ECE458/ECE750T27: Computer Security
Introduction

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

TULiPS
Technology Usability Lab in Privacy and Security

First, the news…

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

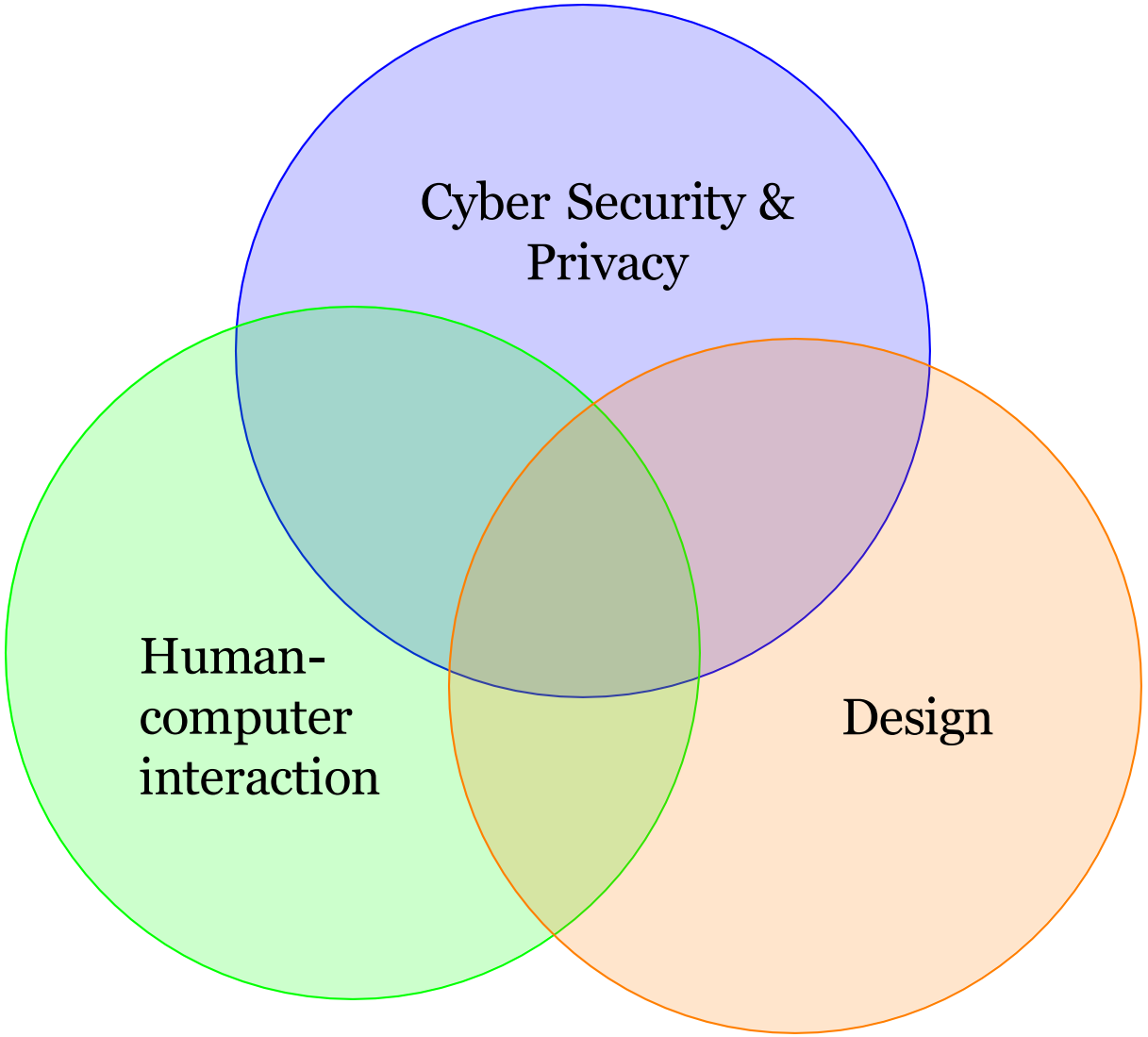
Outline

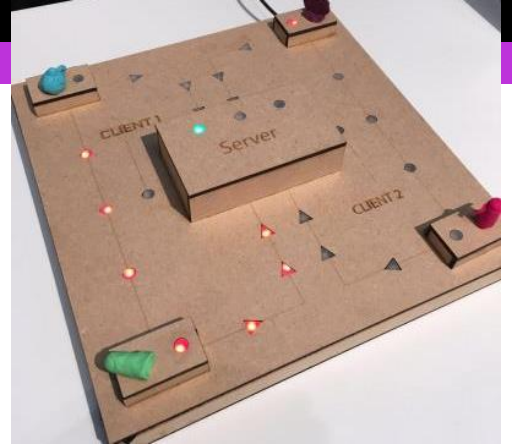
- Introduction of Dr Vaniea
- Course structure
- Definition of computer security
- Data breaches, what do they look like?
- Security properties

INSTRUCTOR: KAMI VANIEA

Instructor

Dr Kami Vaniea
University of Waterloo
tulipslab.org
kami.vaniea@uwaterloo.ca

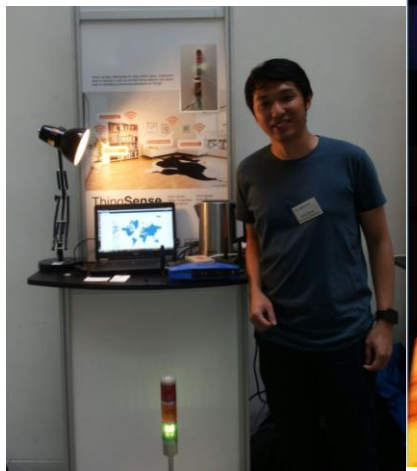




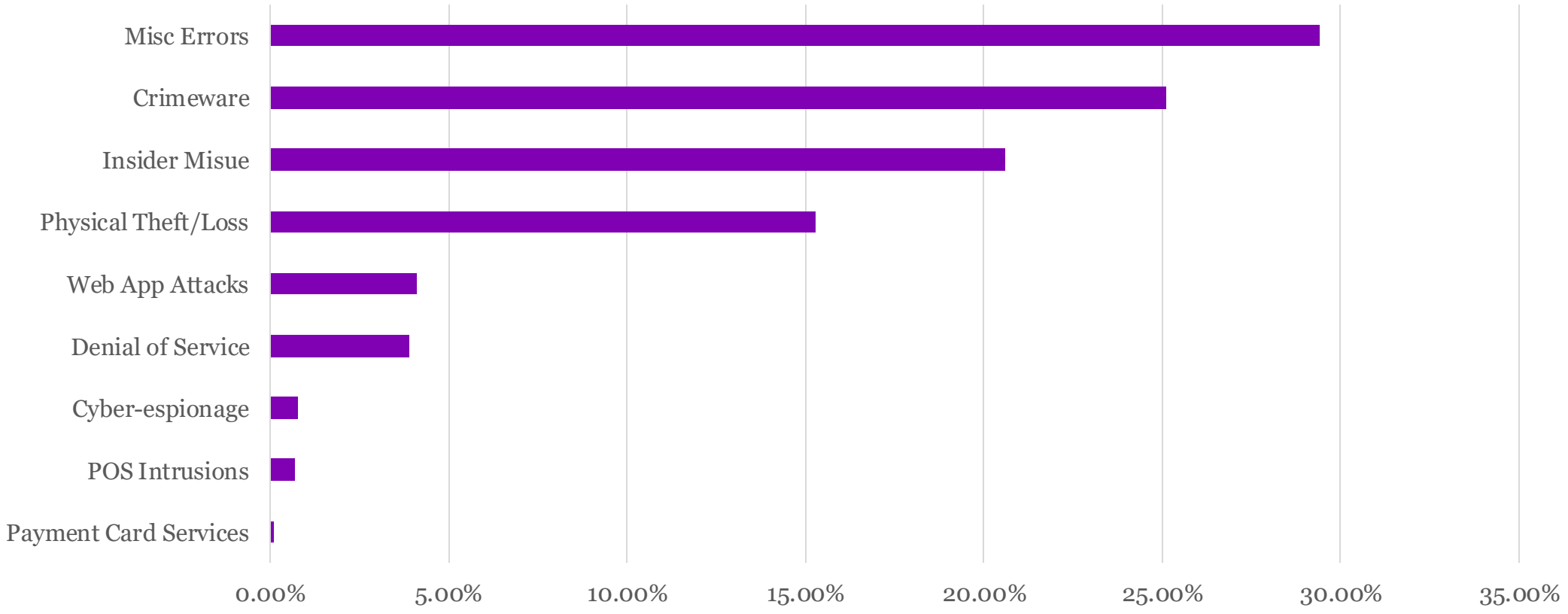
tulipslab.org

- Phishing
- System administration patch management
- Developer-centered privacy
- Experimentation in VR
- Bystander privacy for smart speakers
- Serious games
- IoT
- Behavior tracking on websites

TULiPS
TECHNOLOGY USABILITY LAB
IN PRIVACY AND SECURITY

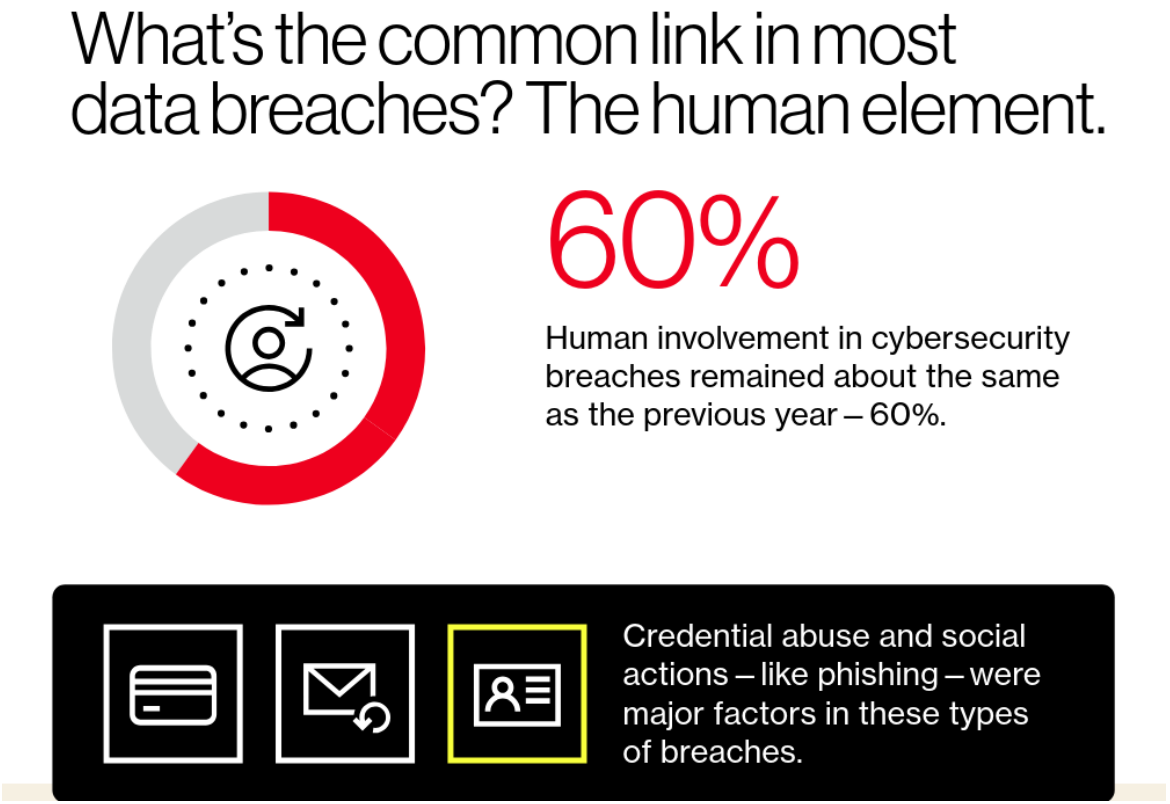


People account for 90% of all security incidents



Humans are an important part of a secure system

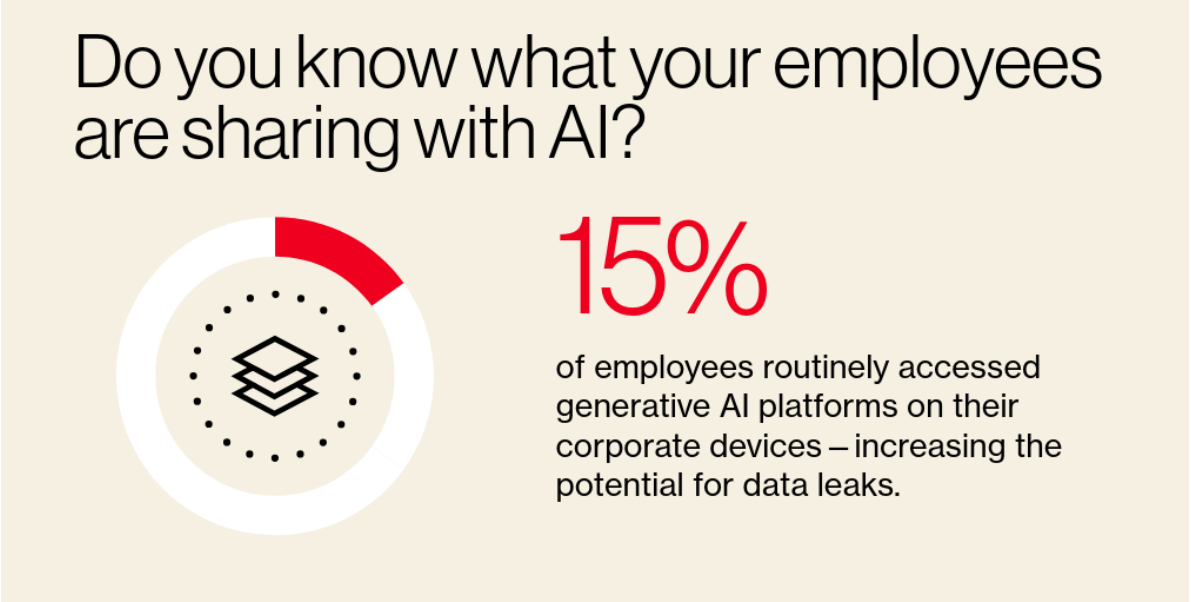
- Phishing – scam emails causing people to give away login credentials
- Giving away important data
- Giving access to important resources



Verizon Data Breach Report Infographic 2025

Humans are an important part of a secure system

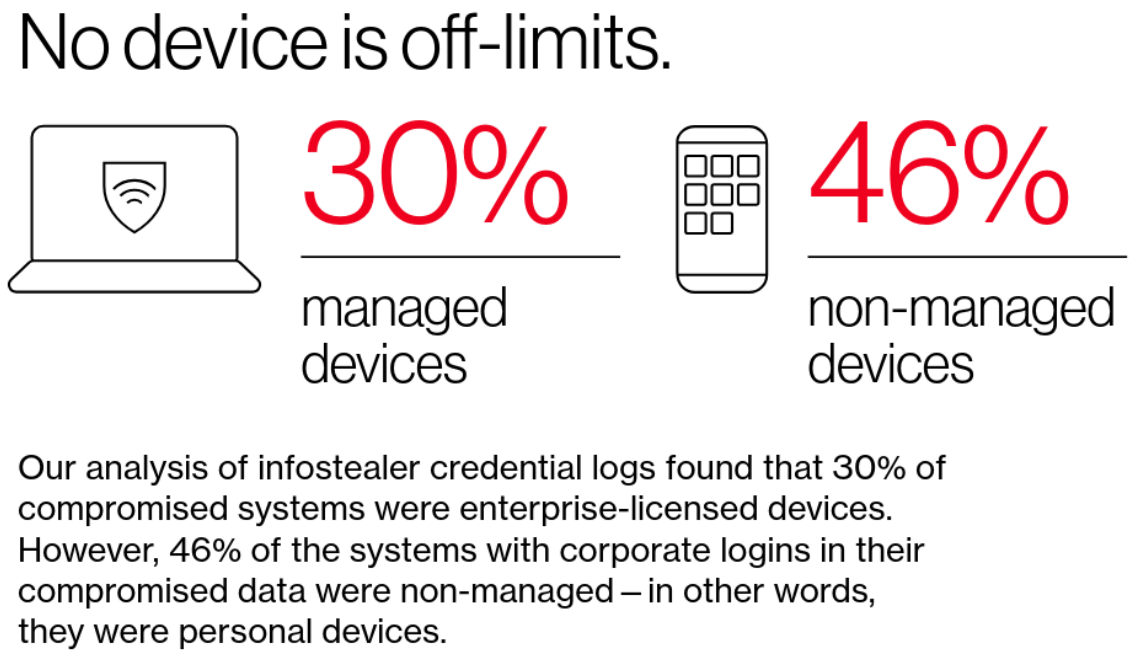
- Phishing – scam emails causing people to give away login credentials
- Giving away important data
- Giving access to important resources
- Putting company information into AI



Verizon Data Breach Report Infographic 2025

Humans are an important part of a secure system

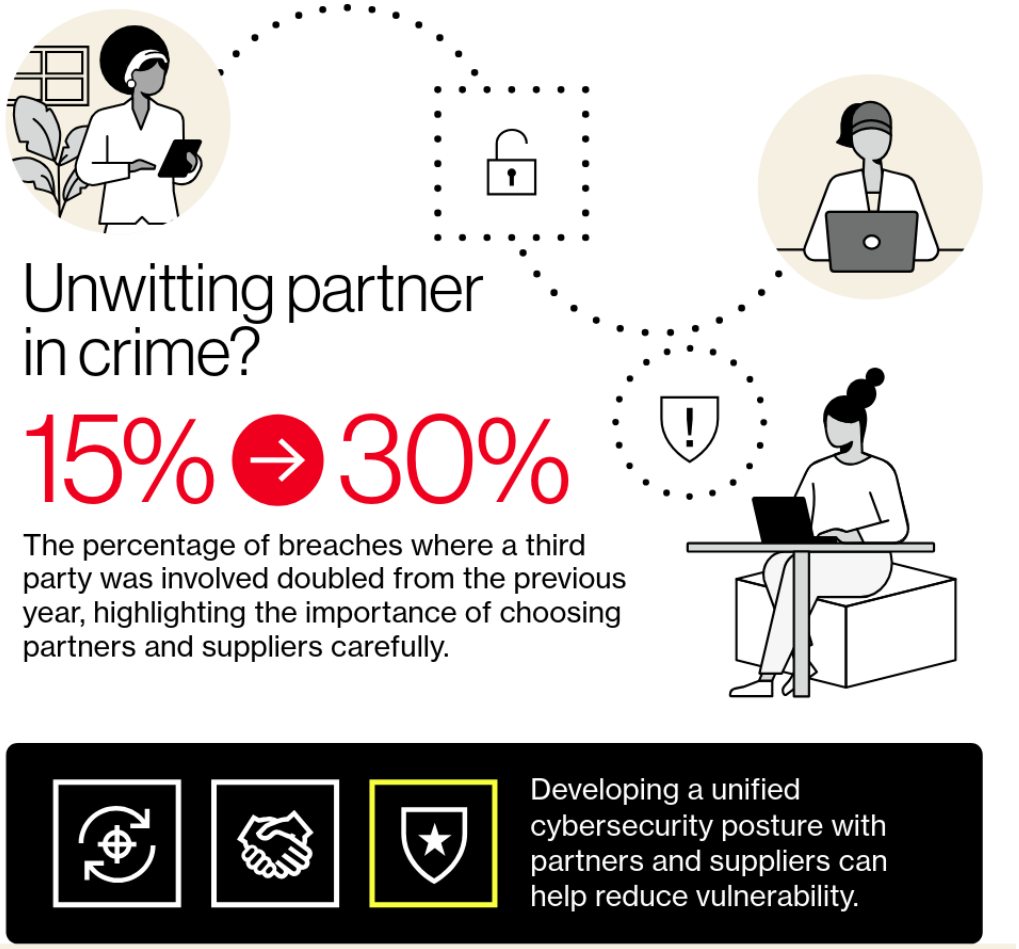
- Phishing – scam emails causing people to give away login credentials
- Giving away important data
- Giving access to important resources
- Putting company information into AI
- Logging in from unmanaged computers



Verizon Data Breach Report Infographic 2025

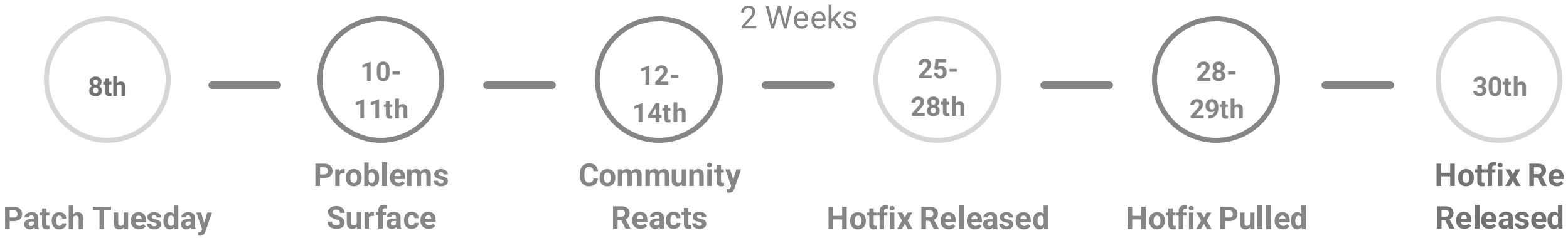
Humans are an important part of a secure system

- Phishing – scam emails causing people to give away login credentials
- Giving away important data
- Giving access to important resources
- Putting company information into AI
- Logging in from unmanaged computers
- Contracting with unsecure partners



Verizon Data Breach Report Infographic 2025

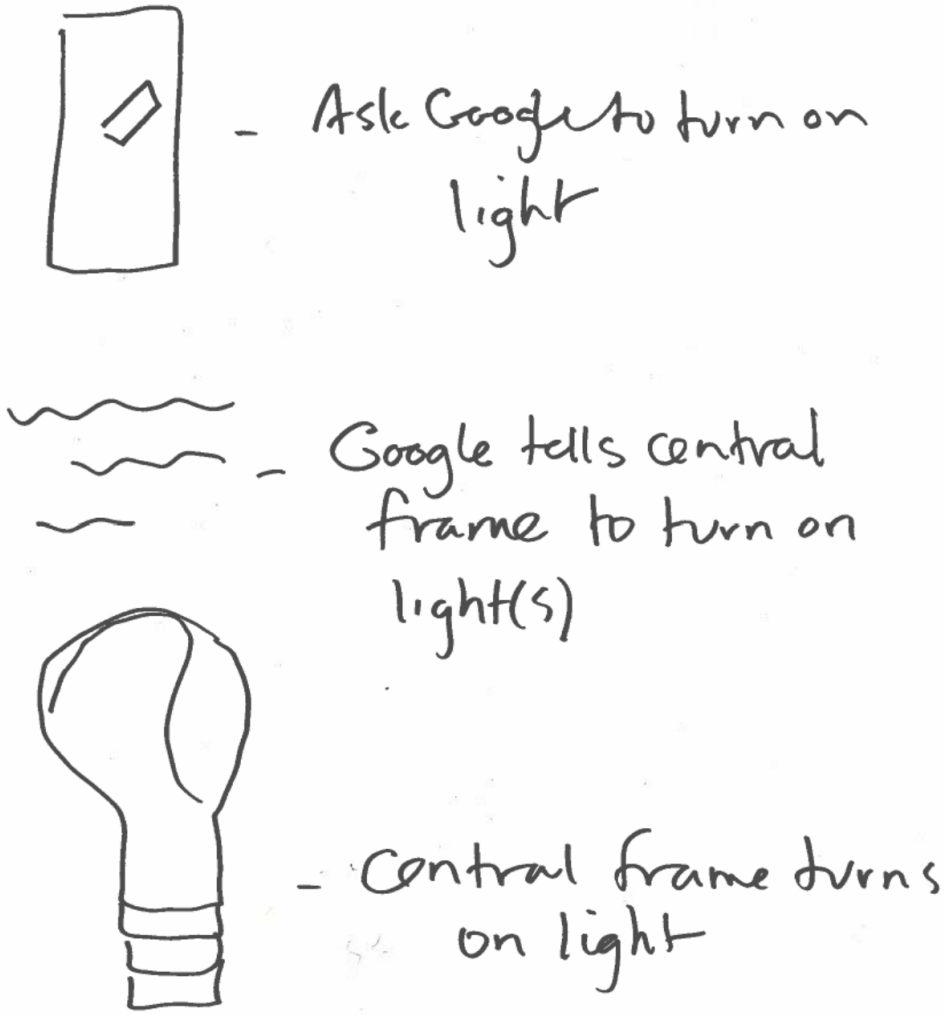
Software Updating
Timeline of a “critical” patch with errors (KB4034664, KB4034679)



Smart speaker bystander privacy

Issues like:

- Learning device exists
- Internet connection not obvious
- One account, but many users
- Unintended connections



N. Meng, D. Keküllüoğlu, K. Vaniea; Owning and Sharing: Privacy Perceptions of Smart Speaker Users; CSCW 2021

Virtual Reality a test-bed for Usable Security research?

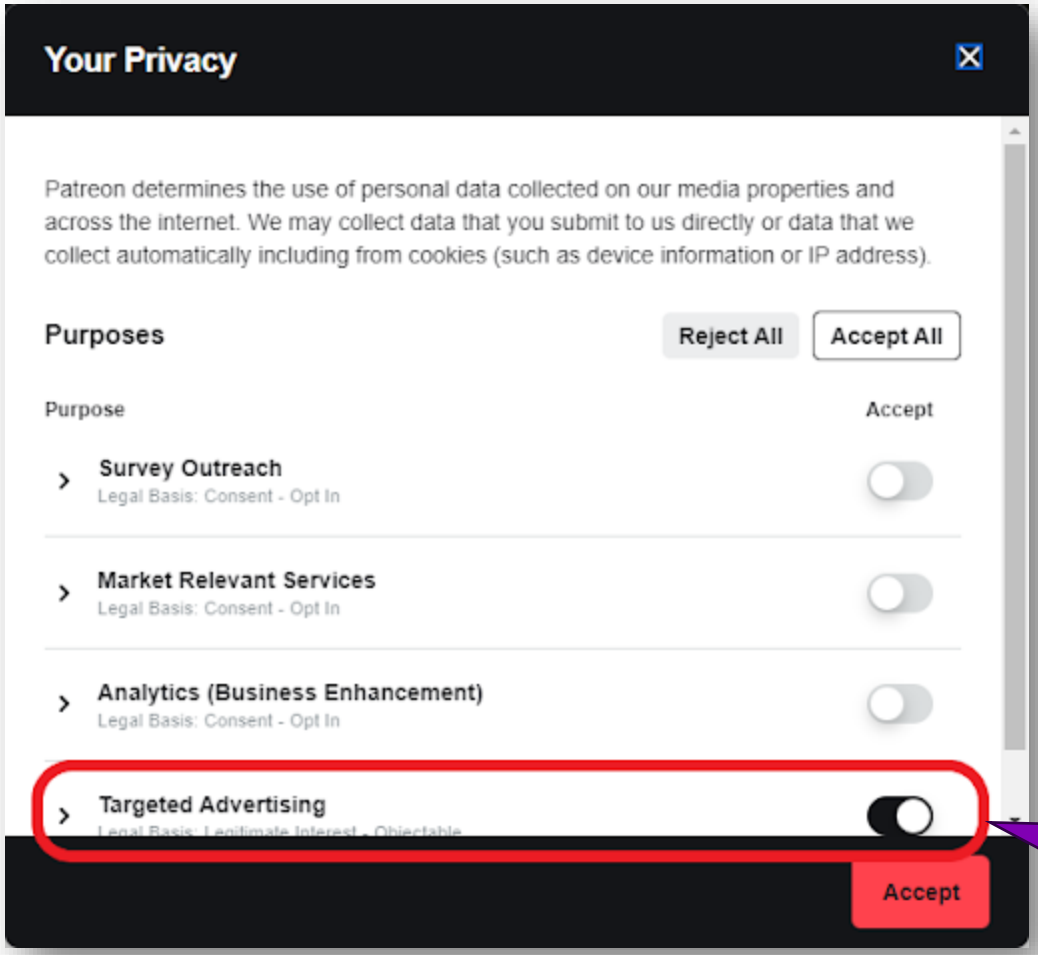
Real World

CueAuth, Khamis et al., IMWUT 2018

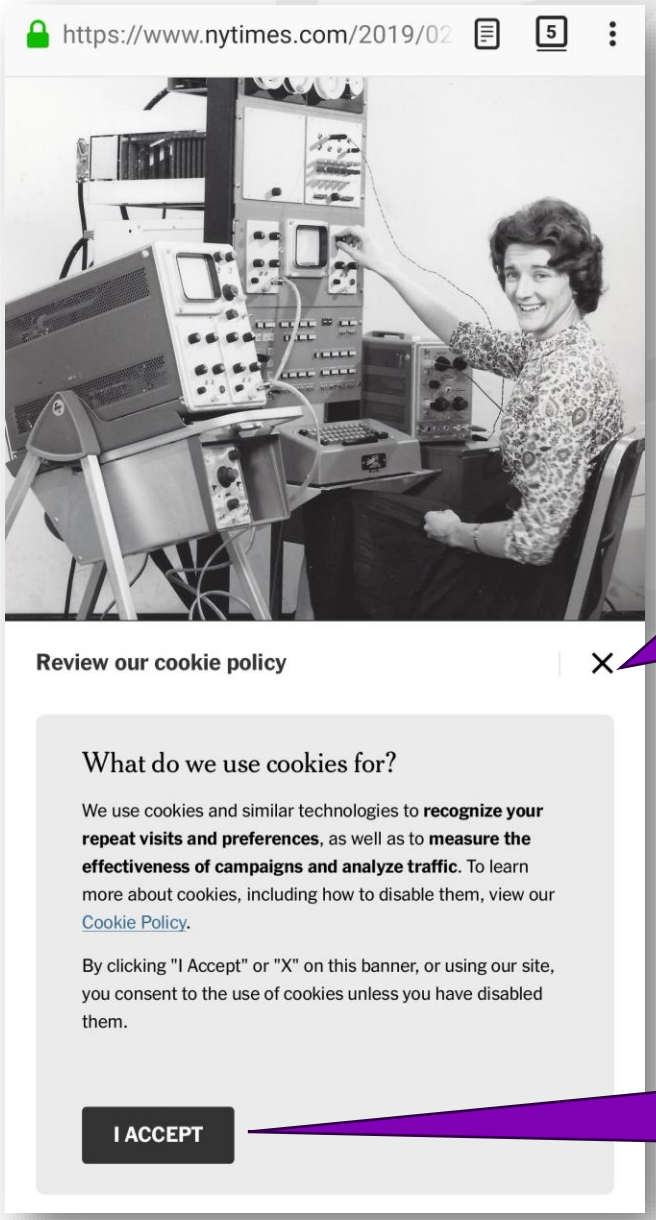
Virtual Reality

RepliCueAuth, Mathis et al., CHI 2021

Cookie dialogs



Hidden options



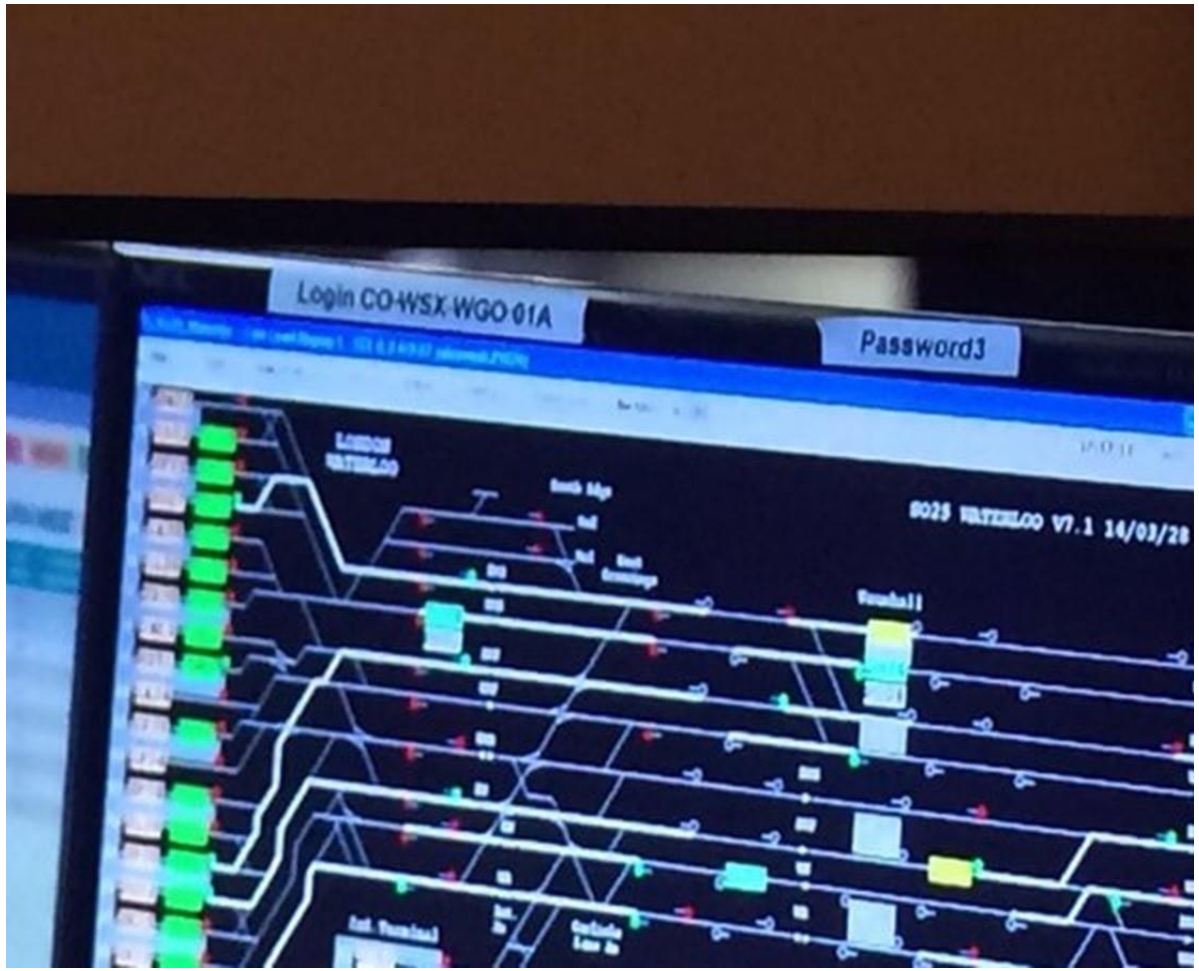
Unclear effect

No choices

D. Kirkman, K. Vaniea, D.W. Woods; DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs; EuroS&P. 2023.

ECE 750 – Usable Security and Privacy

- Grad-level course on the human factors of security and privacy
  - Research paper reading
  - Study design and planning
  - Policy and decision making in regards to security
- Undergraduates can take on request
- https://vaniea.com/teaching



COURSE STRUCTURE

Topics covered

- Basics of security
- Authentication and access control
- Cryptography basics
- Network and wireless security
- Programming security
- Web security
- Privacy

Recommended textbook

- Recommended textbook: Security in Computing 6th edition
- 5th edition would probably work too
  - Examples are all old
  - Main concepts are the same
- Examined content will all be provided in lecture

Schedule

- **Lecture:** Mondays and Fridays 10:00-11:20am
- **Makeup Lectures:**
  - June 2nd I will use the makeup lecture
  - If we use others, I will do a video recording
- **Tutorials:** Thursdays 8:30-9:20am
  - Used before assignment deadlines so TAs can provide more time and/or practice problems
- **Midterm:** Online via Learn June 16-20
- **Final:** Not yet scheduled

Schedule exceptions

- May 19 – No class, holiday
- June 2 – Makeup lecture, two lectures that day
- June 9 – No class, instructor gone
- June 16 & 20 – No class – midterm week
- June 30 – No class, holiday
- July 2 (Wednesday) - extra class to makeup for holidays

Assessment

ECE 458 - Undergraduate

- 0% - Pre-quiz – feedback for the instructor
- 0% - Lecture quizzes – if I have time…
- 30% - Homework assignments
- 10% - Activities
- 2% - Midterm – mostly for feedback, >50% correct pass
- 58% - Final exam, closed book

ECE 750 - Graduate

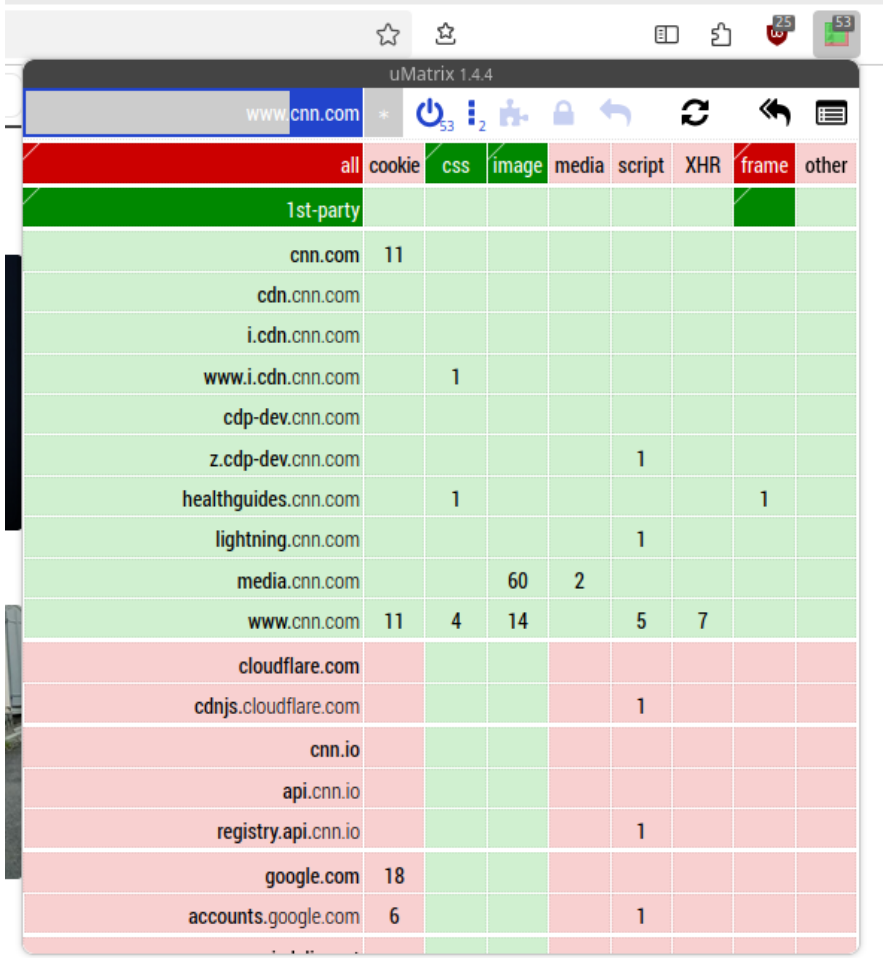
- 0% - Pre-quiz – feedback for the instructor
- 0% - Lecture quizzes – if I have time…
- 30% - Homework assignments
- 5% - Activities
- 1% - Midterm – mostly for feedback, >50% correct pass
- 54% - Final exam, closed book
- 10% - Project

Project (Masters Only)

- Select an Internet of Things device
- Breakdown their claims using class concepts
- Test the security IoT device – how do you know it is providing the security guarantees?

Activities

- Short activities to get you some minor but important practical experience
  - Too many students last year didn't realize that client side JavaScrit can be changed
- Activity can be done in groups
- Self-reflection writing must be done individually
- Activity content can appear on exams



UMatrix plugin for cnn.com

Late policy

- 10% lost per day up till 10 days late, weekend days count.
  - An assignment due on Monday that is submitted on Wednesday has the mark of: marks * 0.8

Academic dishonestly

- See the official policy of the University and on Outline
- Please don't cheat, copy other students, or turn in work that is not your own
- Assignments will have clearly marked areas where you can collaborate
  - Normally the VM setup portion
  - Other learning resources, like games, will sometimes be provided to support you learning from others

Standard security course advisory

- Nothing here is intended as an incitement to hack, crack, or otherwise break into computer systems!
- Breaking into systems to “demonstrate” security problems at best causes a headache to overworked sysadmins, and at worst compromises systems for many users and could lead to **prosecution**.
- If you spot a security hole in a running system, **don’t exploit it**, instead consider contacting the relevant administrators confidentially.

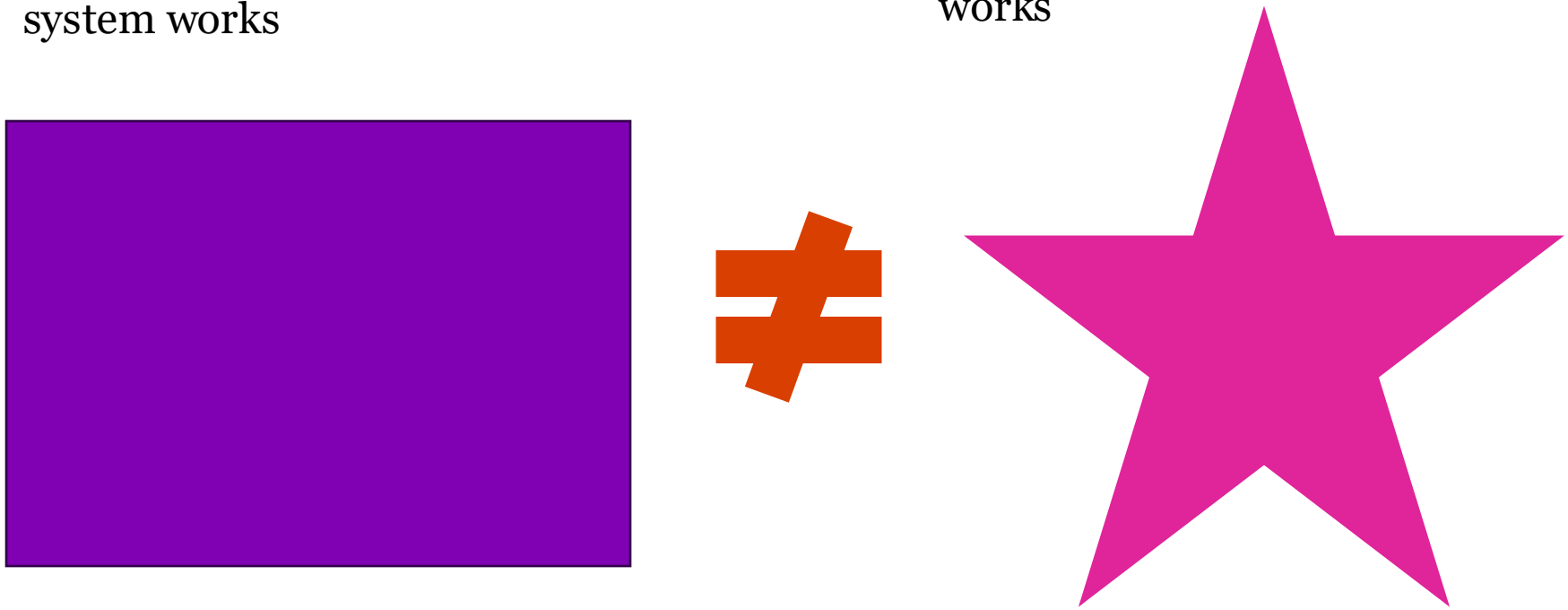
Responsible security experiments

- **If you want to experiment** with security holes, play with your own machine, or better, your own private network of machines.
- **Use VMs**: use virtualization: e.g., VMWare, VirtualBox, KVT/Xen/UML. The SEEDLab VMs are good for safe experimentation.
- **If you accidentally break into something:** tell me, ECE computing services, or University computing services right away. Universities are places of learning, and we respond very differently if you tell us than if we catch you.

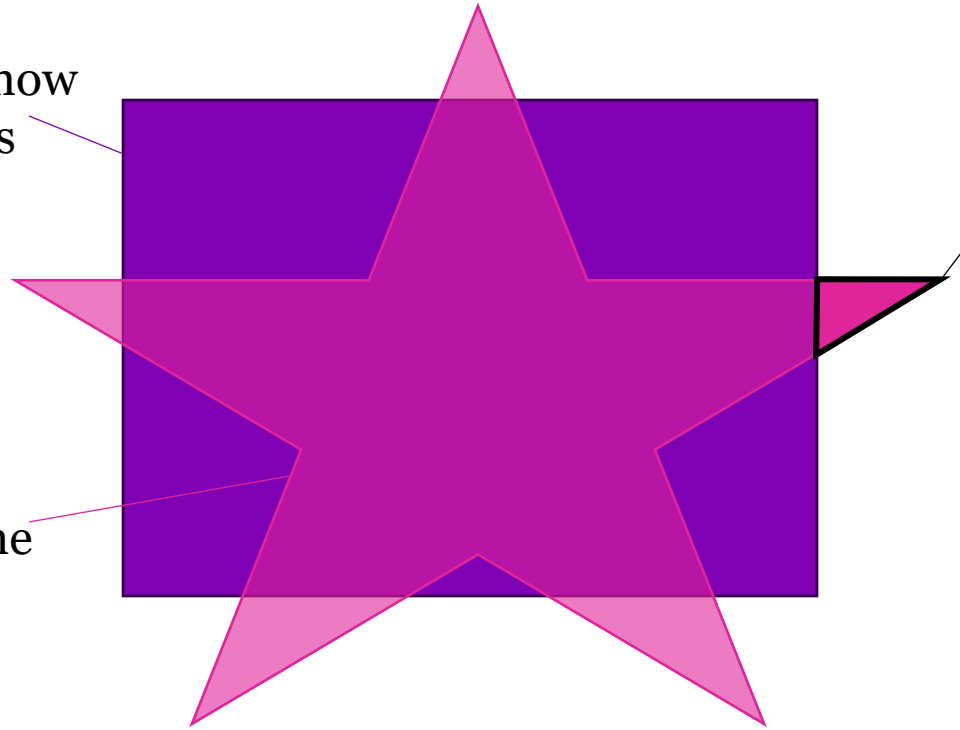
WHAT IS SECURITY?

Theoretically how the system works

Actually how the system works



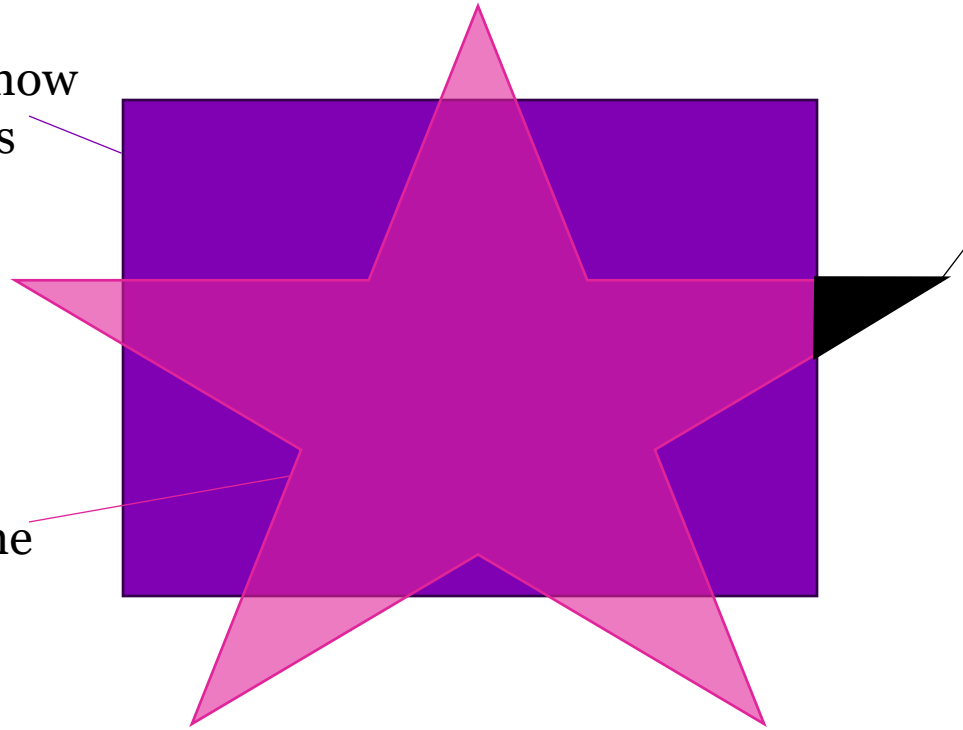
Theoretically how the system works



Hack potential: Get the system to do what the user wants but system designer did not intend.

Actually how the system works

Theoretically how the system works

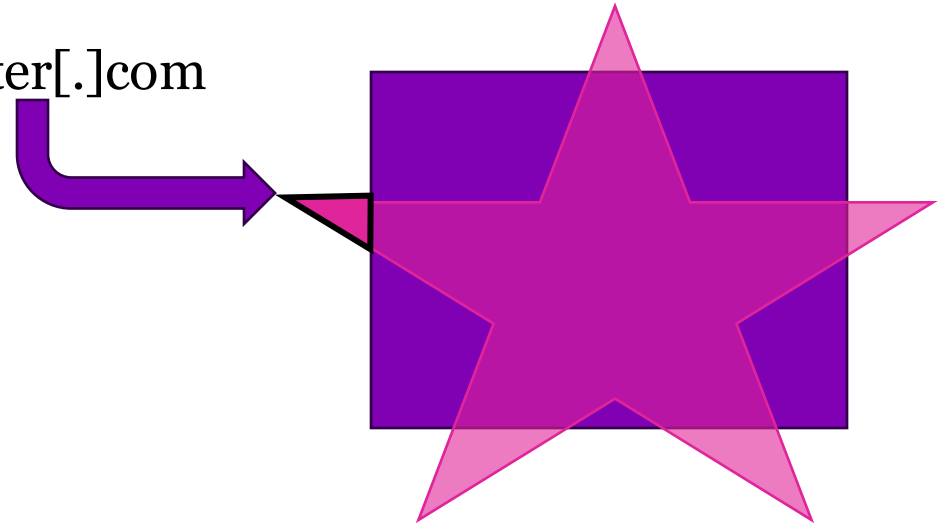


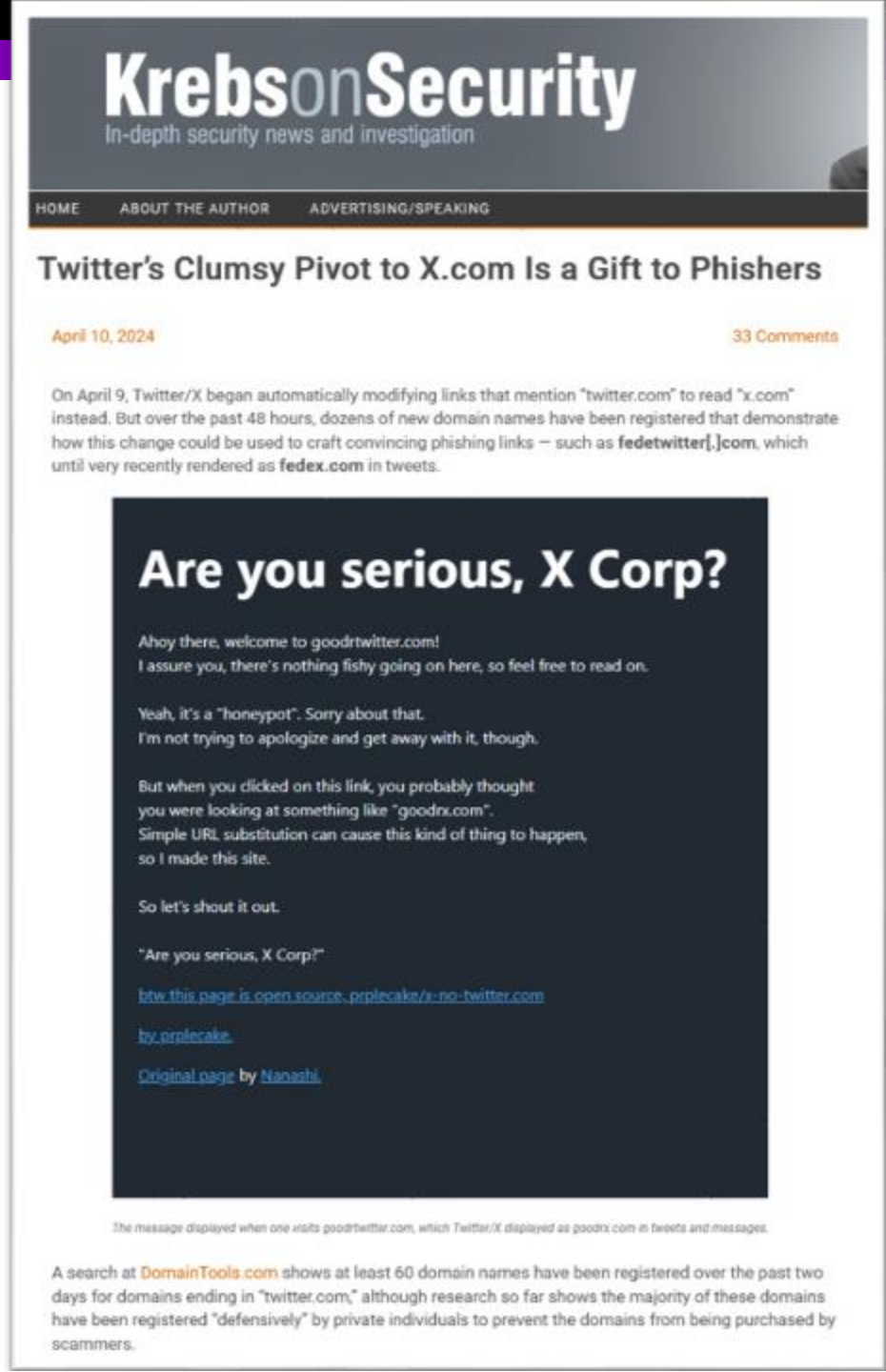
Actually how the system works

Security professional: Remove, block, defend, or otherwise prevent unintended harmful uses of a system.

Example: X rewrote all URLs containing "twitter" to instead say "x"

- Suddently
  - fedetwitter[.]com
- Is shown to users as
  - fedex[.]com
- But still actually goes to
  - fedetwitter[.]com





KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Twitter's Clumsy Pivot to X.com Is a Gift to Phishers

April 10, 2024 33 Comments

On April 9, Twitter/X began automatically modifying links that mention "twitter.com" to read "x.com" instead. But over the past 48 hours, dozens of new domain names have been registered that demonstrate how this change could be used to craft convincing phishing links — such as **fedetwitter[.]com**, which until very recently rendered as **fedex.com** in tweets.

Are you serious, X Corp?

Ahoy there, welcome to goodrtwitter.com!
I assure you, there's nothing fishy going on here, so feel free to read on.

Yeah, it's a "honeypot". Sorry about that.
I'm not trying to apologize and get away with it, though.

But when you clicked on this link, you probably thought
you were looking at something like "goodrx.com".
Simple URL substitution can cause this kind of thing to happen,
so I made this site.

So let's shout it out.

"Are you serious, X Corp?"

btw this page is open source. prplecake/x-no-twitter.com

by prplecake.

Original page by Nanashi.

The message displayed when one visits goodrtwitter.com, which Twitter/X displayed as goodrx.com in tweets and messages.

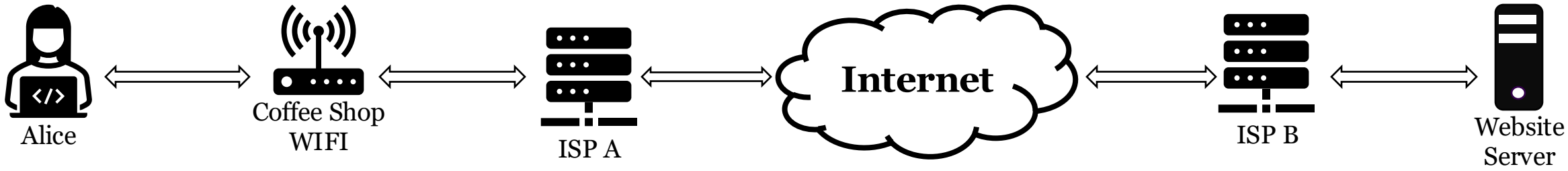
A search at DomainTools.com shows at least 60 domain names have been registered over the past two days for domains ending in "twitter.com," although research so far shows the majority of these domains have been registered "defensively" by private individuals to prevent the domains from being purchased by scammers.

Think-pair-share

- **Think** quietly to yourself for 1 minute
- **Pair** with your neighbor for 3 minutes
- **Share** with the class – group discussion

Sample connection: Alice loads a website

Alice visits: http://example.com

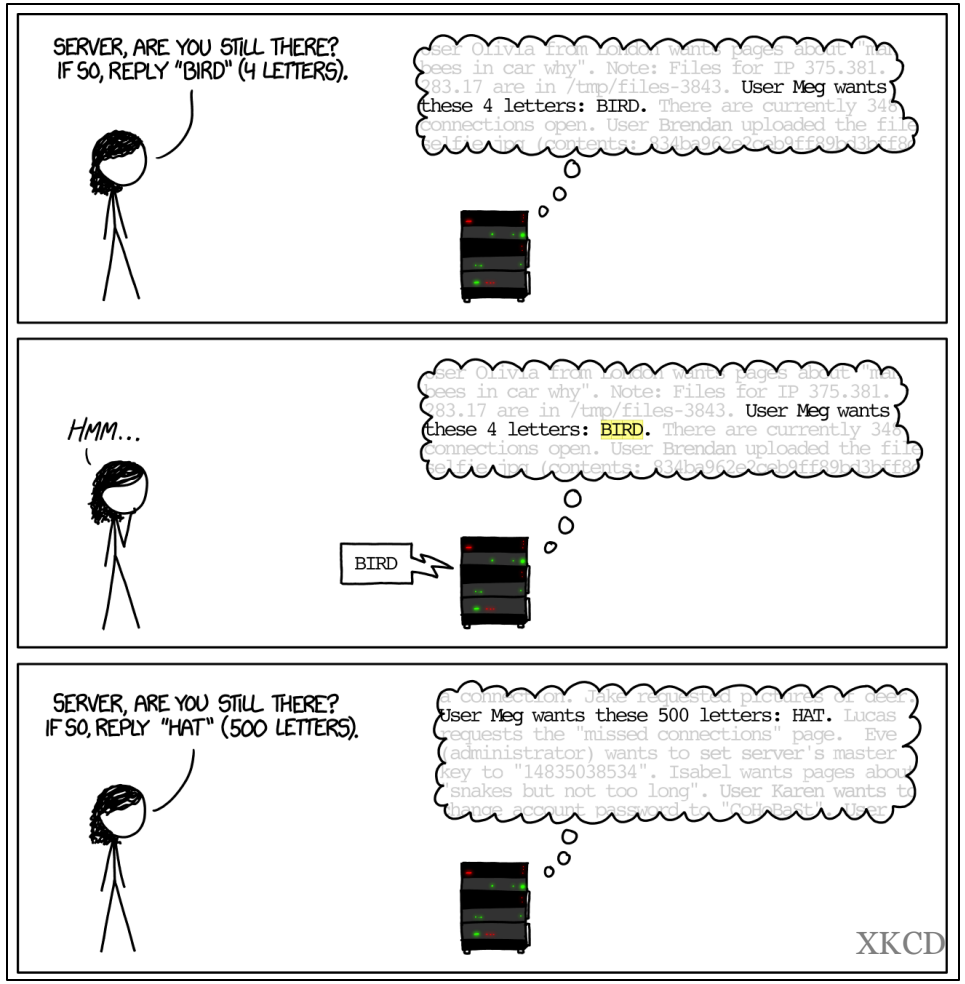


For each of the above connection points, can they learn:

1. The name and/or IP address of the website Alice is visiting
2. The content of the webpage Alice is viewing
3. Alice's Operating System (Linux, Windows, Apple)

DEFINITION OF SECURITY

Computer security is a broad topic



BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

TikTok CEO Shou Zi Chew's Congress showdown: Five takeaways

23 March 2023

Share

By James Clayton, BBC North America technology reporter

Watch: 'Psychological warfare': US politicians grill TikTok boss

Bruising, damaging, relentless. TikTok CEO Shou Zi Chew faced four-and-a-half hours of questioning at a US congressional hearing on Thursday.

As one congressman pointed out, some people run marathons quicker than that.

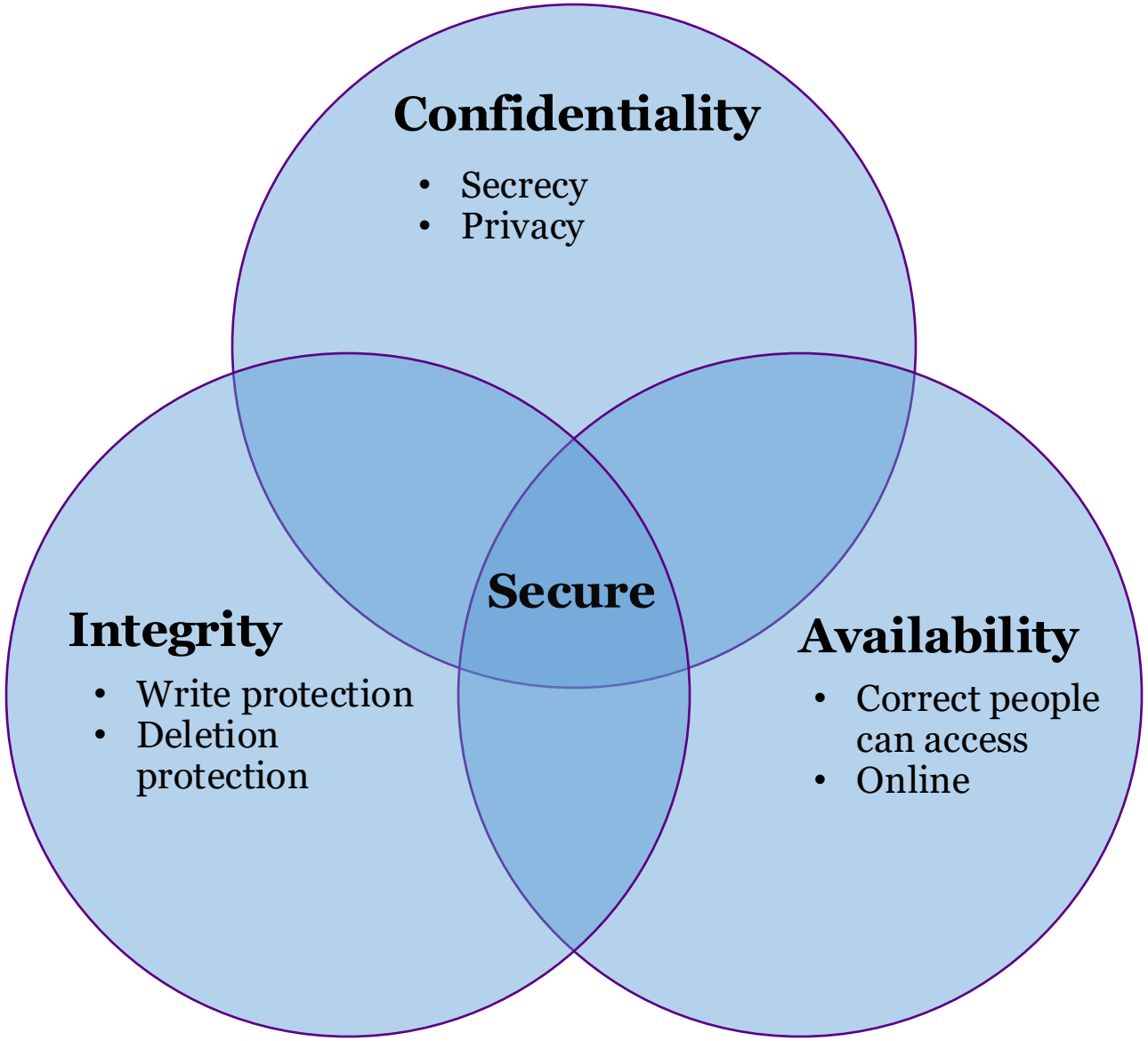
Mr Chew will certainly be feeling it, after a torrid time giving evidence. Many tech execs have stood before Congress, and they often don't get an easy ride.

What is Computer Security?

- **Security** is about protecting assets.
- **Computer Security** concerns assets of computer systems: the information and services they provide.
- Just as real-world physical security systems vary in their security provision (e.g., a building may be secure against certain kinds of attack, but not all), so computer security systems provide different kinds and amounts of security.
- Computer security is quite vast in scope, touching on many areas besides computer science. In this course we will study the fundamentals , some current internet technologies, and a little bit about engineering and management aspects.

Defining Security - CIA

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.

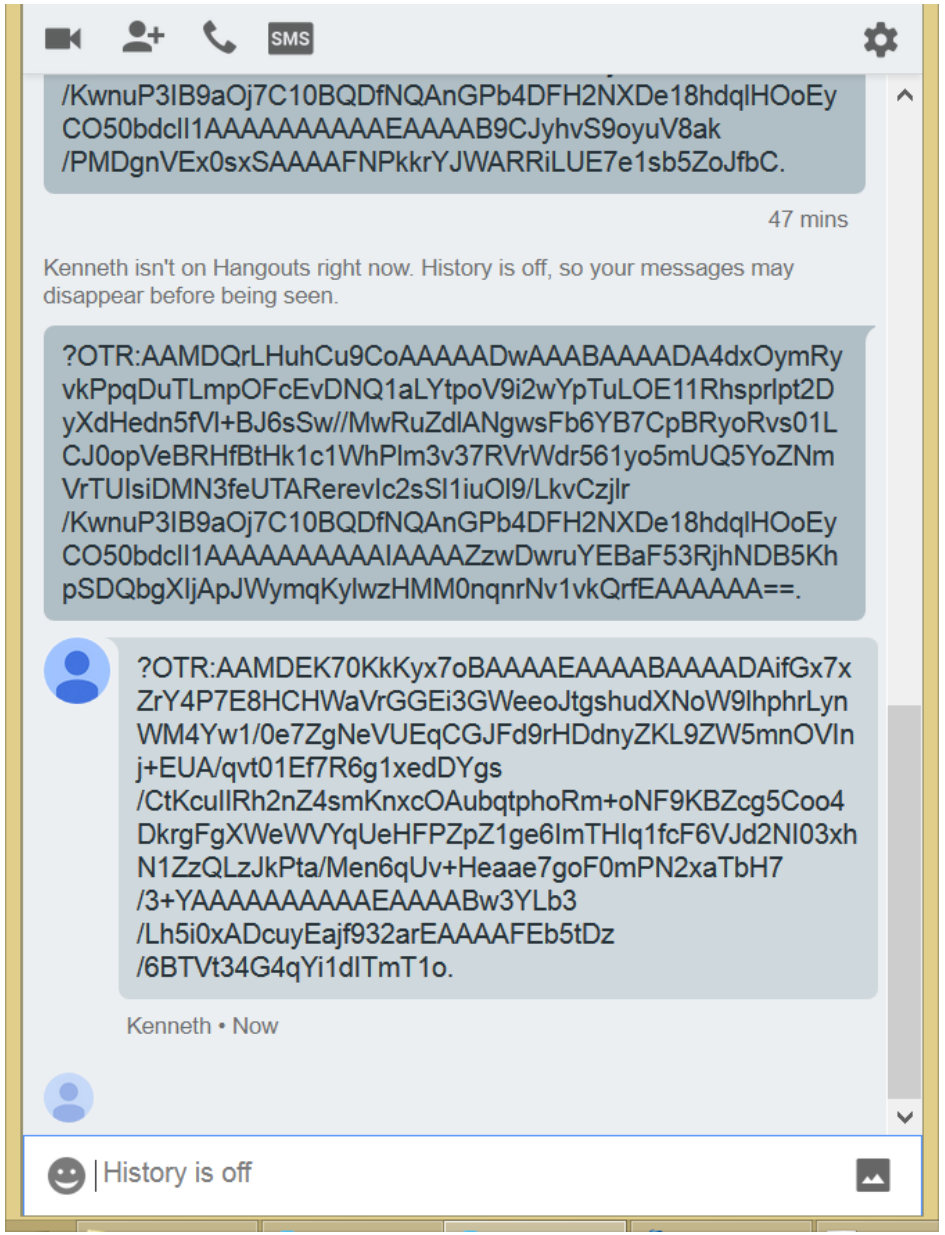


Security properties to ensure

Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

Confidentiality

- **Confidentiality** is characterized as preventing the unauthorized reading of data, when considering access control systems.
- Unauthorized learning of information.
- The GChat on the right is encrypted. How much can you learn from it anyway?



Showing security camera footage to wrong people

- “For 40 minutes, as many as 2,300 people … may have been able to see 10 stranger’s feeds”

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

WYZE WOES —

“So violated”: Wyze cameras leak footage to strangers for 2nd time in 5 months

"In some cases an Event Video was able to be viewed."

SCHARON HARDING - 2/19/2024, 4:03 PM

Frustrated customers

This is the second time that something like this has happened to Wyze customers in five months. In September, some Wyze users reported seeing feeds of cameras that they didn't own via Wyze's online viewer. Wyze claimed that for 40 minutes, as many as 2,300 people who were logged in to the online viewer may have been able to see 10 strangers' feeds. The company blamed this on a "web caching issue" and said that it deployed "numerous technical measures" to prevent the problem from repeating, including limiting account permissions, updating company policies and employee training, and hiring an external security firm for penetration testing.

In 2022, security firm Bitdefender disclosed security vulnerabilities with Wyze cameras that could allow people to access feeds from cameras they didn't own and the contents of strangers' camera SD cards. The vulnerability required the hacker to have been on the same network as the hacked device at some point; however, long-time users still disowned Wyze for not acting on this information or making the information public for years. In March, Wyze settled [PDF] a proposed class action regarding the vulnerabilities; terms weren't disclosed.

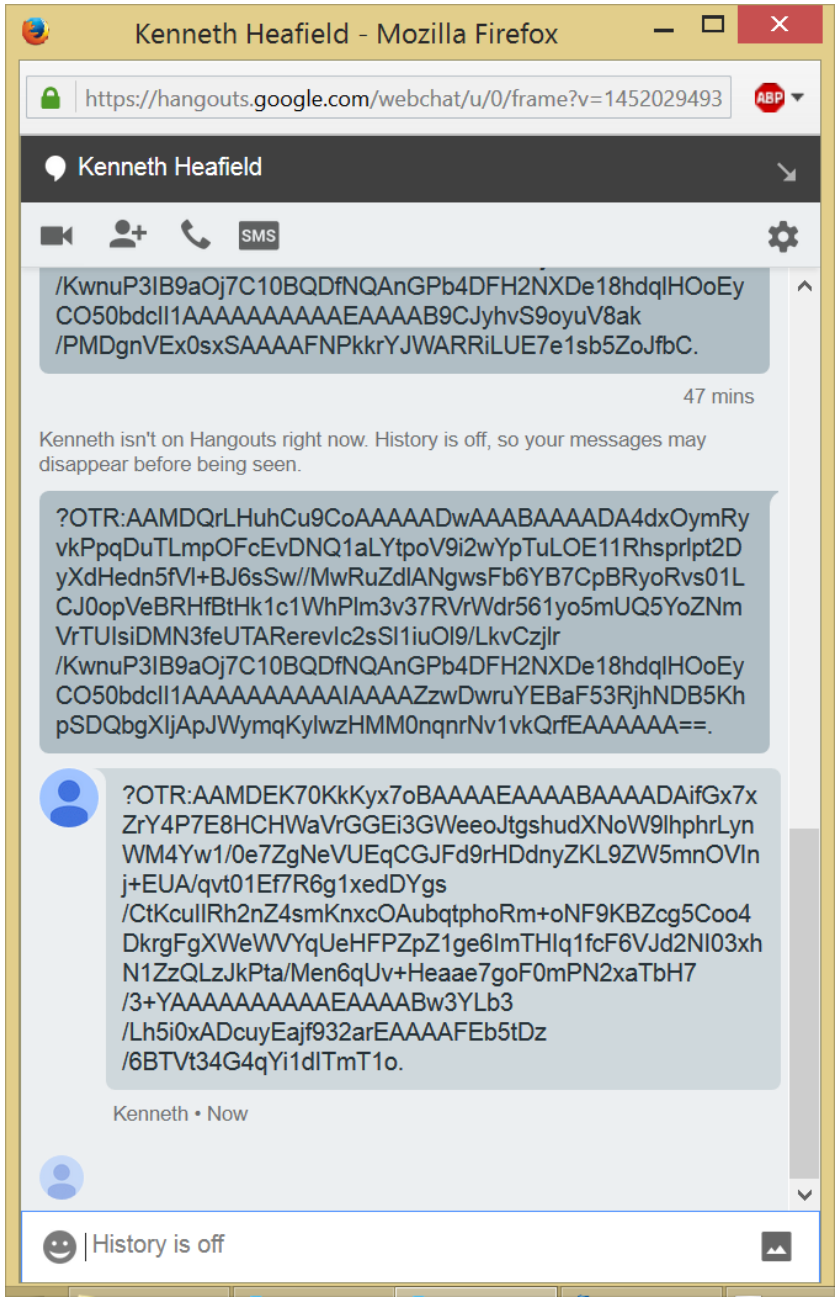
This all gives customers even more reason to be upset about the latest incident. Some Wyze users remain perturbed by the budget smart camera company's announcement. As a user going by FlyPenFly said on the WyzeCam subreddit:

> I hope you have some heads rolling because the already damaged brand is now practically worthless. I've been with you guys from the start but I'm just shocked at the level of hubris and incompetence from a company trying to compete in this crowded space. The savings aren't worth the squeeze here.

Understandably, users who were affected seem disturbed by the news. For example, a Reddit user going by H3H3ather wrote:

Integrity

- Data has not been maliciously altered.
- Integrity can have different meanings, in computer security we are primarily concerned with the unauthorized writing or altering of data.
- Examples:
  - Removing a record from a system.
  - An on-line payment system alters an electronic check to read £10000 instead of £100.00



TikTok: US Congress considers ban

“To protect Americans from the threat posed by certain foreign adversaries using current or potential future social media companies that those foreign adversaries control to surveil Americans, learn sensitive data about Americans, or **spread influence campaigns, propaganda, and censorship**.

117TH CONGRESS
2D SESSION

S. _____

To protect Americans from the threat posed by certain foreign adversaries using current or potential future social media companies that those foreign adversaries control to surveil Americans, learn sensitive data about Americans, or spread influence campaigns, propaganda, and censorship.

IN THE SENATE OF THE UNITED STATES

Mr. RUBIO introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To protect Americans from the threat posed by certain foreign adversaries using current or potential future social media companies that those foreign adversaries control to surveil Americans, learn sensitive data about Americans, or spread influence campaigns, propaganda, and censorship.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Averting the National Threat of Internet Surveillance, Oppressive Censorship

Availability

- Data or services are accessible as expected.
- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infection with a debilitating virus).
- Denial of Service (DOS) threats are the most common form of an Availability threat.

CNN Business Markets Tech Media Calculators Videos

Taylor Swift fans irate at Ticketmaster as huge tour pre-sale demand snarls site

By Jordan Valinsky, CNN Business
2 minute read · Updated 1:29 PM EST, Tue November 15, 2022

New York (CNN Business) — There's some bad blood brewing between Taylor Swift fans and Ticketmaster.

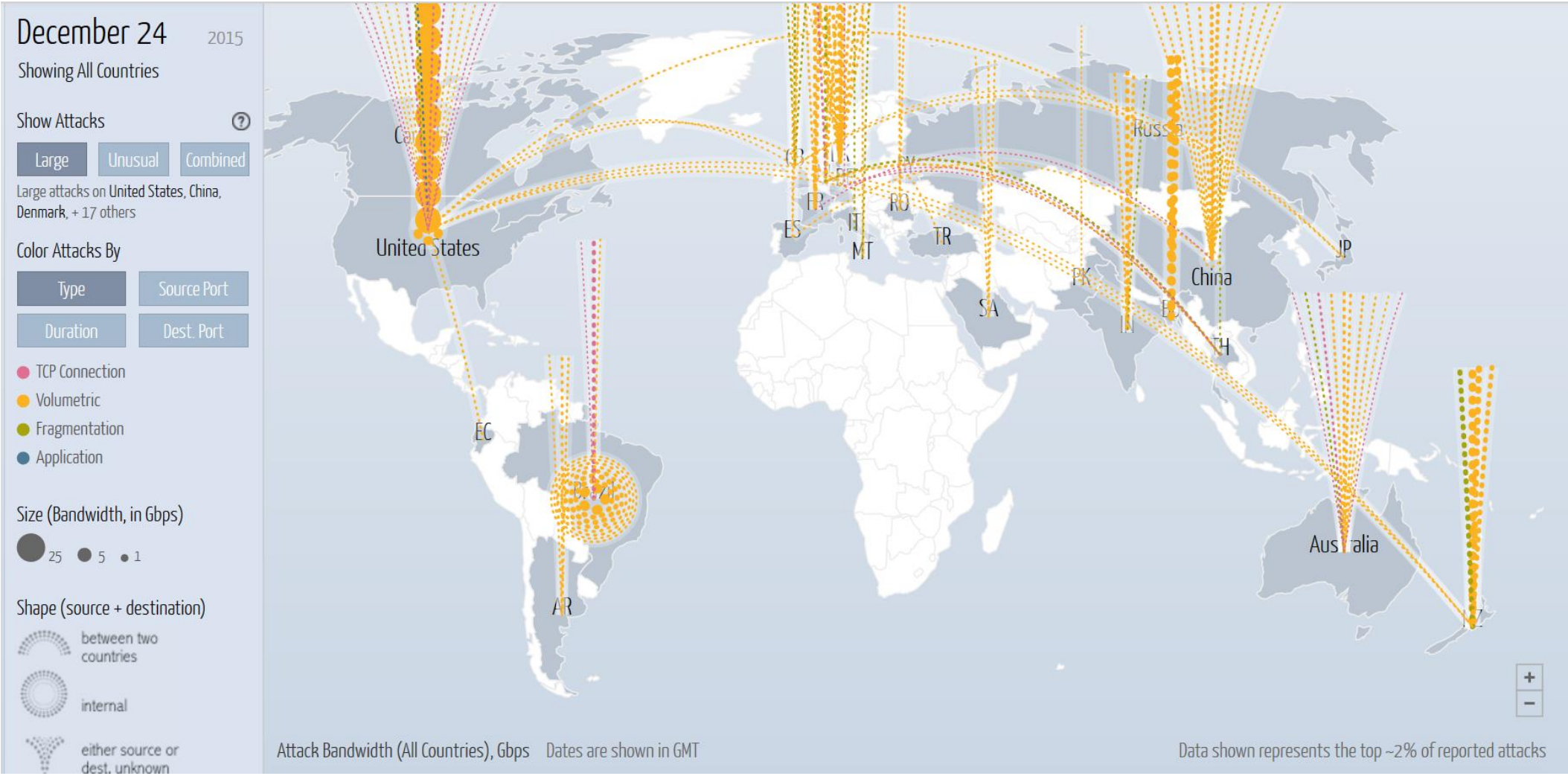
Pre-sales for a handful of dates on the singer's new tour began Tuesday. But infuriated fans report the ticketing website appeared to crash or freeze during purchase. Customers turned to Twitter to complain about Ticketmaster not loading or allowing them to access tickets, despite having a pre-sale code for verified fans.

"I got a code and am logged in to the correct account but it's saying I'm not verified?! What do I do?," a fan wrote on Twitter. Others echoed that complaint, with some calling on Ticketmaster to "FIX THIS."

However, Ticketmaster told CNN Business that the "site is not down" and that "people are actively purchasing tickets."

Ticketmaster issued a follow up statement Tuesday afternoon on Twitter, writing that "there has been historically unprecedented demand with millions showing up" to buy tickets for Swift's tour. It told customers still waiting in the virtual queue that it is moving and to "hang tight."

Availability: DigitalAttackMap



Accountability

- Actions are recorded and can be traced to the party responsible.
- If prevention methods and access controls fail, we may fall back on detection: keeping a secure audit trail is important so that actions affecting security can be traced back.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

CHARGED —

Prosecutor charges former phone company employee in SIM-swap scheme

Charges filed as soaring cryptocurrency prices drive increase in SIM swapping crimes.

DAN GOODIN - 2/13/2021, 9:00 AM

Getty Images

Enlarge

A former phone company worker has been charged with conspiracy to commit fraud for allegedly using his access to customer account data to take over the phone numbers of 19 customers, including at least one cryptocurrency holder.

Stephen Daniel DeFiore of Brandon, Florida, received about $2,325 between October 20, 2018, and November 9, 2018 in exchange for swapping the targeted customers' SIM cards with ones belonging to a co-conspirator, prosecutors in New Orleans said earlier this week. For each SIM swap, the co-conspirator sent DeFiore the customer's phone number, a four-digit PIN, and a SIM card number to which that phone number was to be swapped, prosecutors said.

The charges come eight months after federal prosecutors charged Richard Yuan Li of Hercules, California, with conspiracy to commit fraud for his alleged role in a SIM swap scam that targeted at least twenty people. Li was in possession of an iPhone 8 which the number of at least one of DeFiore's victims was routed to, prosecutors said.

The alleged victim was a New Orleans-area medical doctor with cryptocurrency accounts at exchanges including Binance, Bittrex, Coinbase, Gemini, Poloniex, ItBit, and Neo Wallet. Li and his co-conspirators then

Authentication

- Accurate linking of an access token to a person or a property.
- Authentication is necessary for allowing access to some people but denying access to others.
- Authentication typically characterized as:
  - Something you **have** – an entry card, your phone
  - Something you **know** – a password, your mother's maiden name
  - Something you **are** – a signature, fingerprint, way of typing

The Guardian

Int

News | Opinion | Sport | Culture | Lifestyle

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

Signal group chat leak

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

Mike Waltz (left) and Jeffrey Goldberg. Composite: AP/Reuters

that started during the 2024 campaign and went unnoticed until Waltz created the group chat last month.

"According to the White House, the number was erroneously saved during a "contact suggestion update" by Waltz's iPhone, which one person described as the function where an iPhone algorithm adds a previously unknown number to an existing contact that it detects may be related."

DATA BREACH

A classic data breach

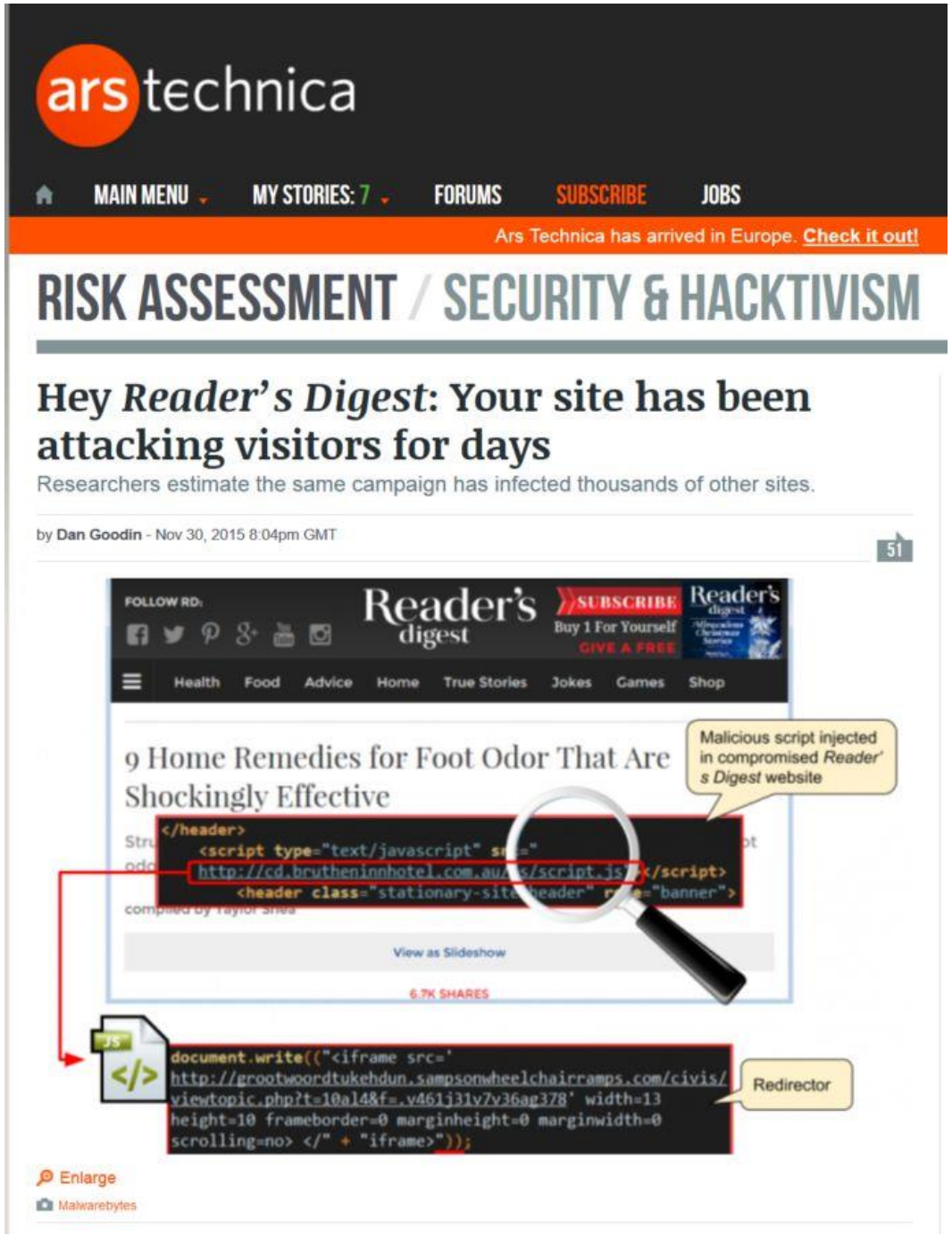
1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in their user name and password.
3. Malicious site collects the password and reassures the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses the user name and password to download sensitive files.

A classic data breach

1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.

- **Prevention**: detect phishing URLs and mark as spam, train employees to notice phishing, identify offsite access of sensitive files and block, encrypt files so useless if leaked.
- **Detection**: Identify that sensitive files have been (past tense) accessed from off site, employee sends email about suspicious email.
- **Response**: Change user's password, prevent further access, notify CTO, notify insurer, begin post-breach plan.

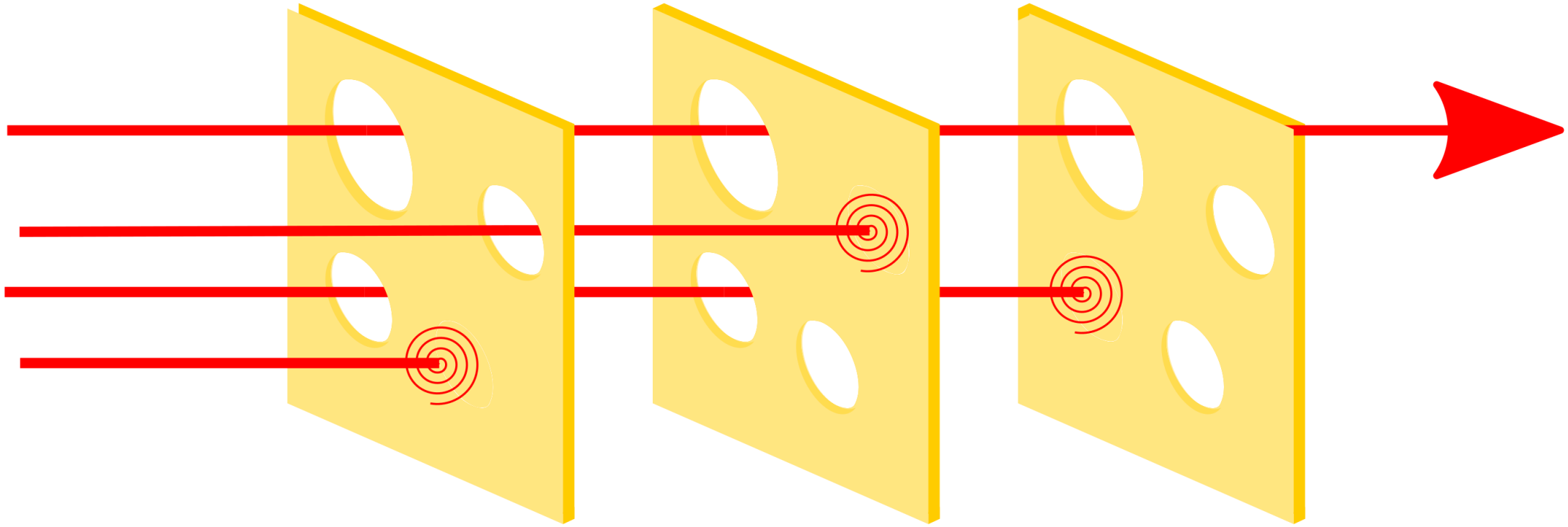
Sites are sometimes the last to know they have been compromised



A classic data breach

1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.
5. Malicious actor identifies an old version of software is running and finds an exploit for it.
6. They use the exploit to trick the system into giving them more access.
7. Using elevated privileges they install ransomware and download sensitive files.
8. Wait for ransomware to spread into the backup files.
9. Lock down the whole system.

Swiss Cheese Model



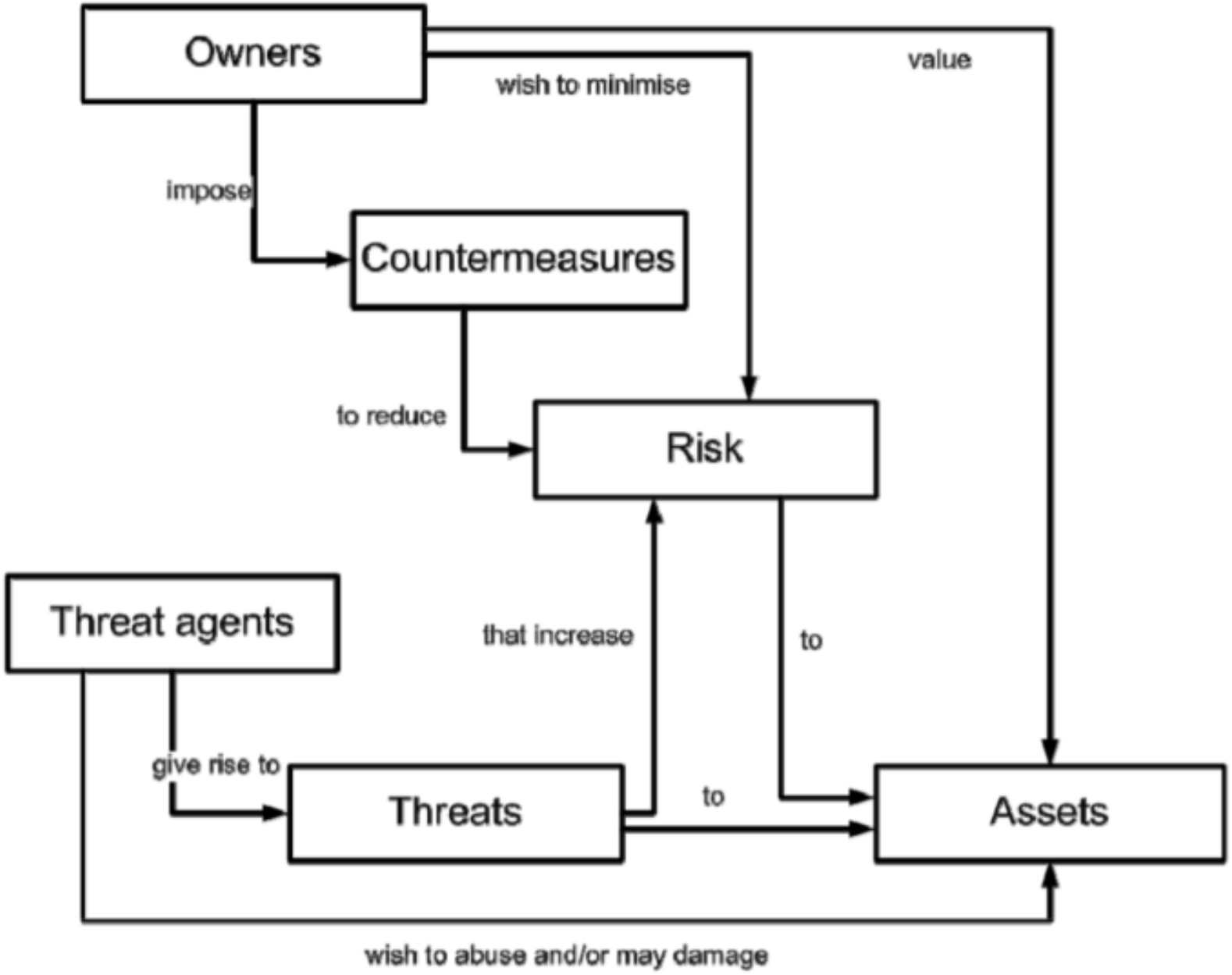
SECURITY CONCEPTS AND RELATIONSHIPS

“A system which is unspecified can never be wrong, it can only be surprising.”

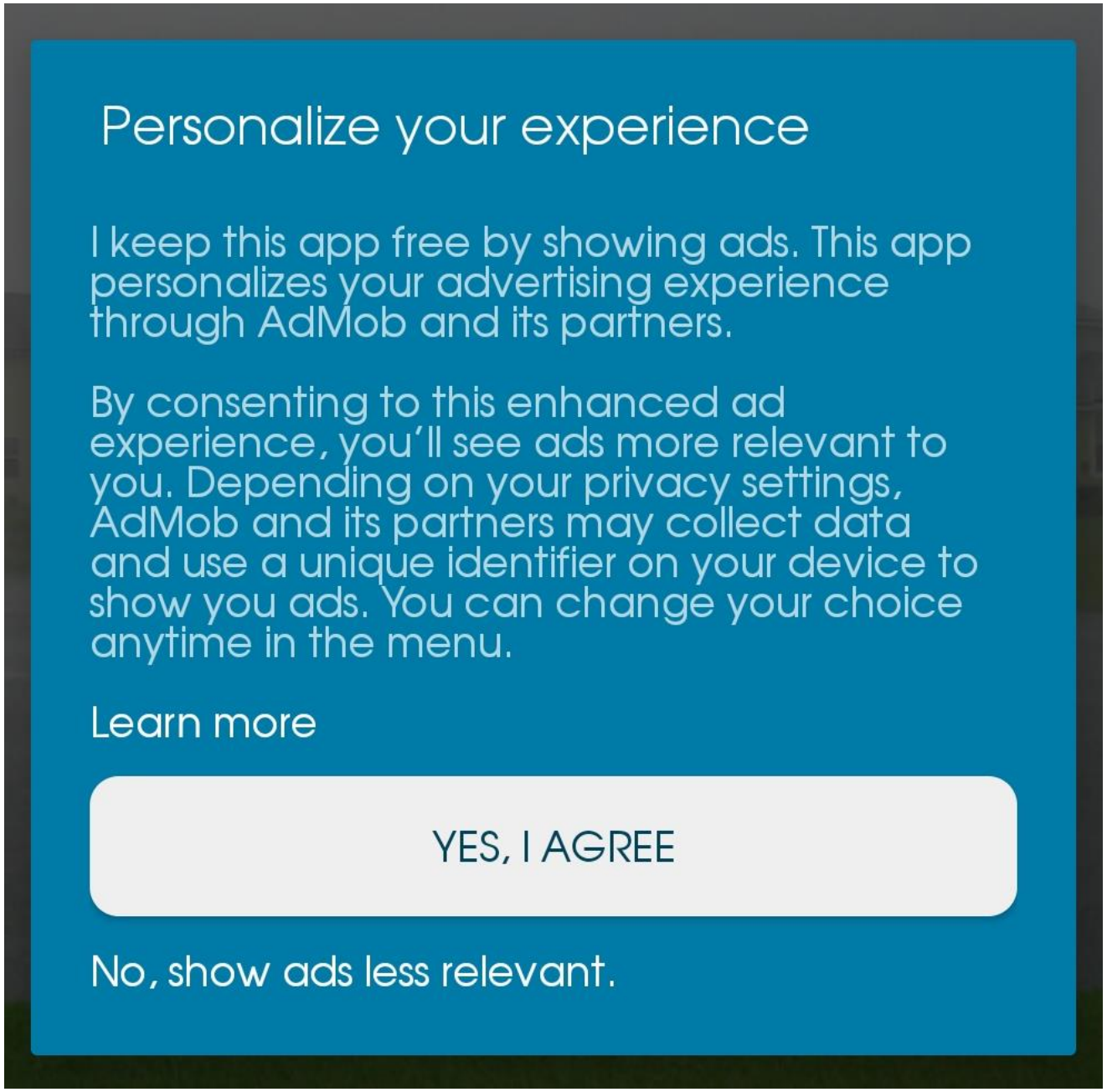
Common Criteria for Information Technology Security Evaluation (CC)

- Security is about protecting assets from threats.
- Threats are the potential for abuse of assets.
- **Owners** value assets and want to protect them.
- **Threat agents** also value assets and seek to abuse them.
- Owners analyze threats to decide which apply; these risks can be costed.
- This helps select countermeasures, which reduce vulnerabilities.
- Vulnerabilities may remain leaving some residual risk; owners seek to minimize that risk, within other constraints (feasibility, expense).

Security concepts and relationships
-- CC V3.1 R4

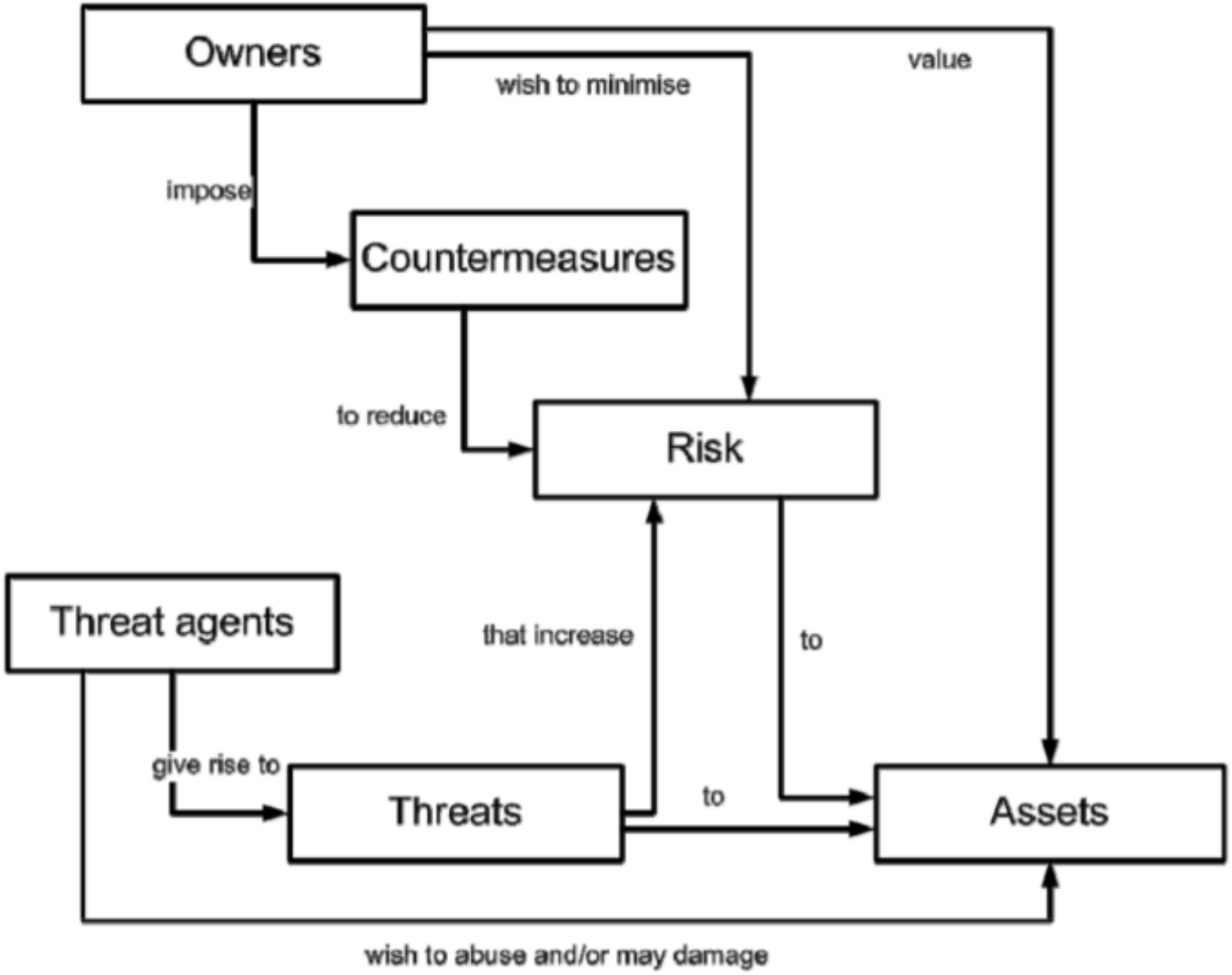


Example: Behavioral Advertising



Example: Behavioral Advertising

- **Asset**: User behavior
- **Owner**: The user
- **Threat agent**: Advertisers
- Risks:
  - Malware
  - Tracking
  - Discriminatory pricing



EXAMPLE ATTACKS

Verizon MITMed traffic and added cookies to all connections so that advertisers could track better and link data to demographics Verizon provided.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Verizon's zombie cookie gets new life

Verizon's tracking supercookie joins up with AOL's ad tracking network.

JULIA ANGWIN AND JEFF LARSON, PROPUBLICA - 10/7/2015, 8:00 AM

65

Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.

FURTHER READING
Verizon will now let users kill previously indestructible tracking code

That means AOL's ad network will be able to match millions of Internet users to their real-world details gathered by Verizon, including "your gender, age range and interests." AOL's network is on 40 percent of websites, including on ProPublica.

AOL will also be able to use data from Verizon's identifier to track the apps that mobile users open, what sites they visit, and for how long. Verizon purchased AOL earlier this year.

On-device MITM Attack

Lenovo shipped computers with software that used MITM to inject ads into all network traffic.

ars TECHNICA

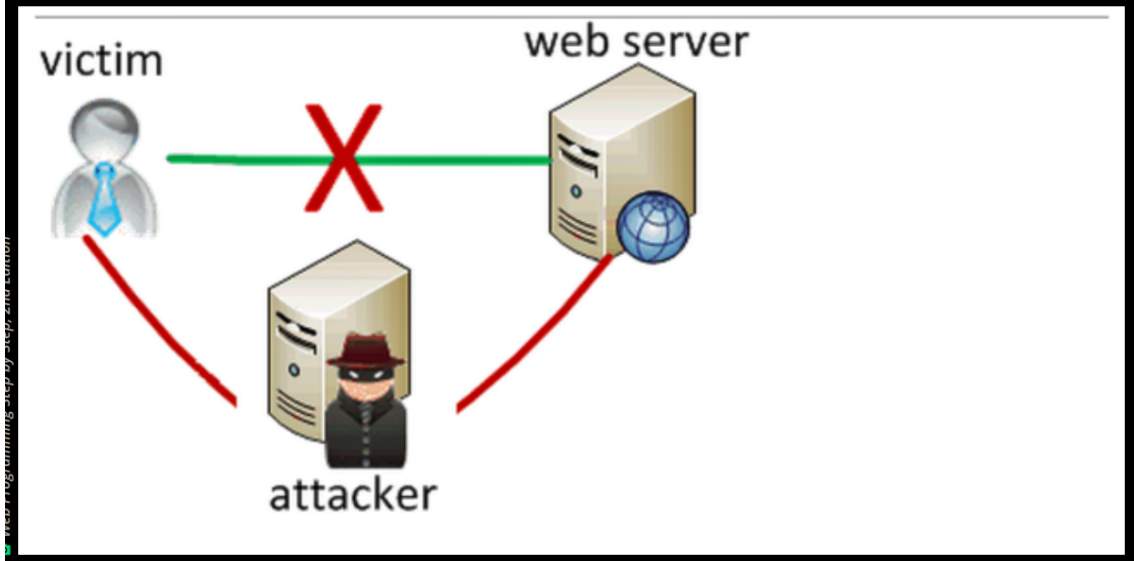
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - 2/19/2015, 11:36 AM



333

Lenovo is selling computers that come preinstalled with adware that hijacks encrypted Web sessions and may make users vulnerable to HTTPS man-in-the-middle attacks that are trivial for attackers to carry out, security researchers said.

The critical threat is present on Lenovo PCs that have adware from a company called Superfish installed. As unsavory as many people find software that injects ads into Web pages, there's something much more nefarious about the Superfish package. It installs a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America, Google, or any other secure destination on the Internet. Under such a scenario, PCs that have the Superfish root certificate installed will fail to flag the sites as forgeries—a failure that completely undermines the reason HTTPS protections exist in the first place.

Questions