CY 2550 Foundations of Cybersecurity

Threat Modeling

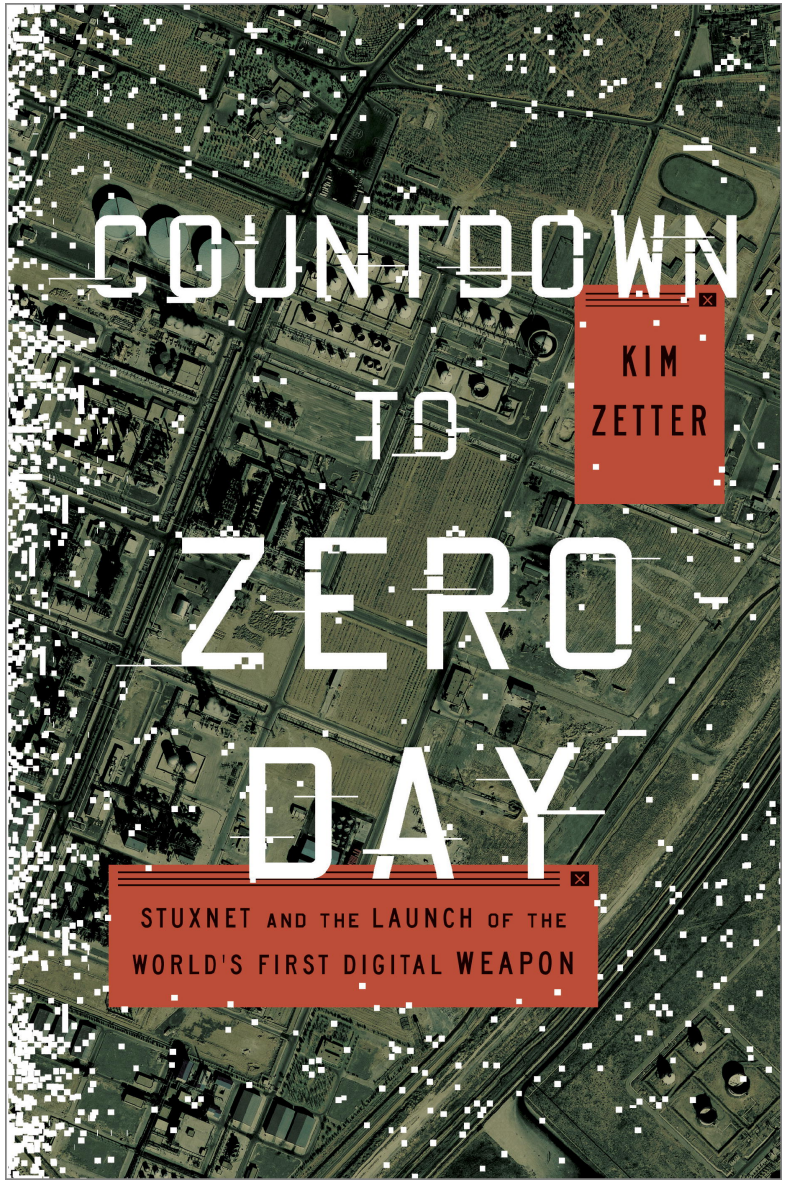
Alina Oprea
Associate Professor, Khoury College
Northeastern University

Online Resources

- Class website: http://www.ccs.neu.edu/home/alina/classes/Spring2020
- Class forum is on Piazza
  - Sign up today!
  - Install their iPhone/Android app
  - www.piazza.com/northeastern/spring2020/cy2550
- When in doubt, post to Piazza
  - Piazza is preferable to email
  - Use #hashtags (#lecture2, #project3, etc.)

Books

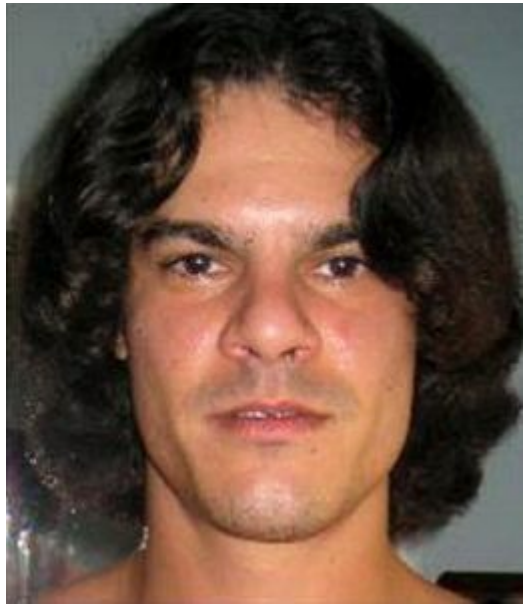
- Textbook available online:
  - Computer Security and the Internet: Tools and Jewels by Paul C. van Oorschot, 2019
  - https://people.scs.carleton.ca/~paulv/toolsjewels.html
  - Chapter 1 for Introduction
- One required reading:
  - Countdown to Zero Day by Kim Zetter
  - Stuxnet attack



Havoc on the Internet

- 1999 – Melissa macro virus spreads via email attachments
- 2000 – ILOVEYOU virus released, infects millions of machines in hours
  - One of the first widespread uses of social engineering tactics
- 2000 – 15-year old “mafiaboy” invents the Denial of Service attack
  - Causes millions of damage to e-commerce websites
  - Yahoo becomes unavailable for an hour
- 2001 – Code Red worm spreads via Microsoft IIS exploit
- 2003 – SQL Slammer and Blaster spread exponentially via exploits in Microsoft products

The Modern Criminal

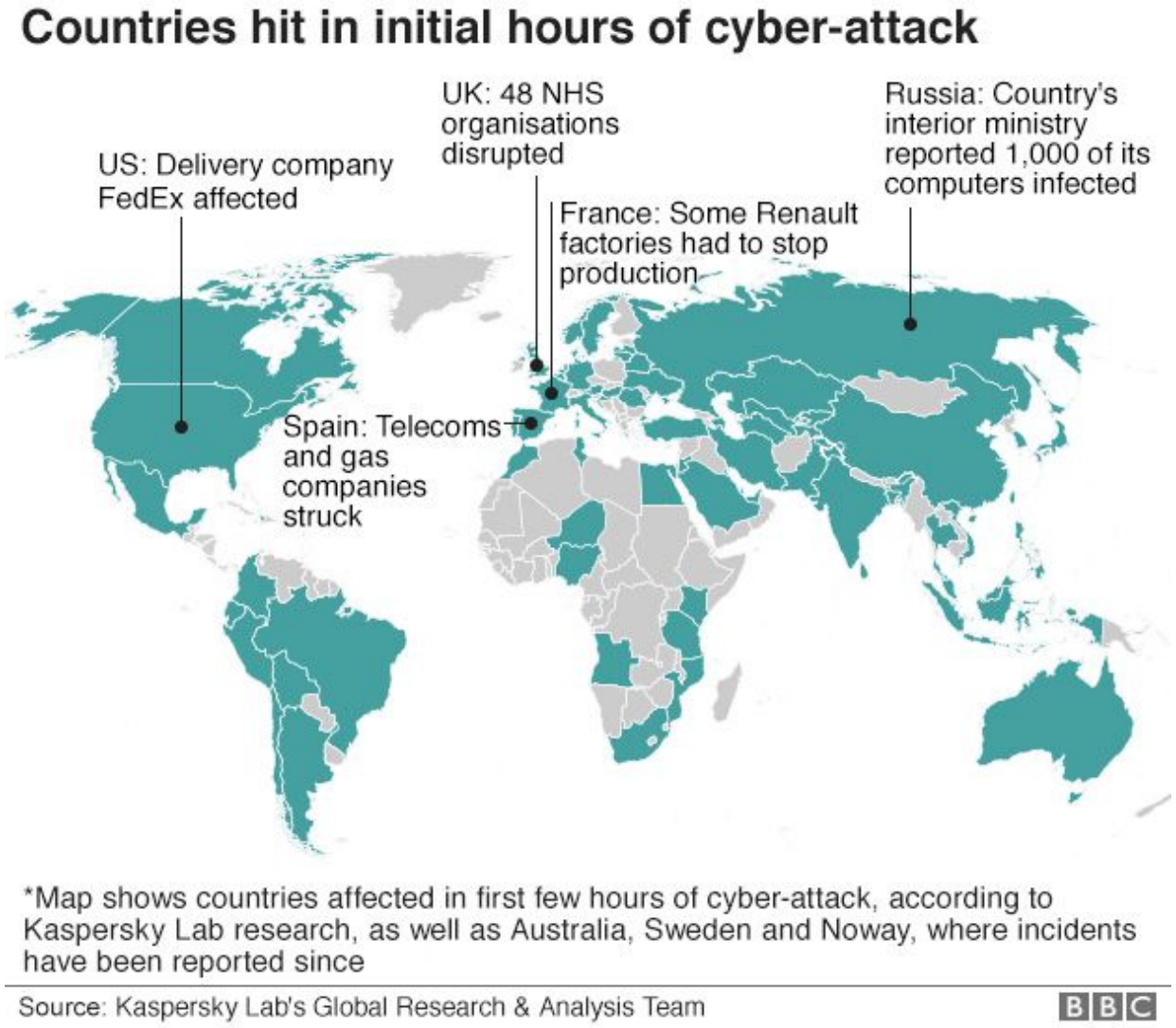


- 2005 – Albert Gonzalez steals 46 million credit cards from TJ Maxx
- 2006 – The Russian Business Network (RBN) comes online
  - Offered bulletproof hosting for criminal enterprises
- 2007 – Storm worm turns infected machines into a botnet
- 2007 – First version of Zeus banking trojan released

Cyberwarfare: Advanced Persistent Threats (APTs)

- 2009 – Chinese hackers from PLA Unit 61398 perform “Operation Aurora”
  - Serious of hacks against US government and industry targets
  - Google was targeted
- 2010 – US and Israel attack nuclear centrifuges in Iran with the Stuxnet worm
  - Designed to jump over air-gapped networks
  - Causes centrifuges to spin out of control, but report no anomalies
  - To this day, parts of the code are undeciphered
- 2011 - RSA attack, part of an espionage group uncovered by the Mandiant APT 1 report: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
- 2014 – “Guardians of Peace” attack Sony Pictures
  - Destroy computers, leak confidential files and unreleased movies
  - Believed to be North Korean hackers

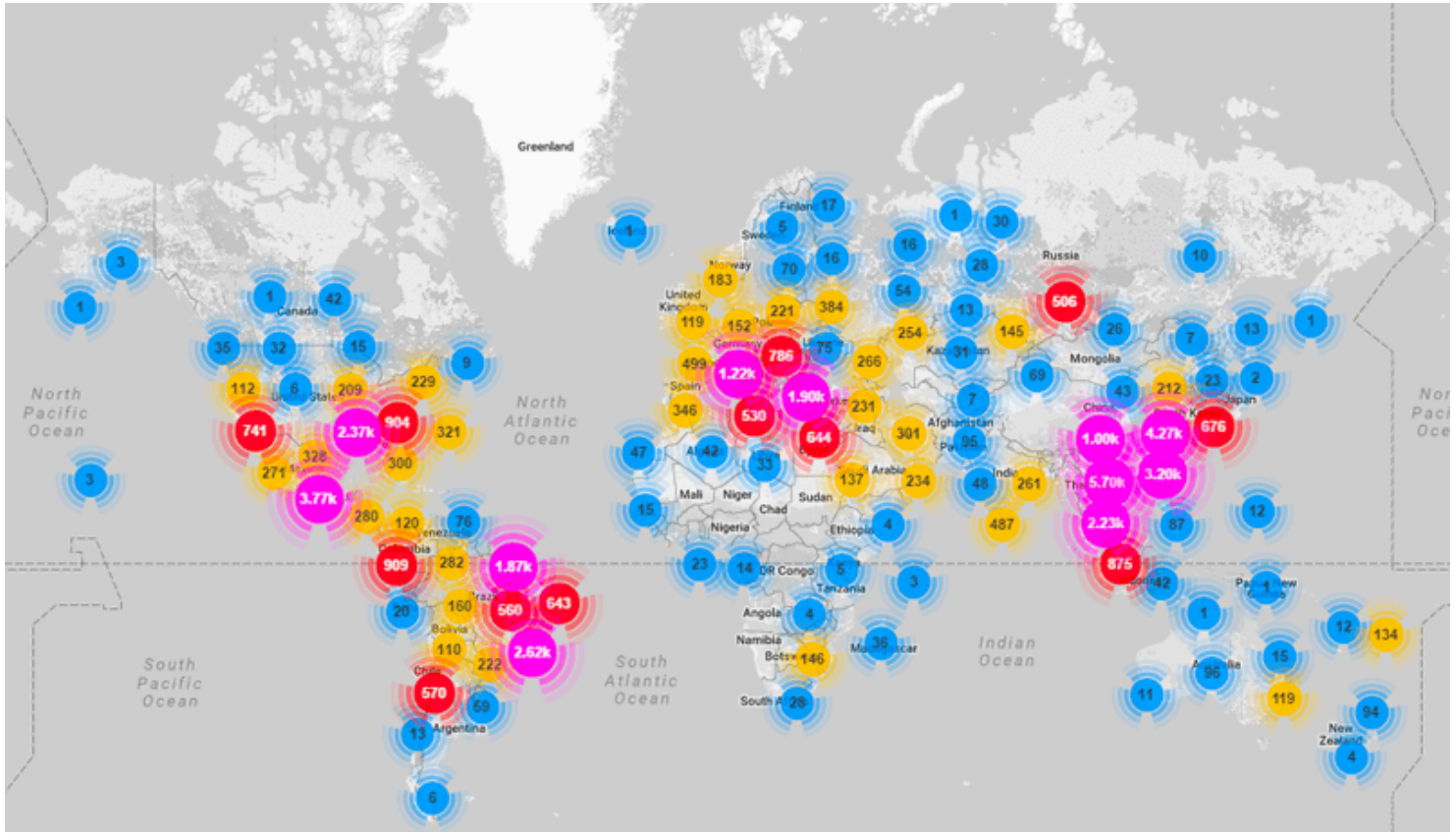
Self-Propagating Ransomware



WannaCry ransomware

- 200K infected machines
- 150 countries
- May 12- May 15, 2017

Mirai botnet



- First massive botnet using IoT devices
- Exploits weak authentication in IoT
- Majority of devices: routers, cameras
- Launched DDoS attacks against Krebs on security
- Follow up attack on Deutsche Telekom
- Peak of 600K infections

Antonakakis et al. Understanding the Mirai Botnet. In USENIX Security 2017

The Future?

- Automated attacks carried out by adversarial AIs
- Remote and deadly hacks of robots and autonomous cars
- Cryptocurrency anarchy
- Widespread social engineering via targeted propaganda
- Actual warfare in cyberspace
- Complete loss of individual privacy

… Training more security experts could prevent these!

Outline

- Chapter 1 of textbook
- Threat modeling
  - Examples: secure your phone
  - Adversarial models
- Types of threat modeling
  - Diagram based
  - Attack-tree based
  - Why modeling threats is hard
- Linux introduction
- Project 0 is released!

Securing Your Phone

- Add a password or passcode
- Add biometric authentication (fingerprint, voice, or face)
- Install an antivirus app
- Encrypt the device
- Subscribe to a Virtual Private Network (VPN) service
- Fork the Linux kernel and develop your own version of Android from scratch

If you do all this, is your phone secure?

From whom?

Ad hoc Security Rarely Succeeds

- Have you considered all possible attackers?
  - What do they want?
  - Why do they want it?
  - How hard are they willing to work to get it?
- Have you considered all possible attack surfaces?
  - Is the network secure?
  - Is the OS secure?
  - Is the hardware secure?
  - Are **you** secure?
- Have you weighed the tradeoffs of mitigations?
  - How much do they cost?
  - Do they introduce alternative forms of risk?
  - How much burden do they place on users?

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

Identify Things of Value

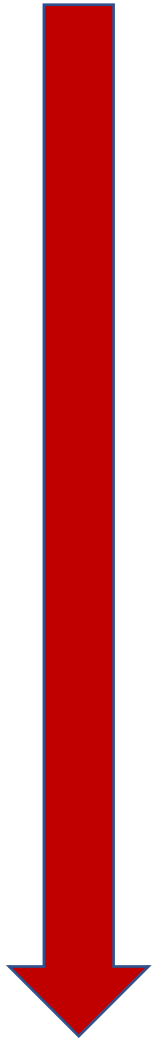
- Saved passwords
- Personally identifiable information (PII)
- Address Book
- Access to sensors (camera, mic, GPS) or network traffic (for surveillance)
- Credit card data (e.g. saved in the browser)
- Access to bank accounts, paypal, venmo, or other financial services
- Pics, messages, browsing/search history (for blackmail)
- Sensitive business documents
- Monetizable credentials (webmail, social networks)
- 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 (e.g., Android)
- Backdoor the handset (hw-level attacks)
- Intercept and compromise the handset in transit

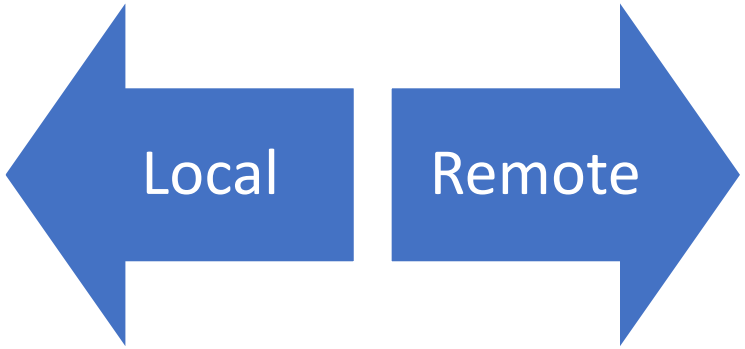


Stronger Attacker

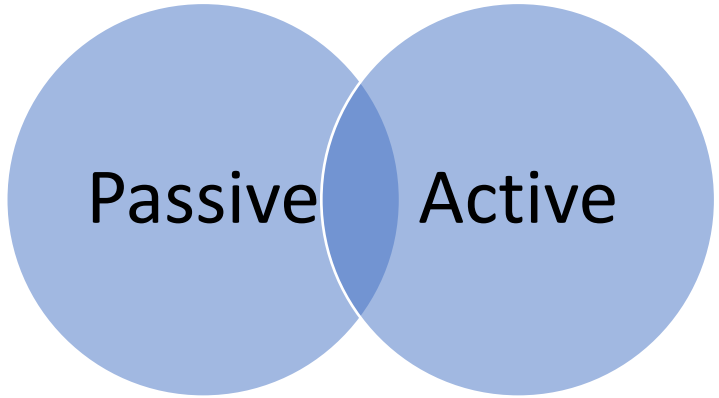
Key Factors for Attacks

When?

Where?



How?



Hypothetical Attackers

Attacker	Capabilities	Goals
The Thief	Steal the phone Connect to USB or networks Disconnect the phone from the internet	The device itself Access to financial services
Law enforcement	Everything the thief can do Legally compel you to do things	Evidence from the device (pics, msgs, GPS logs)
The Eavesdropper	Passively observe network traffic	Steal PII, passwords, bank account numbers, etc.
Active Attacker	Passively observe network traffic Active network attacks	Surveillance

Mitigating The Thief

Mitigation	Issues?
Strong authentication • Strong password • Biometrics	• Annoying to enter • Cannot be revoked if compromised
Full device encryption	• What if you loose the key?
Remote tracking and wiping	• Won't work if the thief disconnects from the internet

Find My Device

by Google Play Protect

Hypothetical Attackers

Attacker	Capabilities	Goals
Law Enforcement	Everything the thief can do Legally compel you to do things	Evidence from the device (pics, msgs, GPS logs)

Mitigating Law Enforcement

Mitigation	Issues?
Strong authentication • Strong password • Biometrics	• Annoying to enter • FBI can compel you to unlock
Full device encryption	
Patch the OS and apps • Use a Nexus/Pixel	• Manufactures are slow to patch
Avoid phishing attacks	• Requires vigilance
Don’t use any cloud services	• Prevents you from using most modern apps

Hypothetical Attackers

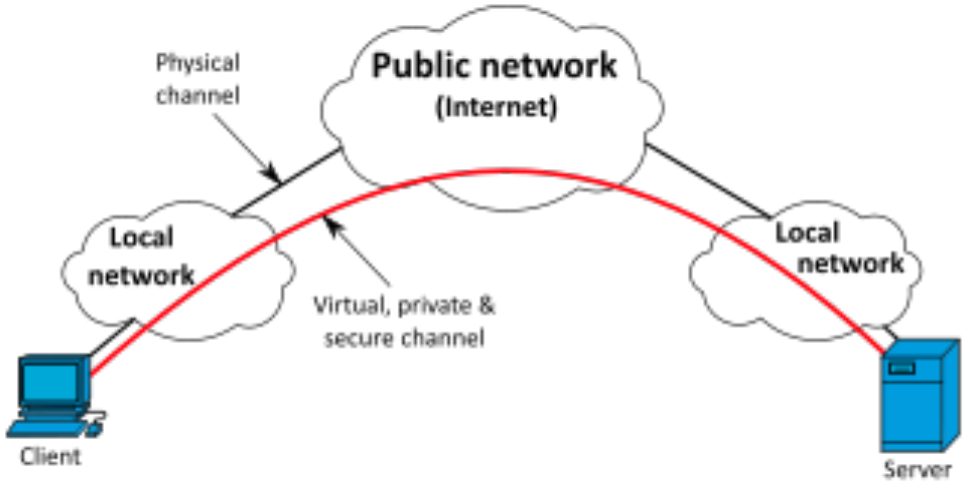
Attacker	Capabilities	Goals
The Eavesdropper	Passively observe network traffic	Steal PII, passwords, bank account numbers, etc.

Mitigating The Eavesdropper

Mitigation	Issues?
Strong authentication • Strong password	• Annoying to enter
Full device encryption	
Patch the OS and apps • Use a Nexus/Pixel	• Manufactures are slow to patch
Avoid phishing attacks	• Requires vigilance

Mitigating The Eavesdropper

Mitigation	Issues?
~~Use HTTPS everywhere~~	• Unclear which apps use HTTPS • No way to force HTTPS
Use a Virtual Private Network (VPN)	• Warning: free VPNs are scams! • May slow your connection



Hypothetical Attackers

Attacker	Capabilities	Goals
Active Attackers	Passively observe network traffic Active network attacks	Surveillance

Mitigating The Active Attacker

Mitigation	Issues?
Use a Virtual Private Network (VPN)	• Warning: free VPNs are scams! • May slow your connection • Does not provide anonymity
Use Tor	• Very slow connection
Patch the OS and apps	
Disable JavaScript & plugins in web browser	• Some websites will break
No cloud services	

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
The Thief	High	Low (biometric login is okay)
Law Enforcement	Low	High (no biometrics or cloud services)
The Eavesdropper	Moderate	Medium (good VPNs are not free)
Active Attacker	Low	High (slow internet, no cloud, broken web)

Threat Modeling

- Identifies threats, threat agents, and attack vectors that the target system considers in scope to defend against
- Consider adversarial models with different objectives, methods, capabilities
- Consider all assumptions made about the target system, environment, and attackers

Adversary Attributes

- Objectives
  - Intention and goals of attackers
- Methods
  - The anticipated attack techniques, or types of attacks
- Capabilities
  - Computing resources (CPU, storage, bandwidth), skills, knowledge, personnel, opportunity (e.g., physical access to target machines)
- Funding level
  - Influences attacker determination, methods and capabilities
- Outsider vs. insider
  - Outsider is remote attacker, while insider has access to network

Threat Modeling Approaches

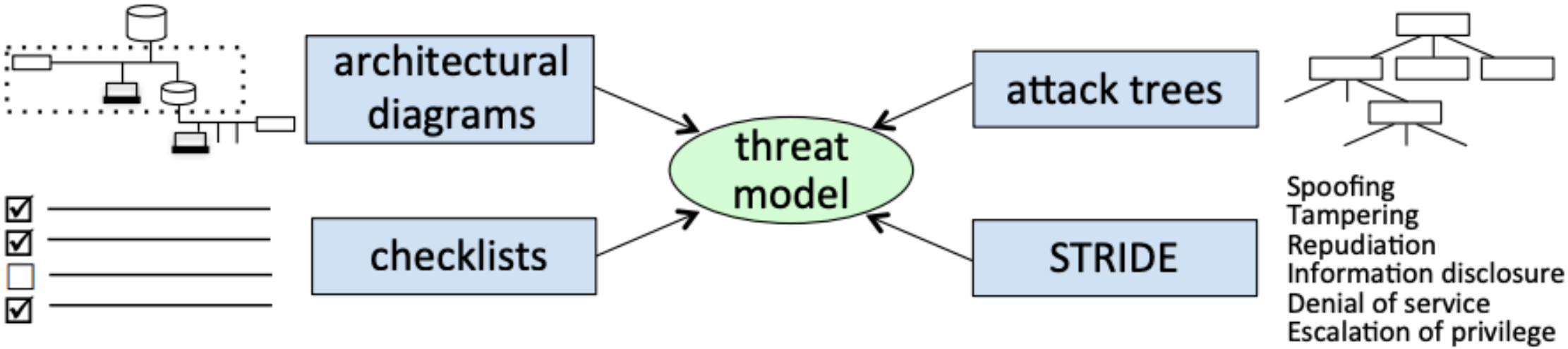
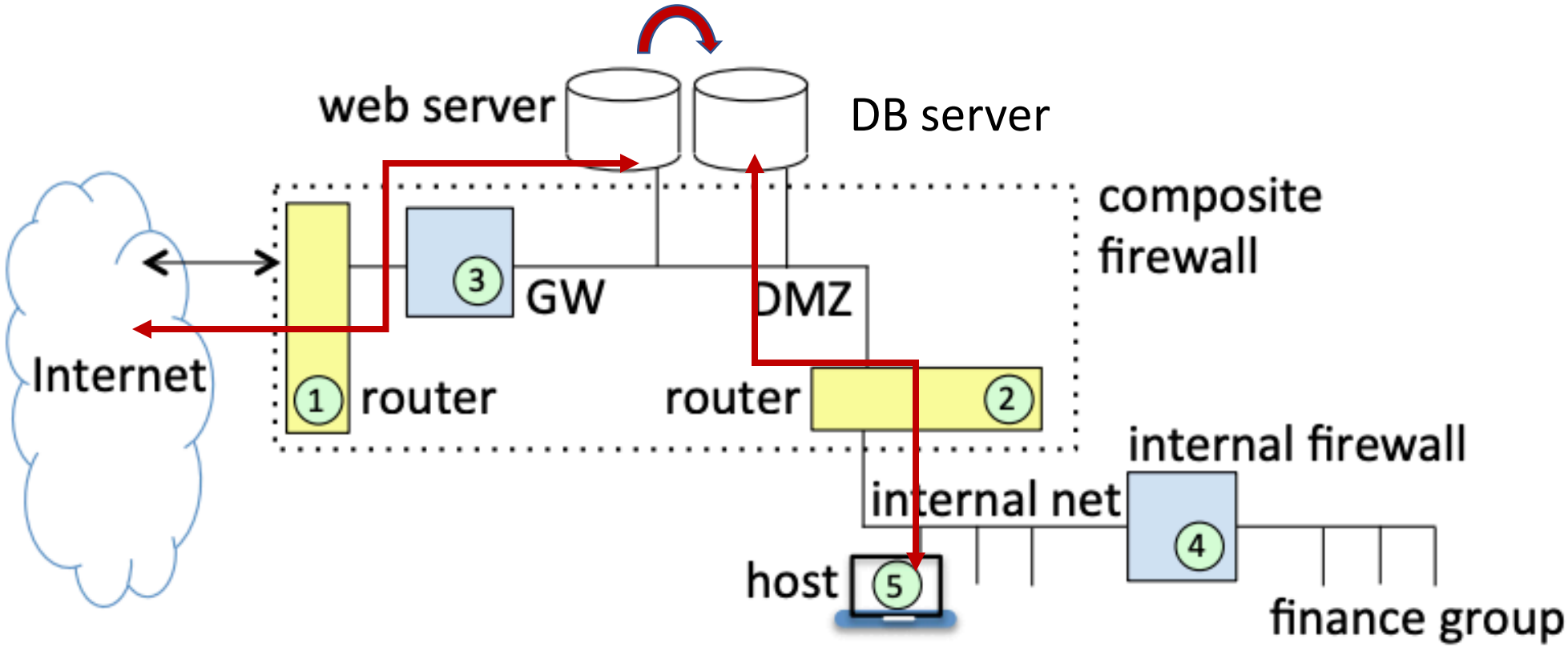


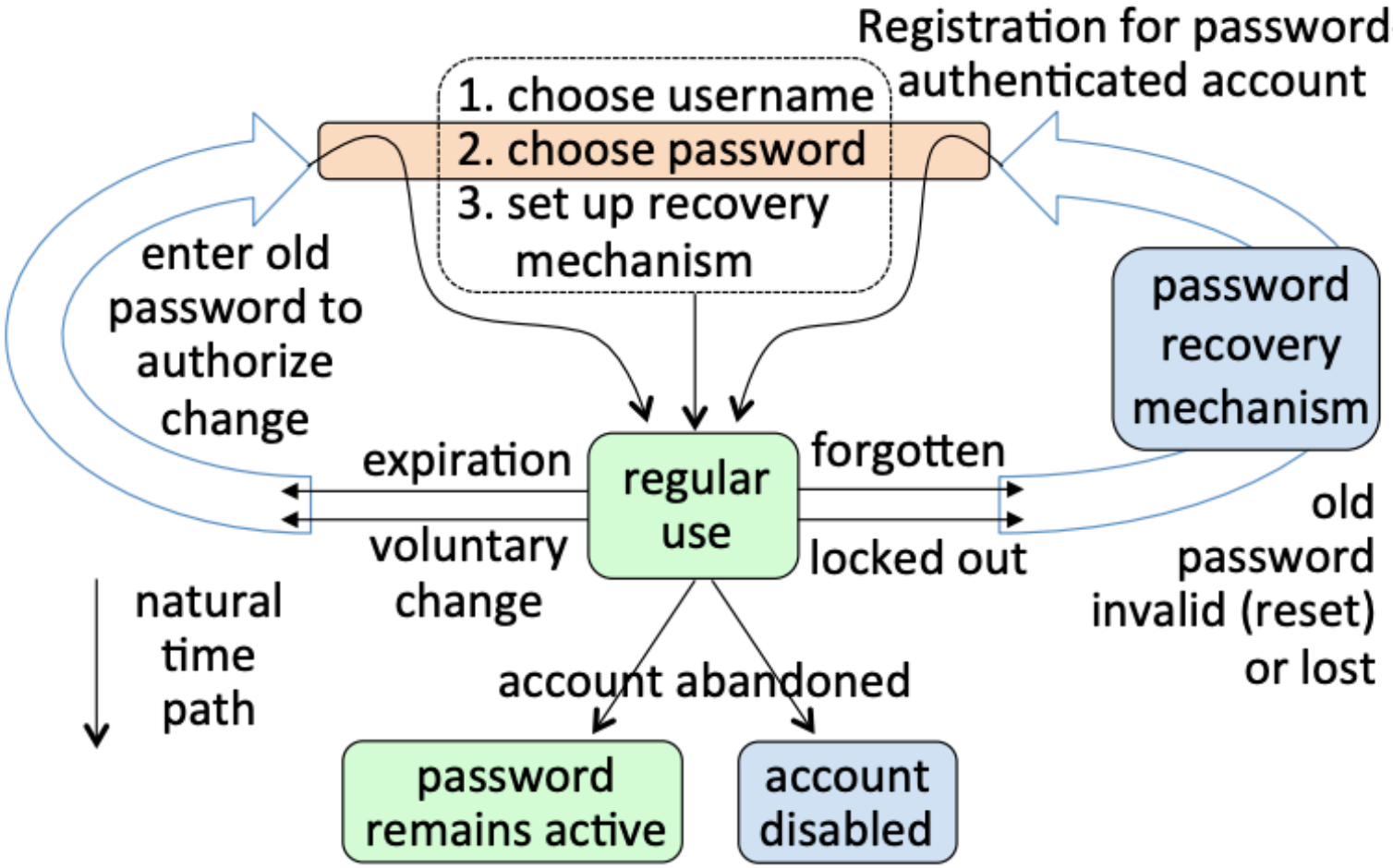
Figure 1.5: Examples of threat modeling approaches.

Diagram-based Threat Modeling



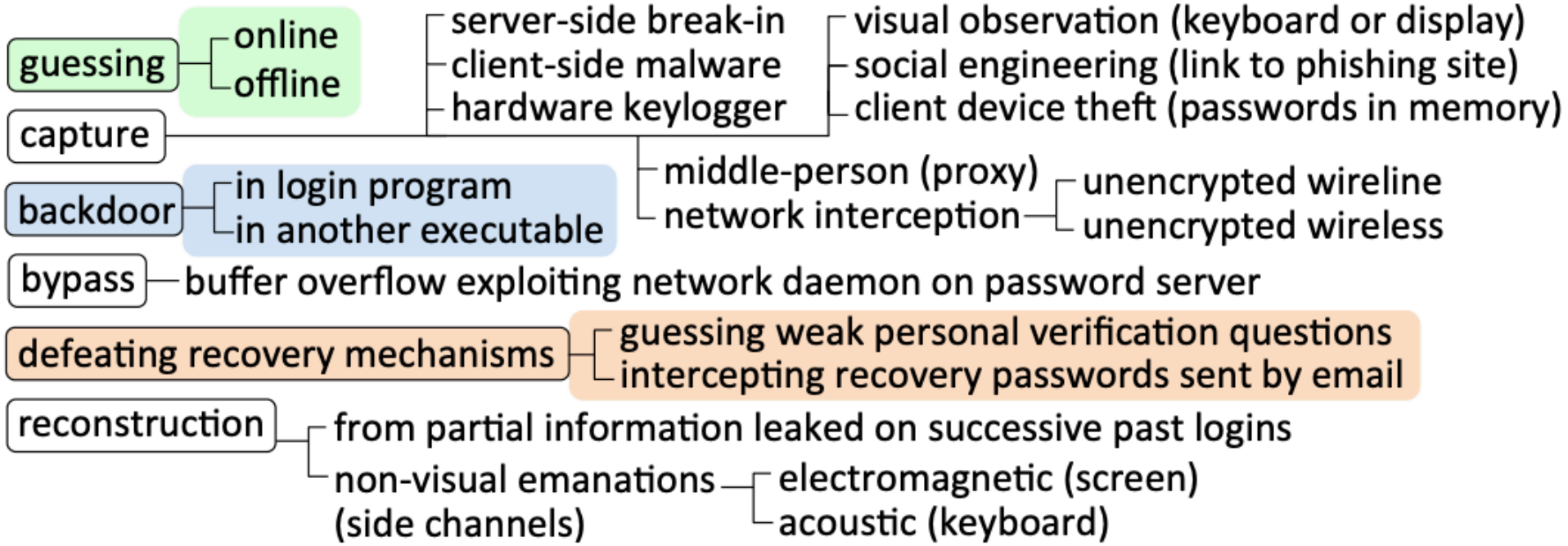
Data flow: how data flows through the system

Password Authentication Lifecycle Diagram



User workflow: model user actions

Attacks on Password-Based Authentication



- Attack objective: compromise user password
- Attack vectors: guessing, capture, backdoor,
- Attacker capabilities: client-side or server-side compromise
- Attack methods: social engineering, use of vulnerabilities

Attack Trees / Graphs

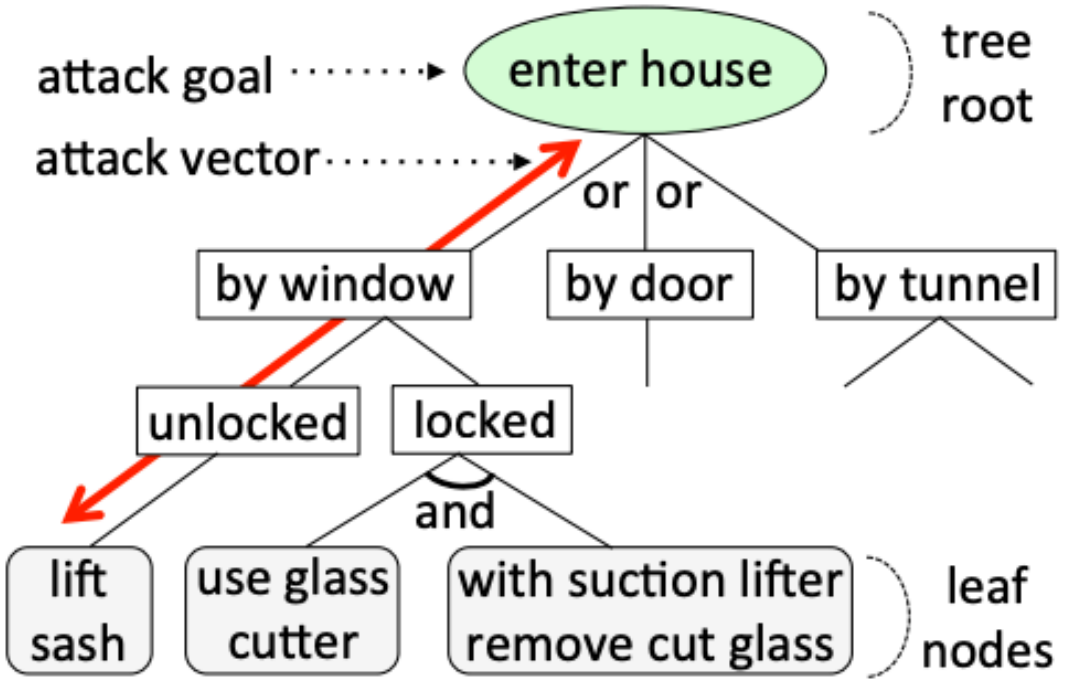


Figure 1.8: Attack tree. An attack vector is a full path from root to leaf.

- Attacker needs one path to get access
- Defender needs to secure all paths

Threat Modeling in Practice

- Important for all organizations to engage in
- Multi-stakeholder process
  - Engineering and IT/DevOps
  - Legal Counsel
  - Executives
- Various methodologies are available
  - Diagram-based
  - Attack-trees
- What can go wrong?
  - Invalid assumptions
  - Mismatch between model and reality
  - Focus on wrong threats

Challenges: What Can Go Wrong?

- Malicious infection in enterprise
  - Create firewall rules to block incoming suspicious network traffic (e.g., all IPs from country X are blocked)
  - Threat model
    - Remote attackers on network
    - Enterprise machines are protected from malicious infection from country X
  - Alice works from her favorite coffee shop and visits a gaming site; her machine visit an IP from country X and gets infected.
  - Bob gets an USB drive from a conference and plugs it into his laptop; his machine gets infected.
- Hotel safebox
  - Alice looks her valuables in the hotel safe box
  - Threat model
    - Attackers might have access to the room (e.g., cleaning personnel) but not to safebox
    - Her values are safe
  - After a nice dinner, she found they were stolen.

Why Computer Security is Hard

- Intelligent, adaptive adversary
- Defender-attacker asymmetry
- Universal connectivity (mobile, IoT devices)
- Pace of technology evolution
- Software complexity
- Usability and new features beat security
- Human factors
- Managing secrets (keys, certificates) for using crypto is difficult
- Security not from design (e.g., the Internet)
- Government obstacles