

CS 55: Security and Privacy

The future

DEAR FUTURE SELF,

YOU'RE LOOKING AT THIS FILE BECAUSE
THE PARSE FUNCTION FINALLY BROKE.

IT'S NOT FIXABLE. YOU HAVE TO REWRITE IT.
SINCERELY, PAST SELF


DEAR PAST SELF, IT'S KINDA
CREEPY HOW YOU DO THAT.

ALSO, IT'S PROBABLY AT LEAST
2013. DID YOU EVER TAKE
THAT TRIP TO ICELAND?

STOP JUDGING ME!



Agenda

- 
1. Internet of Things (IoT)
 2. Cyber war
 3. Wrap up

Discussion

What is the Internet of Things (IoT)?

Ubiquitous/pervasive computing?

The Internet of Things (IoT) has been a long time in the making

The Tacoma News Tribune, April 11, 1953.

There'll Be No Escape in Future From Telephones

PASADENA.—AP —The telephone of the future?

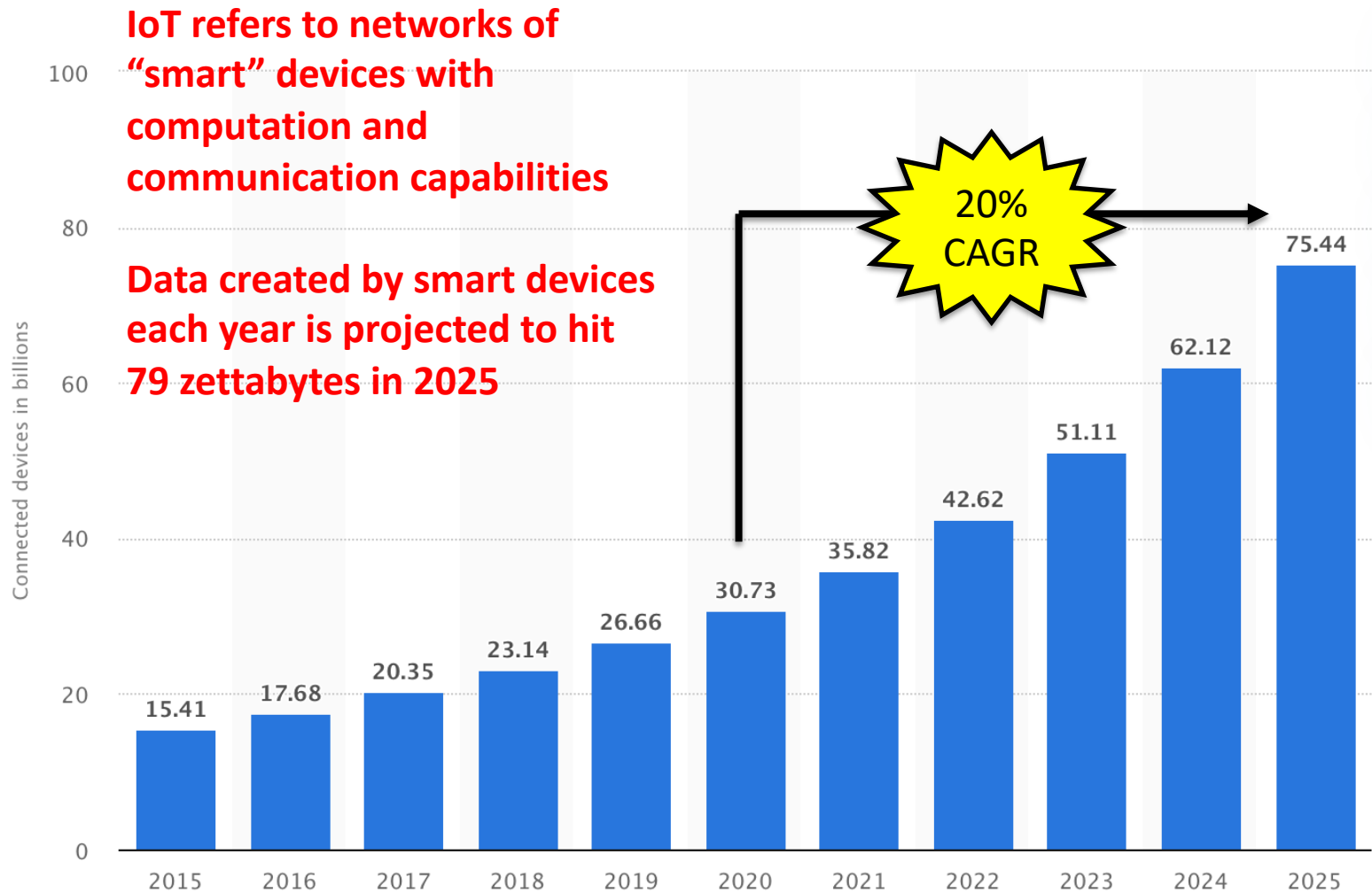
Mark R. Sullivan, San Francisco, president and director of the Pacific Telephone & Telegraph Co., said in an address Thursday night:

"Just what form the future telephone will take is, of course, pure speculation. Here is my prophecy:

"In its final development, the telephone will be carried about by the individual, perhaps as we carry a watch today. It probably will require no dial or equivalent, and I think the users will be able to see each other, if they want, as they talk.

"Who knows but what it may actually translate from one language to another?"

The number Internet connected devices is projected to skyrocket



Typically, IoT deployments involve three layers, each a potential attack vector



Perception layer

- Sensors
- Actuators
- Microcontrollers
 - Frequently low powered (battery and computationally)

Each layer is a potential attack vector



Communication layer

Device to device

- Devices often communicate between themselves (BLE, Zibgee)
- MQTT

Gateway

- Gateway connects devices to cloud (Wi-Fi)
- Not needed if cellular enabled



Hard to tell where data goes from here

Application layer

Aggregate

- APIs
- Bundle data

Analyze

- Develop insights from data

Distribute

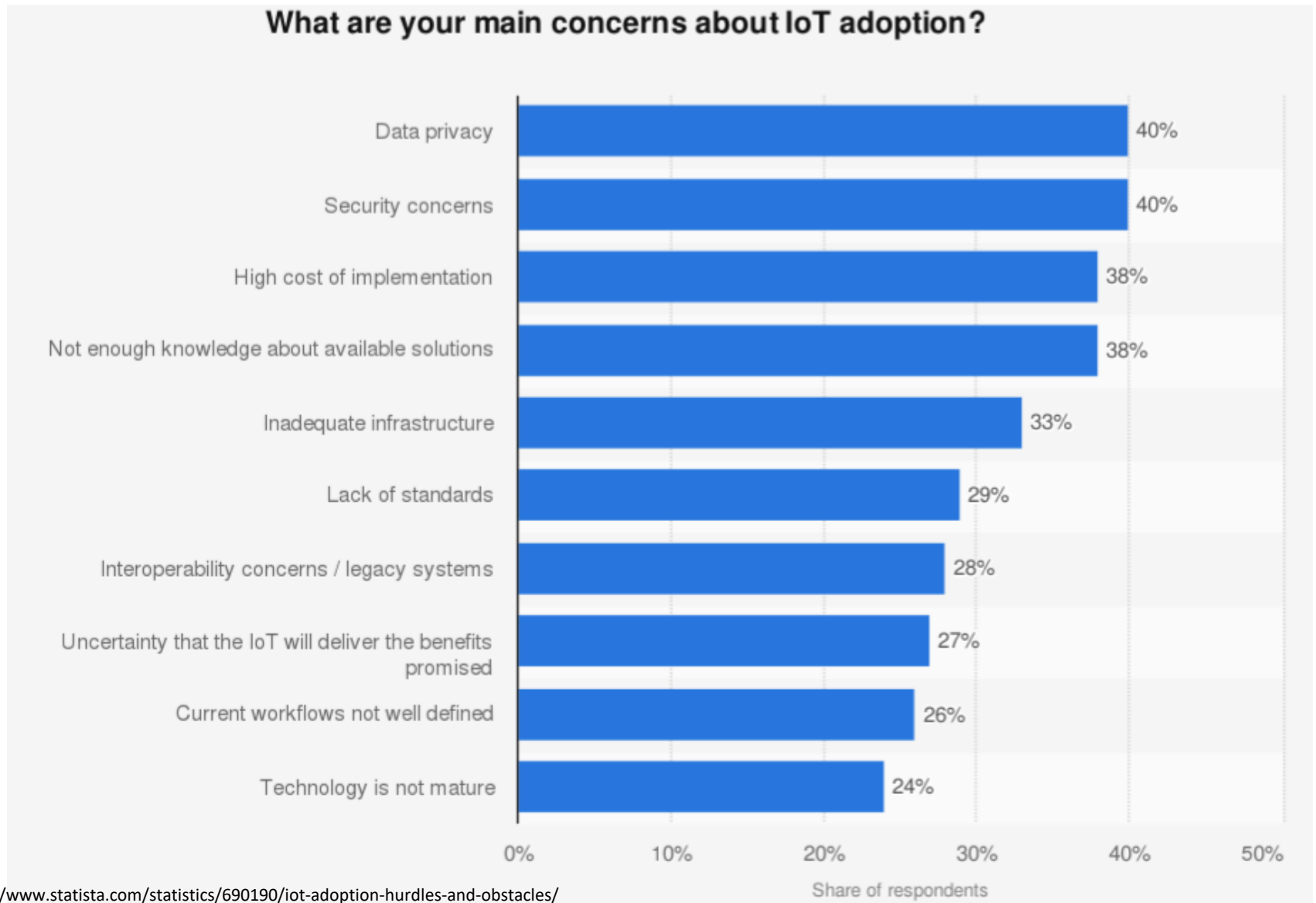
- Provide insights to users (or companies) ⁷

Discussion

If there will be many more smart devices soon

- What are some potential benefits?
- Do you have any concerns?

A survey of nearly 1,000 tech professionals highlighted several concerns



IoT can compromise Confidentiality, Integrity, and Availability

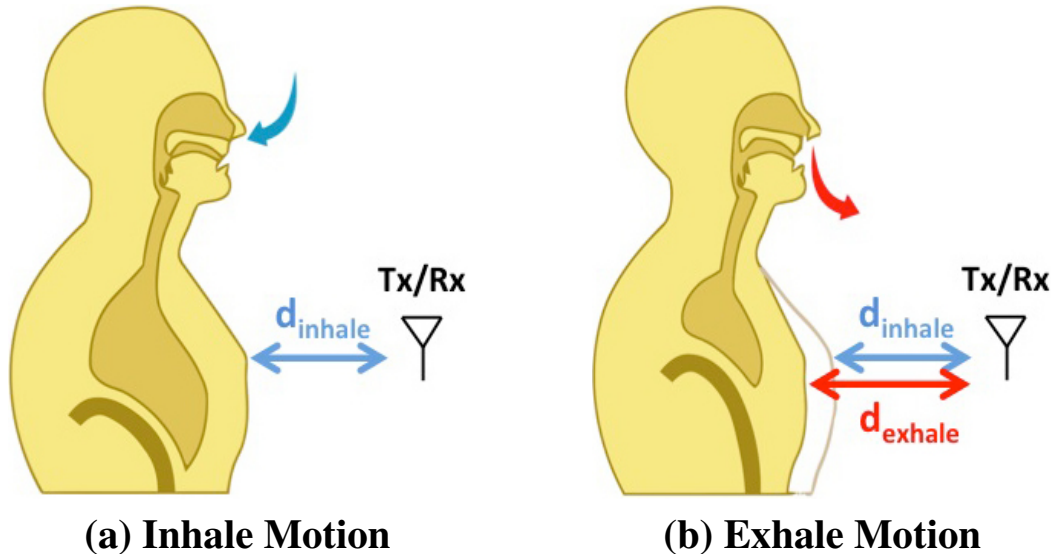
Confidentiality

Integrity

Availability



Confidentiality: IoT can collect data without your knowledge or consent



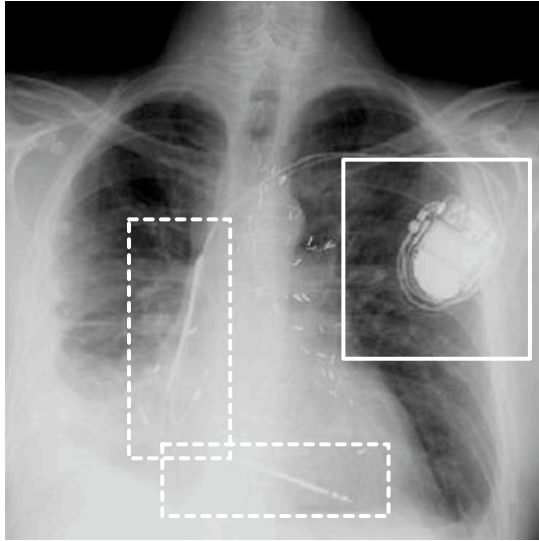
Collecting respiration and heart rate

- Vital Radio project used wireless signal to detect respiration and heart rate
- Could work without subject's knowledge or consent

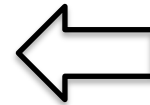
What if health data collected at work shared with insurance company?

Others have tried to use wireless signals as a biometric!

Integrity: Implanted medical devices can be remotely instructed to deliver a shock



Pacemaker implanted into a patient's chest



Programmer can send commands to pacemaker



So can a cheap Software Defined Radio

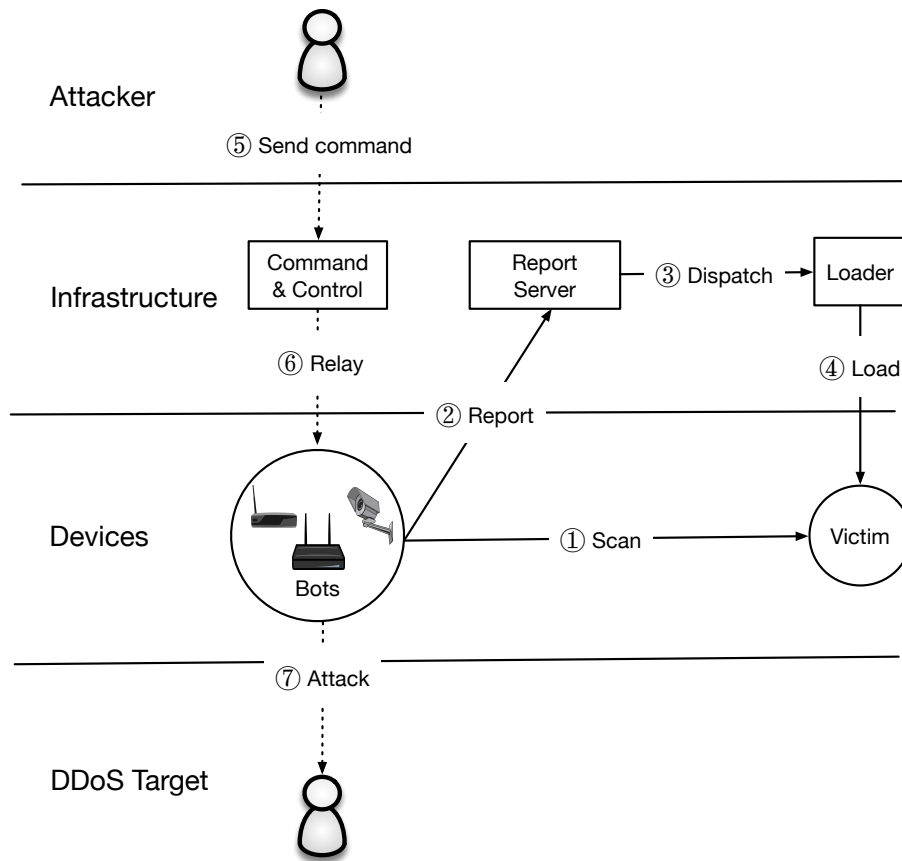
**Older IMDs did not
authenticate programmer
New ones do
Shield could help**

Integrity: Deep fakes are becoming increasingly realistic



Availability: Devices in a botnet can act together to cause major disruption

Mirai botnet



Many devices were vulnerable due to default credentials

Password	Device Type
123456	ACTi IP Camera
anko	ANKO Products DVR
pass	Axis IP Camera
888888	Dahua DVR
666666	Dahua DVR
vizxv	Dahua IP Camera
7ujMko0vizxv	Dahua IP Camera
7ujMko0admin	Dahua IP Camera
666666	Dahua IP Camera
dreambox	Dreambox TV Receiver
juantech	Guangzhou Juan Optical
xc3511	H.264 Chinese DVR
OxhlwSG8	HiSilicon IP Camera
cat1029	HiSilicon IP Camera
hi3518	HiSilicon IP Camera
klv123	HiSilicon IP Camera

Mirai quickly compromised hundreds of thousands of devices

Availability: Devices in a botnet can act together to cause major disruption

Mirai botnet



Distributed Denial of Service (DDOS) attack

- DNS provider Dyn was flooded with traffic in 2016
- Dyn servers overwhelmed
- Users unable to access web sites

Mirai and variants are still alive today

- In 2019 researchers discovered Mirai with updated functionality
- Malware authors used TOR Network for anonymity

Agenda

1. Internet of Things (IoT)



2. Cyber war

3. Wrap up

Five important ways the cyber threat is different from traditional warfare

1. The most powerful is the most vulnerable
2. The government cannot go it alone
3. The attack surface is huge
4. Victims often don't know they are victims
5. Warning and decision times are flipped

Also, the targets can be different!

Some possible cases of cyber war: Estonia attacked with denial of service



Estonia

- 2007
- Possibly first instance of cyber war
- State websites taken down in DOS attack after altercation with Russia

Russia suspected, but no definitive evidence
NATO did not declare attacks an act of war
Others did!

**How can we tell
where an attack
originated?**

Some possible cases of cyber war: Iran attacked with Stuxnet



U.S. and Israel suspected

Iran

- 2009
- Nuclear enrichment plan hit by USB-borne virus
- Virus extremely sophisticated, used several zero-day vulnerabilities
- Destroyed uranium enrichment centrifuges

Some possible cases of cyber war: U.S. OPM records exfiltrated



U.S.

- 2013 - 2015
- U.S. Office of Personnel Management (OPM) discovered millions of SF-86 security background check forms exfiltrated
- Forms contained highly sensitive data on U.S. citizens applying for government jobs

China suspected

Is this war or espionage?

Some possible cases of cyber war: Sony Pictures private data released



North Korea suspected

Company: Sony Pictures

- 2014
- Sony Pictures made a comedy movie called “The Interview” depicting the assassination of North Korea’s leader Kim Jong Un
- Sony Pictures data exfiltrated
 - Movie scripts
 - Salaries
 - Embarrassing emails
- Attackers threatened physical violence at movie theaters

What about when a *company* is suspected of being attacked by a *nation*?

Some possible cases of cyber war:

SolarWinds supply chain attack

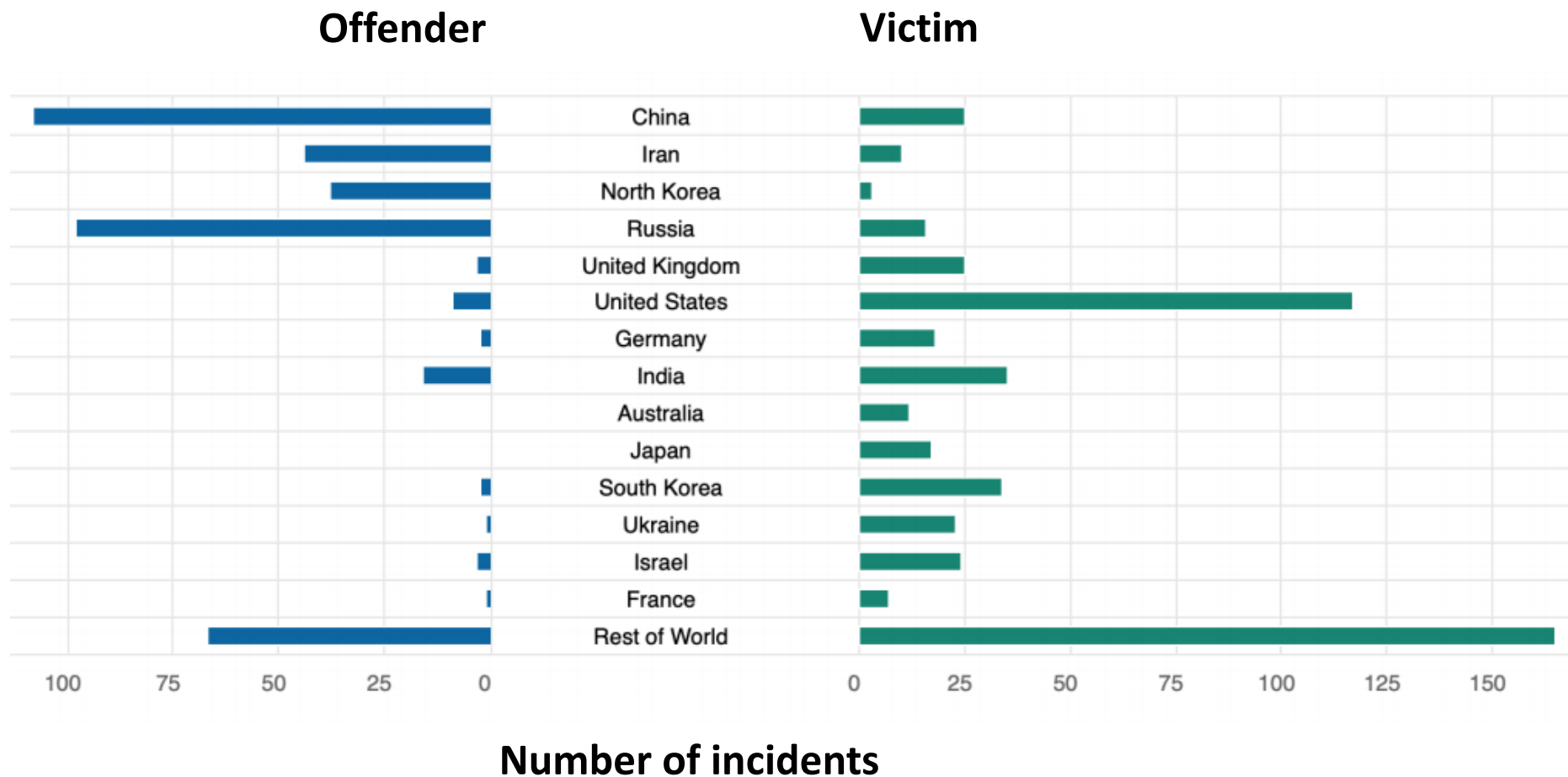


Russia suspected

Company: SolarWinds

- 2020
- SolarWinds makes a network monitoring platform called Orion
- Orion used by thousands of large organizations
 - 425 out of U.S. Fortune 500
 - U.S. government agencies such as State Department, Treasury, DoD
- Malicious trojan code inserted into Orion's code base
- Executable code distributed to SolarWinds customers

Several countries have been linked to possible cyber war events



Discussion

When is an attack on the cyber infrastructure considered an act of war? Are there different types of cyber attack?

How should a country retaliate from a cyber attack?

Is cyber space a separate domain of war; different from land, sea, or air combat?

Autonomous weapons: should humans always be in the loop?

The warrior of the future may look different from the warrior of the past



There is reason for optimism

Your generation is more tech-savvy than the past

You understand how things work and (sometimes) where data goes

People are thinking about privacy and security issues more now than in the past

Agenda

1. Internet of Things (IoT)

2. Cyber war

 3. Wrap up

This class is about security and privacy; we ~~will consider~~ considered seven major topics

Seven main topics for the course:

1. Adversaries
2. Cryptography
3. Common attacks
4. Defensive tools
5. Security operations
6. Privacy and the law
7. The future

Look for a way to say yes

Should humans be in the loop?



INCREASE IN VIOLENT CRIME

SDN

