

F1: security intro

tkkwon@snu.ac.kr

A quote

“Every program has at least two purposes: the one for which it was written, and another for which it wasn't.”

-Alan J. Perlis

SECURITY OVERVIEW

Security may mean different things

- Emotional security
 - Physical security
 - Resource exhaustion
 - System security
 - Network security
 - Cryptography (or cryptology)
 - Social engineering
 - E.g. email prankster
- security vs privacy
 - vulnerability

two categories in IT Security

- Computer (or system) Security
 - automated tools and mechanisms to protect **data in a computer**, even if the computers are connected to a network
 - against hackers (intrusion), malware, ...
 - Access control, authorization, ...
- Internet (or network) Security
 - measures to prevent, detect, and correct security violations that involve the **transmission of information** in a network
 - assumptions
 - Everything on the network can be a target
 - Every transmitted bit can be tapped

* The boundary is blurry

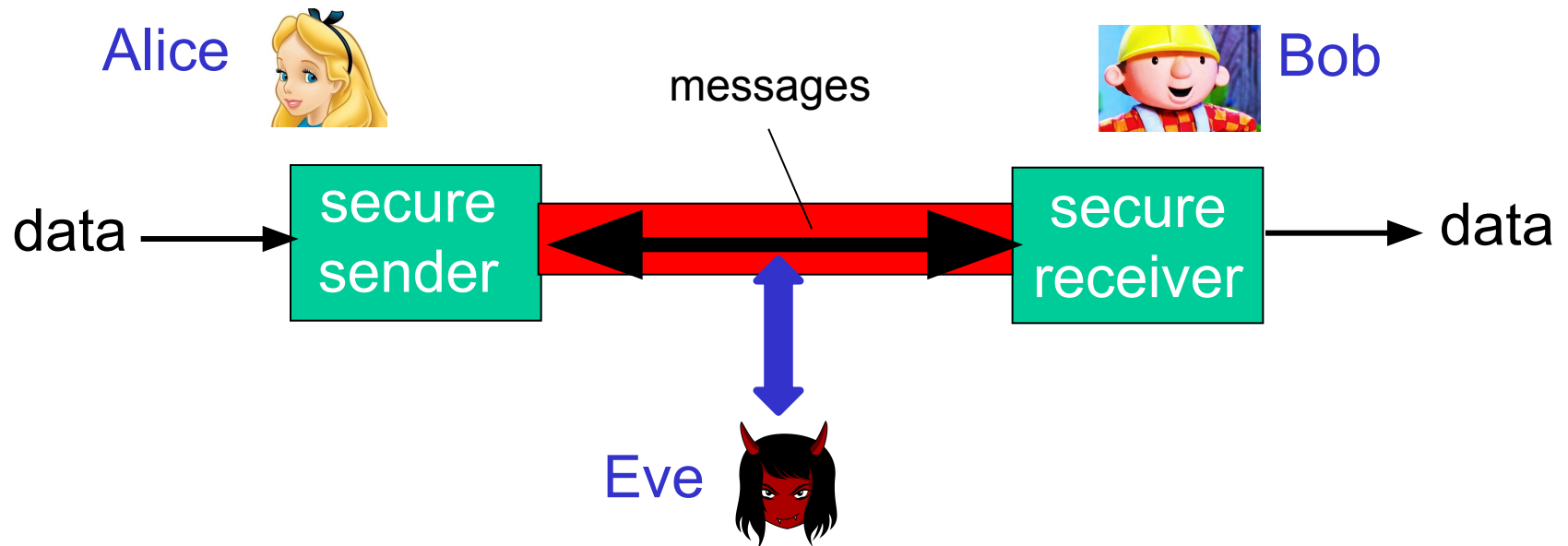
How to model network security?

- Who are the interest parties?
- What do they want to do?



Friends and enemies: Alice, Bob, Eve

- well-known in network security world
- Bob, Alice want to communicate “securely”
- Eve (intruder) may tap, delete, add, modify messages



* Eve, Mallory, Oscar

There are attackers out there!

What can Eve do?

- *tap/eavesdrop/snoop* messages
- *Insert/modify/delete/replay* messages
- *poisoning* data
- *impersonation/masquerade*: pretend to be someone else
- ...
- more attacks coming

ATTACKS

Computer/network attacks (1/3)

- malware
 - Virus
 - Worm
 - Trojan (horse)
 - Spyware
 - Ransomware
- Bot
 - Automate tasks
- Buffer overflow
 - Stack buffer overflow
 - Heap overflow

```
#include <string.h>
void foo (char *bar) {
    char c[12];
    strcpy(c, bar); // no bound checking
}
int main (int argc, char **argv) {
    foo(argv[1]);
    return 0;
}
```

Computer/network attacks (2/3)

- Denial of service (DoS)
 - a single host
 - Distributed DoS: numerous hosts
 - DDoS-as-a-service
- Network-based attacks (upcoming)
- Physical attacks
 - Van Eck
 - Energy weapon
 - E.g. Electromagnetic (EM) wave



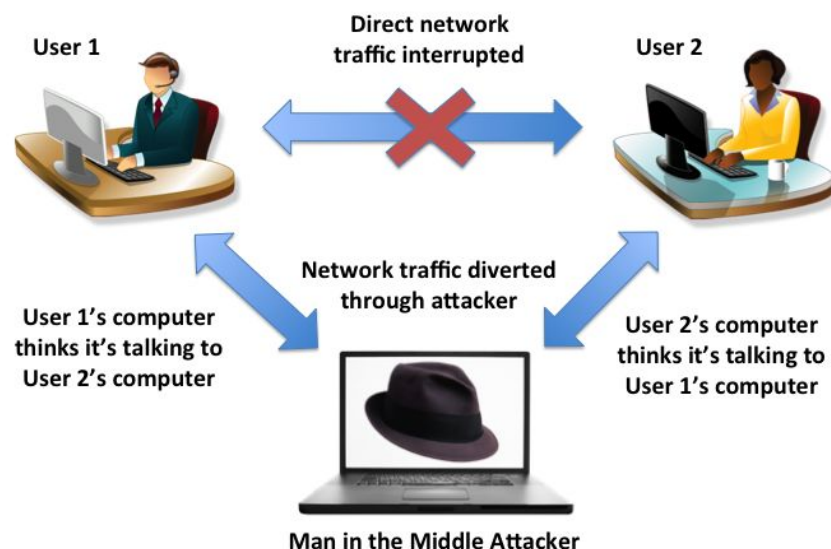
Computer/network attacks (3/3)

- Password attacks
 - Password guessing/dictionary attack
 - Brute force
- Information gathering attacks
 - Phone, web, SNS,...
 - Phishing with cloned website
 - via links in email, online ad,...
 - Security scanning
- Side channel attacks
 - Timing/power analysis
 - EM wave
 - Data remanence
 - e.g. degaussing

Phishing vs pharming (fraud) (DNS)
--

Network-based attacks!

- cryptographic attacks
 - E.g. find the key, ciphertext to plaintext
- Spoofing
 - ARP, DNS,...
 - Cache poisoning
- Session hijacking
- Impersonation
- Man-in-the-middle
- ...
- network domain-specific
 - Internet, Wireless, Web, Mobile, IoT,...



source: Gary Chao and Bryant Khau@UCLA

passive attacks



- (wire)tapping/eavesdropping
 - cf. lawful interception
- port scanner
 - idle scan: secretly scanning

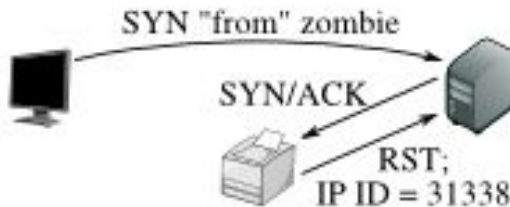
IP IDs are now randomized

Step 1: Probe the zombie's IP ID.



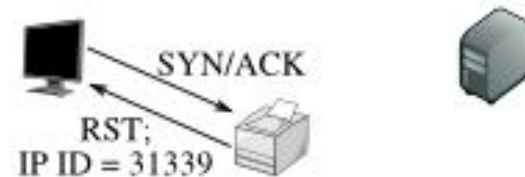
The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.



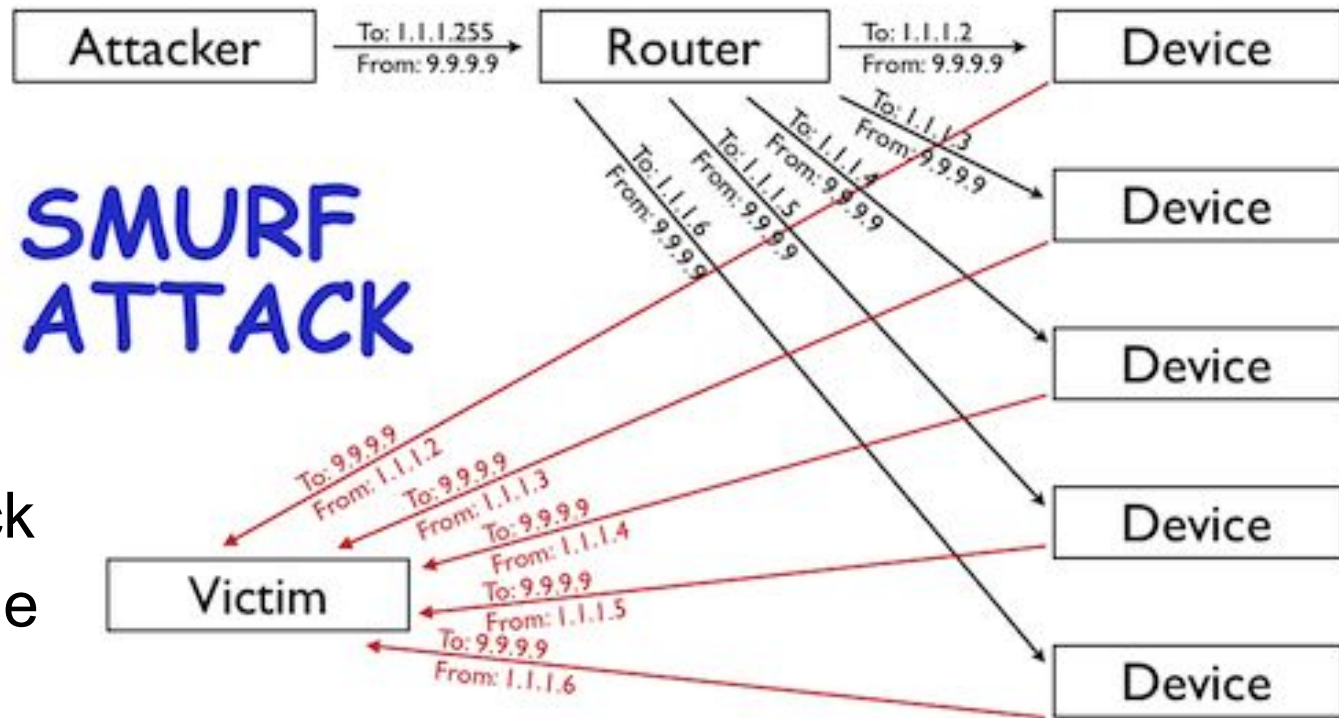
The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.



The zombie's IP ID has increased by 2 since step 1, so the port is open!

active attacks



- DoS/DDoS attack
- Man in the middle
- poisoning
 - DNS, ARP,...
- Smurf attack
 - ICMP: src addr: spoofed addr., dest addr: IP broadcast addr.
- system attacks
 - virus propagation, SQL injection,...

src: source
dest: destination
addr: address

SECURITY SERVICES AND MECHANISMS

what kind of security services user want?

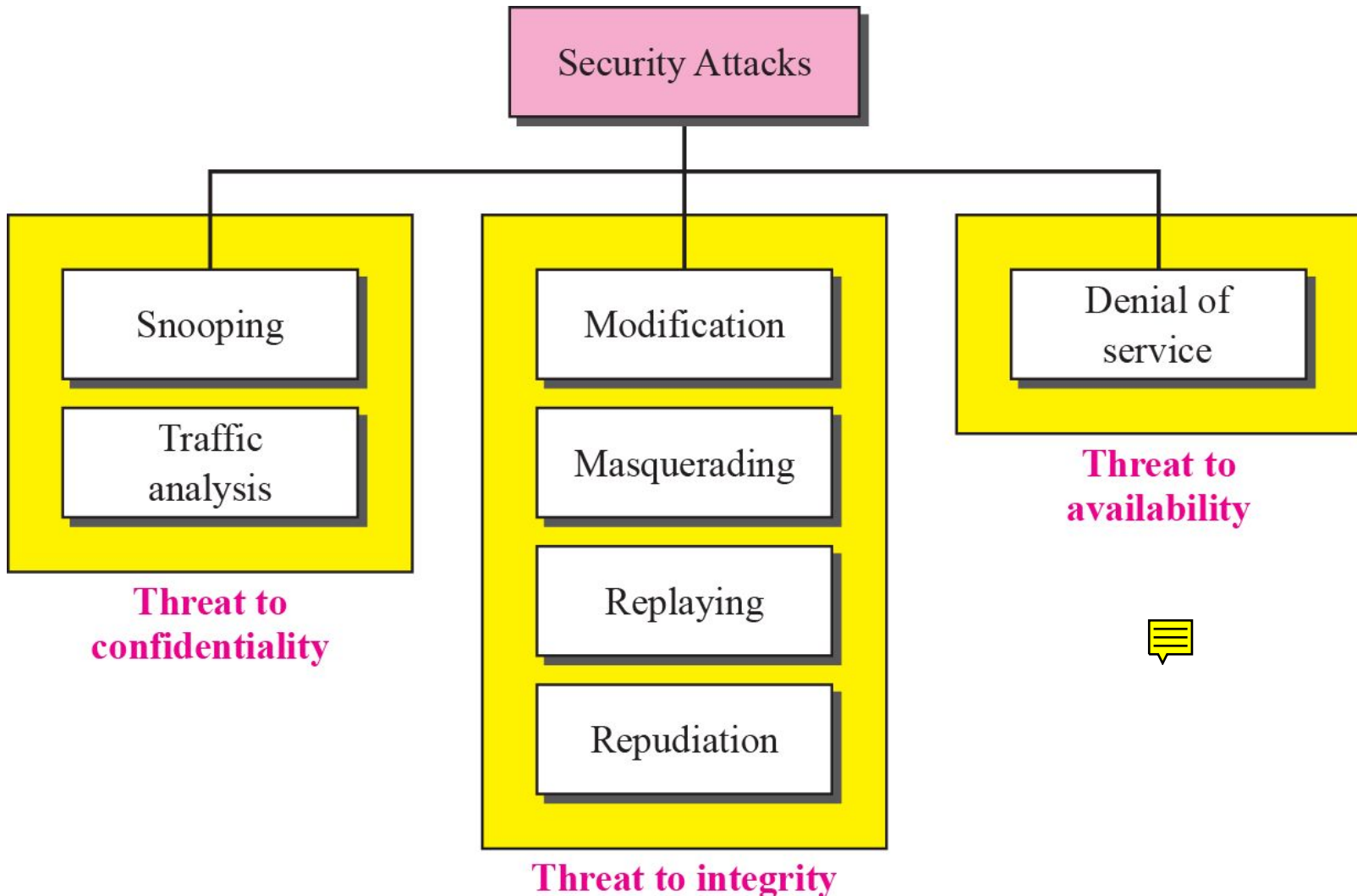
- Basic Network Security services

- **C**onfidentiality
- **I**ntegrity
 - Data (or message) integrity
- **A**vailability
- authentication
- Non-repudiation



source: Anthony Henderson@panmore.com

attacks against CIA



More Security services

- Access control
 - identification
 - authentication
 - authorization
- Anonymity
- Accountability
- security audit
- Privacy
- digital forensics


Security mechanisms

- cryptography
 - Encryption and decryption
 - Keys
 - Key distribution/management
- credential
- Message digest
 - Hash function
 - Input: message
 - Output: message digest (fixed length)
 - message authentication code (MAC)
- traffic padding
- Digital Signatures
 - the authenticity of a digital message or document
- trusted third party (TTP)
 - e.g. notarization
- append-only server, blockchain

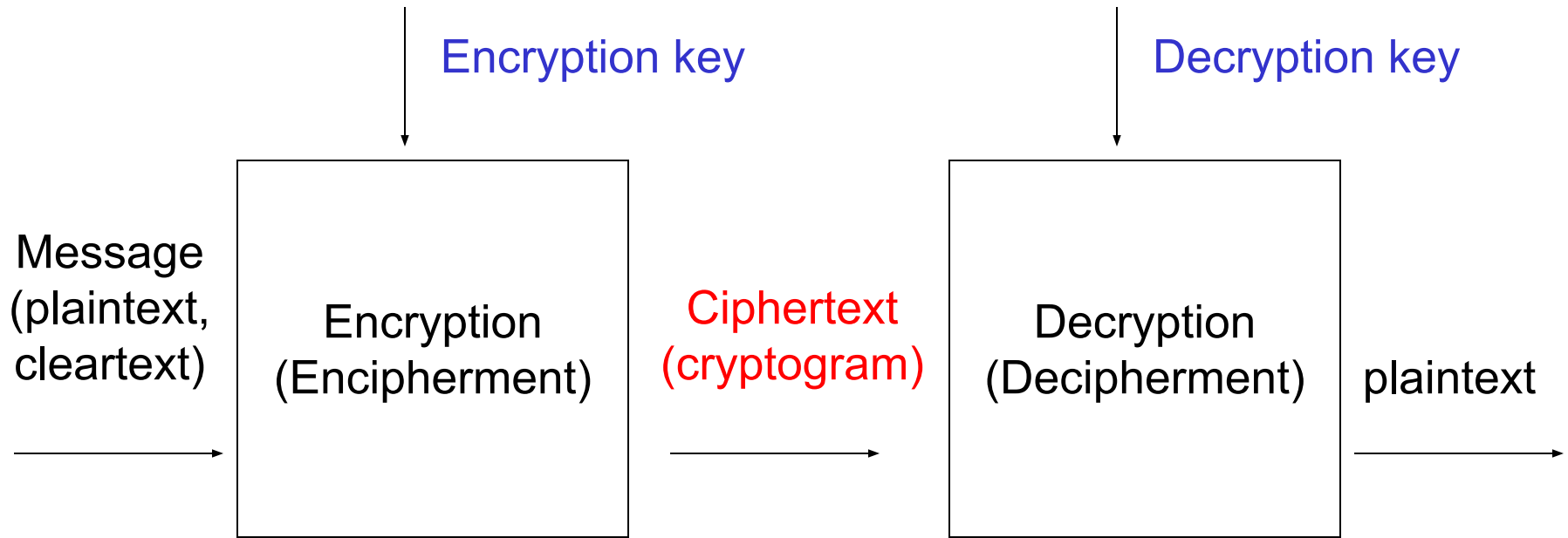


CRYPTOGRAPHY

Meaning of Cryptography

- from Greek
 - Cryptos: secret, hidden
 - graphos: writing
 - cryptography: study of secret writing
- Related words 
 - Cryptology \approx cryptography
 - Cryptanalysis
 - the study of methods for obtaining the meaning of encrypted information without access to the key
 - Steganography
 - the hiding of a secret message within an ordinary message

Basics of a cryptosystem



cipher - algorithm for performing encryption or decryption

key - info used in cipher known only to sender/receiver

encipher (encrypt) - converting plaintext to ciphertext

decipher (decrypt) - recovering ciphertext from plaintext

cryptography - study of encryption principles/methods

cryptanalysis (codebreaking) - the study of principles/methods of deciphering ciphertext *without* knowing key

Classification of Cryptosystems

- The way in which keys are used
 - Symmetric cryptography
 - Single key
 - Public key cryptography
 - Two different keys
- the way in which plaintext is processed
 - Block cipher
 - Stream cipher

Kerckhoffs's Principle

- two choices for security of a cryptosystem
 - the encryption/decryption algorithm can be hidden
 - security by/through obscurity
 - the key can be hidden
- A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

THREAT MODELING

Threat Modeling

Threat modeling is the process of systematically identifying the threats faced by a system

1. Identify things of value that you want to protect
2. Enumerate the attack surfaces
3. Hypothesize attackers and map them to
 - Things of value they want from (1)
 - Their ability to target vulnerable surfaces from (2)
4. Survey mitigations
5. Balance costs versus risks

Let's walk through a case of a smartphone!

Identify Things of Value

- Saved credentials (e.g. passwords)
- Personally identifiable information (PII)
- Address Book
- Access to sensors (camera, mic,...), network traffic, or location
- Credit card data (e.g. saved in the browser)
- Access to bank accounts, paypal,...
- Pics, messages, browsing/search history
- Sensitive documents
- The device itself



Enumerate Attack Surface

- Steal the device and use it
- Direct connection via USB
- Close proximity radios (Bluetooth, NFC)
- Trick the user into installing malicious app(s)
- Passive eavesdropping on the network
- Active network attacks (e.g. man-in-the-middle, SMS of death)
- Backdoor the OS (Google)
- Backdoor the handset (e.g. OnePlus EngineeringMode)

Hypothetical Attackers

Attacker	Capabilities	Goals
Thief	Steal the phone Connect to USB or over networks Disconnect the phone from the internet	The device itself Access to data No tracking
FBI	Everything the thief can do Legally compel you to do things Infect you with surveillance malware	Evidence from the device (pics, msgs, GPS logs)
Eavesdropper	Passively observe network traffic	Steal PII, passwords, bank account numbers, etc.

Mitigating Thief

Mitigation

Strong authentication

- Strong password
- Biometrics

Full device encryption

Remote tracking and wiping

Issues?

- Annoying to enter

- Won't work if the thief disconnects from the internet

Mitigating FBI

Mitigation

Issues?

Strong authentication

- Strong password
- Biometrics

- Annoying to enter
- FBI can compel you to unlock

Full device encryption

Remote tracking and wiping

- Will get you thrown in prison for obstruction

Patch the OS and apps

- Manufacturers are slow to patch

Avoid phishing attacks

- Requires vigilance

Don't use any cloud services

- Prevents you from using most modern apps

Mitigating Eavesdropper

Mitigation

Use HTTPS everywhere

Use a Virtual Private Network (VPN)

Issues?

- Unclear which apps use HTTPS
- No way to force HTTPS

- Warning: free VPNs may be scams!
- May slow your connection

Balancing Cost and Risk

- Assess the likelihood of different attacks
 - Purely subjective, will change based on context
- Compare to the cost of mitigations
 - Sometimes, the risk/reward tradeoff is quite poor

Attacker	Likelihood?	Cost of Countermeasures
Thief	High	Low (biometric login is okay)
FBI	Low	High (no biometrics or cloud services)
Eavesdropper	Moderate	Medium (good VPNs are not free)