is observable and recordable.

Why?

- “security versus privacy?”
- The real choice is liberty versus control
- Liberty requires security without intrusion, security plus privacy.
- And that’s why we should champion privacy even when we have nothing to hide!!

Security by Design, Privacy by Design

- a framework to proactively (“by design”) integrate privacy principles into the design of software, hardware, networks, and business practices
- two National Institute of Standards and Technology (NIST) frameworks: Cybersecurity Framework (CSF) and Privacy Framework

Stalkerware

- for many years, both the Google and Apple mobile app stores routinely approved “stalkerware” apps.
- These are apps that are used to covertly surveil device owners, tracking their location and communications.
- Stalkerware is not benign or secure. Rather, it is widely implicated in domestic violence and intimate partner abuse.
- (Eventually, due to unrelenting pressure from organizations like the Electronic Frontier Foundation, the dominant platforms instituted a policy banning stalkerware, but not before many of their customers were placed in harm’s way by the platforms’ poor judgment)

Moving forward

- VPNs are a key tool to help users evade surveillance and censorship by oppressive governments.
- Jailbroken phones allow more than just unsanctioned apps to be installed; they can also harbor spyware without their owner's knowledge.
- Jailbreak detection is a useful function for people who have purchased a used phone, or who may be victimized by someone close to them.
- (But Apple determined that this security app was against its App Store terms of service, depriving at-risk users of a valuable layer of protection.)

(2022)

- US Senate Bills (S.2992 and S.2710) - attempt to redress the power of dominant technology firms
- S.2992 bars large tech companies from unfairly preferencing their own products on platforms they own or control.
- S.2710 prohibits forcing app developers to use a specific in-app payment system owned or controlled by the owner of the app store.

Background

- Both Apple and Google have approved apps that egregiously violate user privacy and security, often in direct contradiction to their own policies
- The incredible volume these marketplaces handle (Apple's App Store receives 100,000 submissions per week) means that they cannot possibly vet every single app as thoroughly as desired.
- Furthermore, app store review processes frequently bar apps that would meaningfully improve user privacy and security. For example, Google's Play Store policies prevent the development of ad- and tracker-blocking software
- A smaller, alternative app store could set its own policies that are stronger and better enforced than a large platform is capable of.

Introspection

- these platforms have chosen profits over their user's security and privacy
- We cannot, and should not, trust a single company to make the correct decisions about device security, privacy, and integrity for billions of users

More (S.2992 and S.2710)

- App store monopolies cannot protect users from every risk, and they frequently prevent the distribution of important tools that actually enhance security.
- Furthermore, the alleged risks of third-party app stores and “side-loading” apps pale in comparison to their benefits. These bills will encourage competition, prevent monopolist extortion, and guarantee users a new right to digital self-determination.

Concern(s) by Apple Inc. - S.2992

- Apple: S.2992 would erect “steep obstacles” in front of new privacy and security protections
- Actually - the bill only prohibits “unfairly preferencing” a platform’s products or services or “unfairly limiting” another business relative to the platform
- The bill does not prohibit changes that affect all apps, such as Apple’s App Tracking Transparency framework, which limits every app’s access to personal information until a user has granted their informed consent.
- Any future changes that a platform makes to enhance privacy and security will still be permitted, as long as those changes are applied fairly to the platform’s own products and services as well as to third parties.

Concern(s) by Apple Inc. - S.2710

- Apple attacks S.2710's interoperability requirements, claiming that its requirement to allow "side-loading" of apps will likely lead to "millions" of new malware attacks
- It also claims that this requirement prevents users from "choosing" a secure and private device.
- First, nothing in S.2710 requires Apple or anyone else to open its devices to side-loading. (Sideloading refers to the installation of apps that have not been verified by any app store.)
- interoperability does not require one-click installation of random apps from the Internet, only that companies relinquish their monopoly control over app stores.
- Alternative stores could have the same, or even more, security restrictions than Apple. And instead of one app store controlled by Apple, users would be able to choose between many.

Concern(s) by Apple Inc. - S.2710

- Second, Apple's reasoning regarding side-loading is self-interested, oversimplified, and dishonest.
- Side-loading is not a means for bad actors to vault over a platform's secure walls and into user's private lives; it's a way for users to exercise agency over their own devices.
- Sideloaded apps bypass the app store moderation process, but moderation is not the only level of protection between users and malware.
- Sophisticated malware often relies on technical exploit to get around operating system-level restrictions on its behavior, and side-loading wouldn't affect Apple's ability to restrict what rogue apps are capable of doing.

Users' Rights

- Our devices are our own, and interoperability will allow us to use them as we choose.
- Any user who prefers to use only Apple-approved applications will have no trouble doing so.
- But S.2710 will finally give users the freedom to leave the walled garden: to build, share, and install software that hasn't been approved by Apple's moderation machine.
- Allowing alternative app stores—and allowing users to choose different moderators—is the only way to ensure users can configure their devices securely.

Concluding Remark

- Out in the real world, we give people the freedom to choose their own level of risk.
- It might be objectively true that Disneyland is safer than a public park, but that doesn't mean we should outlaw all public parks and give Disney a monopoly on park-like gathering places.
- People are free to visit Disneyland, and pay for the privilege.
- They are free to visit other companies' commercial parks. And they are free to visit any of our nation's public parks.

Concluding Remark (cont.)

- Yes, there is malware. Yes there are attacks.
- But there is security and safety as well.
- Hundreds of companies innovate in this space, developing new security and privacy technologies that we are free to install if we choose.
- Our laptops are like public parks, that we can arrange with whatever amenities and safeguards we choose.
- **There is no reason our phones should not be as well.**

Welcome to PISP 2022

- Revised Syllabus based on Course outcomes
- Principles of Information Security
- (Classical and Modern Cryptography)
- Principles of Information Privacy
- Attacks, Risk, Cost and Management
- Applied Security and Privacy requirements
- Technology v/s Systems – Real world use cases
- <e.g. IIT Madras attendance system – Technology works, System does not!!(Ack. Prof S V Raghvan)>