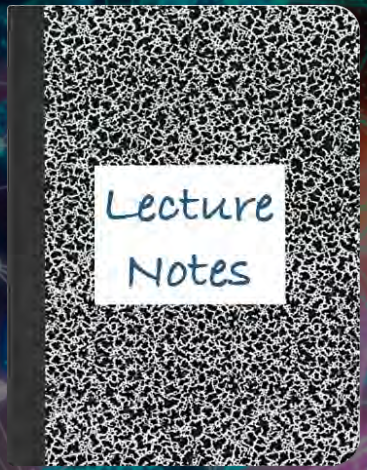
CS 419: Computer Security

Week 1: Part 4

Internet-Enabled Threats

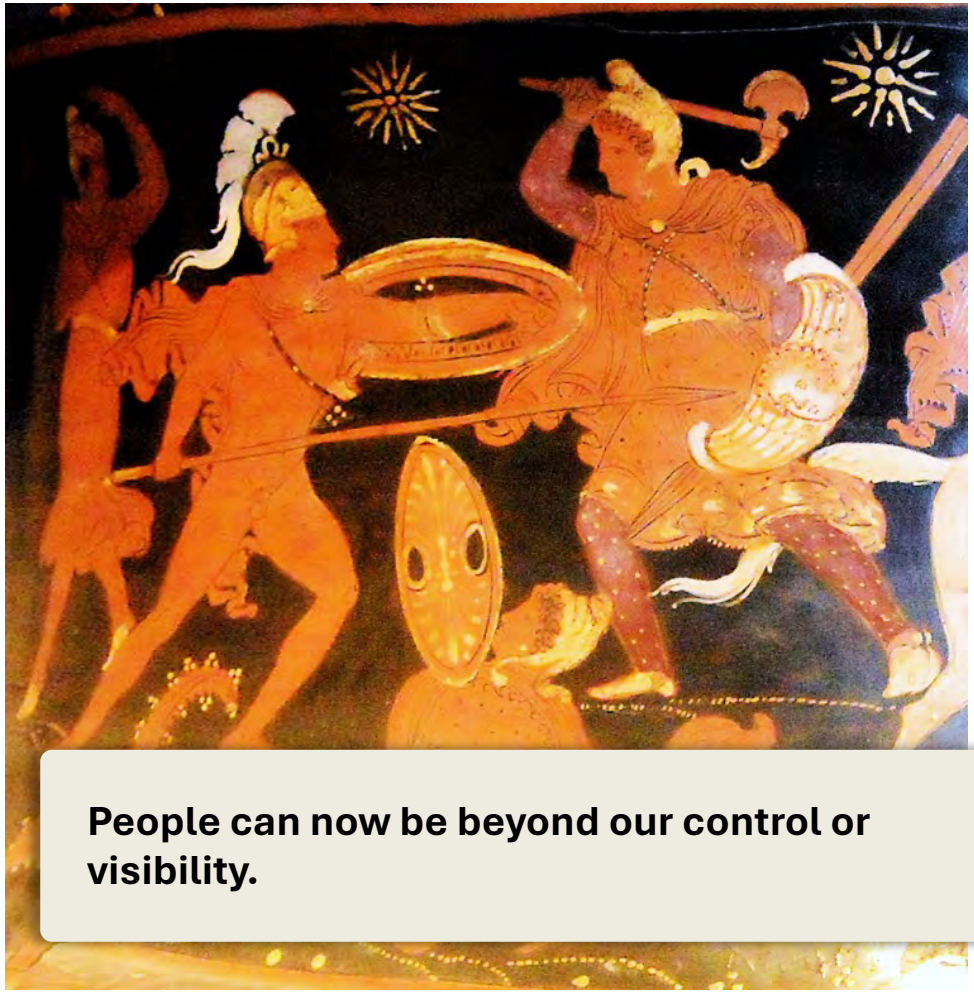


Paul Krzyzanowski

How the Internet Creates Vulnerabilities

- **Action at a distance**
- **Asymmetric force**
- **Actors can be anonymous**
- **No borders or checkpoints**
- **No distinction**
  - Hard to distinguish valid data from attacks
  - Can’t tell what code will be harmful until it’s executed

Action at a Distance



People can now be beyond our control or visibility.

Asymmetric Force

Information Technology has “opened up a whole new asymmetry in future warfare”

— *William J. Lynn III, Deputy Defense Secretary, 2010*

- The Pentagon’s 15,000 networks and 7+ million computers are being probed thousands of times daily
- Traditional deterrence models of retaliation do not apply in cyberspace

Asymmetric Force

- **Actors can project or harness greater force**
  - Low barriers to entry
  - Offense can be more effective than defense
  - A small number of actors can have a large effect
    - E.g., The *Anonymous* hacking group that tries to take down corporations or governments, attackers who send fraud or spam email, or those who send Facebook requests for money.
- **Sending millions of messages costs almost nothing.**
- **Distributed Denial of Service (DDoS) attacks allow rogue actors to overwhelm large companies and nation-states**
  - Small countries can now inflict damage on countries like the US or China.

Botnets

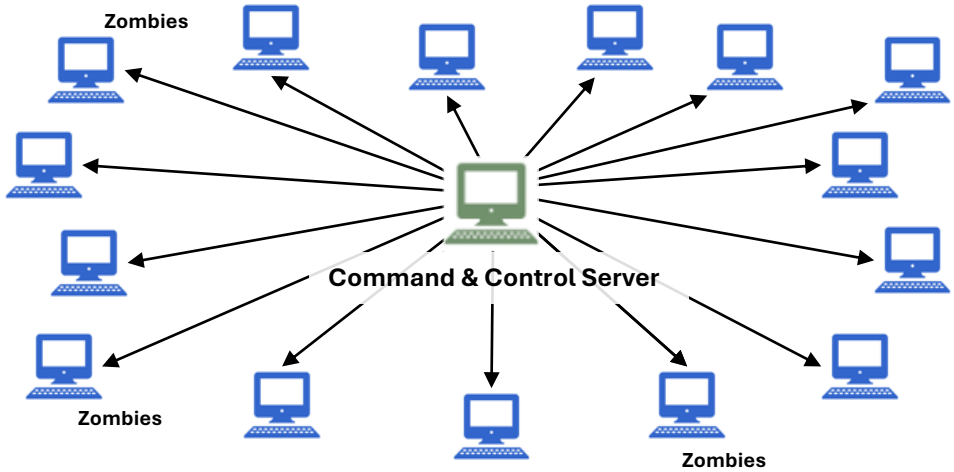
Botnet:

Collection of computers owned by innocent people but infected with malicious software

Botnet software periodically contacts a command & control server for directions on what additional software to download and what to run and whom to attack

Three common uses are:

1. **Distributed Denial of Service (DDoS) attacks**
   - One company has only so many servers
   - Send too much traffic to the servers and the server gets overloaded
   - Now nobody can get through – even legitimate traffic
   - Data is not destroyed but service is disrupted
   - Attacks come from the network of zombies
2. **Spamming/phishing**
   - Send tens of millions of malicious emails or texts
3. **Cryptocurrency mining**
   - Use the computing power of the zombies



Some large botnets

911 S5 Botnet

- >19 million compromised machines across almost 200 countries
- Deployed via malicious VPN software.
- Sold as ransomware-as-a-service.
- Taken down by FBI and international partners in 2024

Srizbi Botnet

- ~450,000 compromised machines
- Responsible for sending out more than half of all the spam being sent by all the major botnets combined.
- Crippled in 2008 by Estonian ISP

Emotet Botnet

- ~1.6 million compromised machines
- Distributed as an email attachment from infected computers.
- Eight countries worked to take this down in 2021

Mēris Botnet (2021 – now)

- **Exploited a 2018 bug in routers from Latvian router vendor MikroTik**
  - Winbox, a management component and a Windows GUI application for MikroTik's RouterOS
  - Allowed attackers to write files in the router, reconfiguring it for remote access
  - Only 30% of routers had the patch applied
  - Estimated 250,000 MikroTik routers were hacked
- **The Meris botnet broke the record for the largest volumetric DDoS attack twice in 2021**
- **Attacks**
  - Targets 50 different websites every single day with a daily average of 104 unique DDoS attacks
  - Top targets are banking, financial services, and insurance companies
  - 21.8 million RPS (requests per second) attack at a Russian bank hosting infrastructure on Yandex servers
  - 33%+ of attack traffic targeted China-based sites

https://blog.cloudflare.com/meris-botnet

https://cybernews.com/security/weve-seen-just-the-tip-of-the-meris-botnet-iceberg/

Mirai Botnet (2016-now)

- **Created by a Rutgers student**
  - Frustrated that upper-class students were given priority for CS electives
  - Assembled 40,000 bots to attack the Rutgers central authentication server
  - Later released the code so others built on it
- **Launched massive DDoS attacks that disrupted major internet services like Dyn, Twitter, and Netflix**
- **Most recently, spread primarily to compromised IoT devices**
  - Exploited a bug in Four-Faith industrial routers as well as Neterbit routers and Vimar smart home devices
- **October 29, 2024:**
  Responsible for the largest distributed denial of service attack to date:
  - Traffic at 5.6 terabits per second from over 13,000 IoT devices for 80 seconds

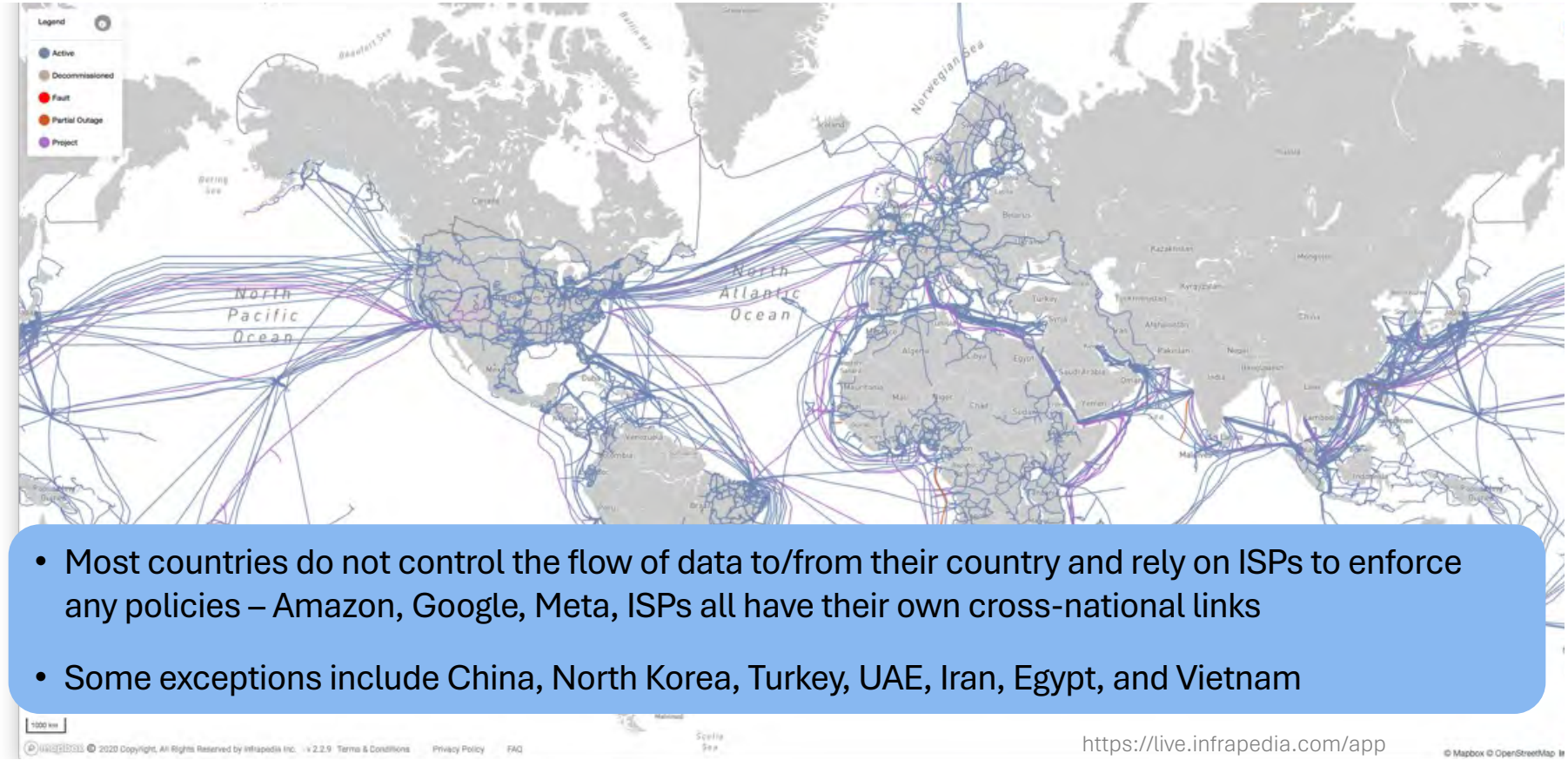
Anonymity: Identifying attackers

- **Internet protocols don't require identification**
- **We often can't identify the attacker**
  - Nobody knows who ran some of the biggest botnets or cyber-attacks
  - Botnet traffic comes from compromised innocent machines around the world
  - Identifying a source can be difficult
  - **Plausible deniability:** Governments can always deny initiating or funding cyberattacks
  - *Attack with impunity. We won't know who fired the missile.*
- **Make guesses**
  - Reverse engineer the code, compare to other known malware and attacks
  - Identify the location of the command & control server & who is accessing it
  - Trace packets & propagation paths
- **Sometimes we will never know**
- **Anonymity can lead to impersonation: trust becomes a challenge**
  - How do you know you are really communicating with your bank? How does the bank know it's you?

Integrity: Identifying legitimate users & services

- **Anonymity can lead to impersonation: trust becomes a challenge**
  - How do you know you are really communicating with your bank?
  - How does the bank know it's you?
- **Massive data breaches leaked everything about you**
  - Name, SSN, every address where you've lived, every school you attended
- **Caller-ID spoofing**
  - Enables attackers to send email or make phone calls that appear to come from trusted sources
- **Domain name confusion**
  - Users may not know what the legitimate domain names for an organization are or how to check
    - ✓ `verizonwireless.com`
    - ✗ `verizon-wireless.com`
    - ✓ `bankofamerica.com`
    - ✗ `bank-of-america.com`

Lack of Borders & Checkpoints



- Most countries do not control the flow of data to/from their country and rely on ISPs to enforce any policies – Amazon, Google, Meta, ISPs all have their own cross-national links
- Some exceptions include China, North Korea, Turkey, UAE, Iran, Egypt, and Vietnam

https://live.infrapedia.com/app

We expect you to show up in court…

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

REMARKS

CAUTION

Allegedly part of hacking team responsible for WannaCry ransomware, attack on Sony Pictures, and others

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a

Allegedly responsible for stealing terabytes of data, including coronavirus research, from western companies in 11 nations

Lack of Distinction in Data

- **All bits look the same**
- **How can you tell which data is malicious?**
- **Content may be hosted at Amazon, Google, or Microsoft servers, so the domains don’t look suspicious**

Networked Computer vs. Real-World Risks

Same motivations … but no need for physical presence!

- Mechanisms, risks, and access are different than in the physical world

- **Physical world risks are low (for most of us)**
  - Most people are not attacked
  - Most people are not victims of espionage
  - Most homes/offices aren't randomly broken into
- **Same threats in cyberspace as real-world threats:**
  - Theft, vandalism, extortion, fraud, coercion, con games

The End