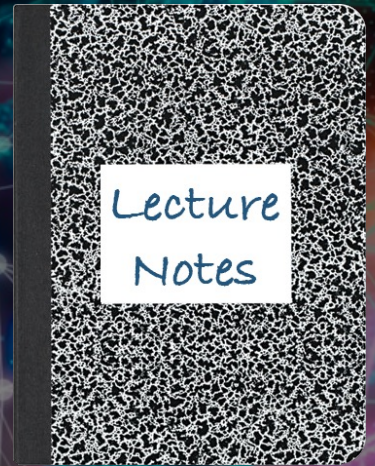


CS 419: Computer Security

Week 1: Part 1

Introduction

Paul Krzyzanowski



© 2022-2024 Paul Krzyzanowski. No part of this content may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

What is security?

security

noun se·cu·ri·ty \si-'kyūr-ə-tē\

the quality or state of being secure: such as

a : freedom from danger : safety

b : freedom from fear or anxiety

c : freedom from the prospect of being laid off
<job *security*>

What is computer security?

Keeping systems, programs, and data "safe"

The **CIA Triad***:

1. Confidentiality

2. Integrity

3. Availability

**No relationship to the Central Intelligence Agency*

Confidentiality

- **Keep data & resources hidden**
 - Data will only be shared with authorized individuals
 - Sometimes – conceal the existence of data or communication
- **Traditional focus of computer security**
 - Usually accomplished with access control and encryption

Data confidentiality:

“The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”

– *RFC 4949, Internet Security Glossary*

Confidentiality – Privacy – Secrecy – Anonymity

Privacy

- Limit what information can be shared with others
- Control other's use of information about you
- Freedom from intrusion

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

*See: HIPAA, personal information, Privacy Act of 1974
RFC 4949, Internet Security Glossary*

Privacy is a reason for confidentiality

Anonymity: conceal the individual's identity

Secrecy: hide the existence of information

Privacy is increasingly harder to attain

- **“Free” services**
 - Facebook, Google, X, LinkedIn, Instagram, TikTok, ...
 - Information collection, browser cookies to track web access
- **More data is online and widely accessible**
 - No need to go to town hall to get real estate transactions
- **Phone companies know every place you go**
- **Big data analytics**
 - It's increasingly easy to correlate data:
Credit card spending, travel, jobs, marriages/divorces, kids, cars, ...

This can be good and bad

Privacy & data mining ... on a national level

- **U.S. credit scores**

- Credit reporting companies track employment, spending, home ownership, loan repayment, ...
- Credit scores affect the ability to borrow money, buy a home

- **China's Social Credit System**

- Track the trustworthiness of everyday citizens, corporations, and government officials
- Track behavior: frivolous spending, major & minor infractions
- Boost public confidence and fight problems like corruption and business fraud
- Has not yet become a single score but a collection of data

- **AI simplifies data analysis**

- UNESCO adopted a Recommendation on the Ethics of AI in 2021
 - "AI systems should not be used for social scoring or mass surveillance purposes"*

Integrity

- The trustworthiness of the data or resources
- Preventing unauthorized changes to the data or resources

Data integrity

Property that data has not been modified or destroyed in an unauthorized or accidental manner

Origin integrity & Recipient integrity

Authentication

System integrity (Functional integrity)

The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

Integrity is often more important than confidentiality!

Availability

- Being able to use the data or resources
- Property of a system being accessible and capable of working to required performance specifications

Turning off a computer provides confidentiality & integrity but hurts availability

Denial of Service (DoS) attacks target availability

Amazon Outage Took Citi Bike Offline At Height Of Rush Hour



Security isn't always about adversaries attacking ... sometimes it's services failing

Jake Offenhardt • December 22, 2021

Citi Bike riders were left stranded on Wednesday after an outage at an Amazon data center knocked out service to the bike-share system during the height of the morning rush hour.

The disruption began shortly after 7:00 a.m., sparking complaints and confusion from monthly subscribers unable to unlock a bike. A spokesperson for Lyft, the Citi Bike parent company, said stations were beginning to come back online as of 9:20 a.m., though some riders continued to report issues.

Outside Bellevue Hospital in Manhattan on Wednesday morning, would-be commuters stood in front of a docking station fruitlessly trying to connect to the bikes with their phones.



<https://gothamist.com/news/amazon-outage-took-citi-bike-offline-height-rush-hour>

University loses 77TB of research data due to backup error

BLEEPINGCOMPUTER

Sometimes it's human error

Bill Toulas • December 30, 2021

The Kyoto University in Japan has lost about 77TB of research data due to an error in the backup system of its Hewlett-Packard supercomputer.

The incident occurred between December 14 and 16, 2021 and resulted in 34 million files from 14 research groups being wiped from the system and the backup file.

After investigating to determine the impact of the loss, the university concluded that the work of four of the affected groups could no longer be restored. All affected users have been individually notified of the incident via email, but no details were published on the type of work that was lost.

At the moment, the backup process has been stopped. To prevent data loss from happening again, the university has scrapped the backup system and plans to apply improvements and re-introduce it in January 2022.

<https://www.bleepingcomputer.com/news/security/university-loses-77tb-of-research-data-due-to-backup-error/>

Terabytes of Deleted Case Data Forces Dallas PD to Revise Policy



A Dallas Police employee accidentally deleted 22 TBs of case files when trying to migrate data between servers. Officials say they're now working to recover what they can and prevent future issues.

Jule Pattison-Gordon • August 17, 2021

In Dallas, at least one murder trial has been delayed after a police employee accidentally destroyed 8 terabytes of digital case files and materials during a routine data migration process gone wrong.

A Dallas Police Department (DPD) employee attempting to move older case files out of a cloud-based archive and onto an on-premise server housed in the city's data center accidentally deleted 22 terabytes worth of files, the DPD told media in an emailed statement.

Police recovered 14 terabytes, but DPD believes the remaining 8 terabytes are “permanently deleted and unrecoverable from the archive location,” per its statement.

The impacted files include audio recordings, case notes, images, videos and other materials, the DPD said. According to an Aug. 11 memo released by the Dallas County Criminal District Attorney's Office, the data loss affects prosecution of cases for which the offending event occurred before July 28, 2020.

Thinking about security

Security is not

- adding encryption
- ... or using a 512-bit key instead of a 64-bit key
- ... or changing passwords
- ... or setting up a firewall

It is a systems issue

- = Hardware + firmware + OS + app software + networking + people
- = Processes & procedures, policies, detection, forensics

“Security is a chain: it’s only as secure as the weakest link”
– Bruce Schneier

Security is hard

- **Software is complex**

- Windows 11: 60-100 million lines of code
- Google services comprise ~2 billion lines of code
- Linux distribution: over 200 million lines of code
 - Linux kernel: ~36M lines of code across 66,492 files
 - Linux kernel at the end of 2023: 74,198 commits from 5,006 different authors
 - 5.3 million lines of new and changed code



**Try to
find the bugs!**

- **Systems are complex**

- Lots of layers: microcode + firmware + OS + libraries + apps + devices
- Lots of elements: clients, servers, networks, embedded devices
- Interaction with cloud services
- Third-party components
- Complex interaction models, concurrency
- All parts are not always under the control of one administrator

- **Human factor**

- People make mistakes

Some big data breaches

Exfiltration

Exfiltration – getting data

Why steal data?

- **Corporate espionage:**
 - Strategy, schedules, employees, intellectual property
- **Obtaining credentials:**
 - Your login/password for your AT&T account might be the same as your Chase bank account
- **Extortion (ransomware):**
 - Threaten disclosure if not paid

Some big data breaches

- **CAM4** – March 2020 (data leak – exposed data due to misconfiguration)
 - Adult video site – 10.88 billion records
 - Full names, email, chat transcripts, payment logs, IP addresses
- **Microsoft** – January 2021
 - Attack on Exchange servers, affecting 60,000 companies worldwide
- **India Govt – Aadhaar database** – March 2018
 - Personal information of more than 1.6 billion Indian citizens stored in the world's largest biometric database leaked via website
 - Names, unique identity numbers, bank details, photos, thumbprints, retina scans
 - *Attacked again in July 2023 – 810+ million user accounts*
- **Verifications.io** – February 2019
 - Email validation service exposed 763 million unique addresses
 - Public MongoDB instance with no password
 - Names, phone numbers, dates of birth, genders
- **Yahoo** – October 2017
 - Three billion user accounts compromised
 - Names, security questions & answers

CAM4



yahoo!

Some big data breaches

- **Alibaba** – July 2022
 - 1.1 billion customer records from its cloud hosting servers
 - Names, phone numbers, physical addresses, criminal records
- **First American Financial** – 2019
 - 885 million customer records from its Title Insurance unit
 - *Attacked again in December 2023*
- **Facebook** – April 2019
 - Two 3rd-party app datasets exposed to the public Internet
 - Contains comments, likes, reactions, account names
 - 540 million users affected
- **Marriott** – November 2018
 - Data from about 500 million Starwood hotel customers from 2014-2016
 - Names, contact info, passport numbers, Preferred Guest numbers, etc.
 - Credit & debit card numbers and expiration dates from 100 million customers
- **Adult Friend Finder** – October 2016
 - 412.2 million accounts from 20 years of data from six databases
 - Names, email addresses, passwords



facebook



AdultFriendFinder®

COMB: largest breach of all time leaked cybernews online with 3.2 billion records

Bernard Meyer • February 12, 2021

It's being called the biggest breach of all time and the mother of all breaches: COMB, or the Compilation of Many Breaches, contains more than 3.2 billion unique pairs of cleartext emails and passwords. While many data breaches and leaks have plagued the internet in the past, this one is exceptional in the sheer size of it. To wit, the entire population of the planet is at roughly 7.8 billion, and this is about 40% of that.

However, when considering that only about 4.7 billion people are online, COMB would include the data of nearly 70% of global internet users (if each record was a unique person). For that reason, users are recommended to immediately check if their data was included in the leak. You can head over to the CyberNews personal data leak checker now.

...

So how did the COMB data leak happen?

On Tuesday, February 2, COMB was leaked on a popular hacking forum. It contains billions of user credentials from past leaks from Netflix, LinkedIn, Exploit.in, Bitcoin and more. This leak is comparable to the Breach Compilation of 2017, in which 1.4 billion credentials were leaked.

However, the current breach, known as “Compilation of Many Breaches” (COMB), contains more than double the unique email and password pairs. The data is currently archived and put in an encrypted, password-protected container.

<https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/>

The Mother of All Breaches (MOAB)

January 2024:
12 TB, 26 billion
records

Another indexed compilation of records from breaches and privately-sold databases

BRANDS WITH 100M+ LEAKED RECORDS

BRAND NAME	RECORDS LEAKED
Tencent	1.5B
Weibo	504M
MySpace	360M
Twitter	281M
Wattpad	271M
NetEase	261M
Deezer	258M
LinkedIn	251M
AdultFriendFinder	220M
Zynga	217M
Luxottica	206M
Evite	179M
Zing	164M
Adobe	153M
MyFitnessPal	151M
Canva	143M
JD.com	142M
Badoo	127M
VK	101M
Youku	100M

<https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/>

Ransomware attacks

- **CDK Global (serving car dealerships) – June 2024 – crippled car sales – \$25M**
- **Colonial Pipeline – May 2021 – Stopped fuel delivery – \$4.4M**
- **Costa Rican govt – April 2022 – shut down multiple govt systems - \$30M/day**
- **JBS Meats – May 2021 – Stopped meat delivery – \$11M**
- **Kronos – December 2021 – workforce mgmt software affected numerous companies**
- **Maersk – June 2017 – shipping company suffered ~\$300M in losses – 2 weeks to recover**
- **Acer – March 2021 – demanded \$50M**
- **Brenntag – chemical distribution – \$4.4M**
- **Kaseya – IT monitoring – 800-1500 businesses – demanded \$70M**
- **Quanta – contract manufacturing (Apple) – demanded \$50M**

Just a few recent security attacks

SonicWall Issues Critical Patch for Firewall Vulnerability Allowing Unauthorized Access

The Hacker News

Ravie Lakshmanan • August 26, 2024

SonicWall has released security updates to address a critical flaw impacting its firewalls that, if successfully exploited, could grant malicious actors unauthorized access to the devices.

The vulnerability, tracked as CVE-2024-40766 (CVSS score: 9.3), has been described as an improper access control bug.

"An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash," the company said in an advisory released last week.

<https://thehackernews.com/2024/08/sonicwall-issues-critical-patch-for.html>

RANSOMWARE American Radio Relay League Paid \$1 Million to Ransomware Gang

The American Radio Relay League (ARRL) says it paid out a \$1 million ransom after falling victim to ransomware in May 2024.

Ionut Arghire • August 26, 2024

The national association for amateur radio American Radio Relay League (ARRL) last week revealed that it paid out a \$1 million ransom after a disruptive May 2024 ransomware attack.

The attack occurred on May 15 and resulted in multiple systems within ARRL's internal network being encrypted, including desktops, laptops, and Windows and Linux servers.

Last week, the association revealed that the attackers had compromised its on-site systems and most cloud-based systems weeks before deploying file-encrypting ransomware, and that information purchased on the dark web was used for the intrusion.

...

ARRL also noted that the attackers demanded a multi-million-dollar ransom payment, but they eventually agreed to receive a \$1 million payment, as “their ransom demands were dramatically weakened by the fact that they did not have access to any compromising data.”

<https://www.securityweek.com/american-radio-relay-league-paid-1-million-to-ransomware-gang/>

Major Backdoor in Millions of RFID Cards Allows Instant Cloning

A significant backdoor in contactless cards made by China-based Shanghai Fudan Microelectronics allows instantaneous cloning of RFID cards used to open office doors and hotel rooms around the world.

Ryan Naraine • August 20, 2024

French security services firm Quarkslab has made an eye-popping discovery: a significant backdoor in millions of contactless cards made by Shanghai Fudan Microelectronics Group, a leading chip manufacturer in China.

The backdoor, documented in a research paper by Quarkslab researcher Philippe Teuwen, allows the instantaneous cloning of RFID smart cards used to open office doors and hotel rooms around the world.

Although the backdoor requires just a few minutes of physical proximity to an affected card to conduct an attack, an attacker in a position to carry out a supply chain attack could execute such attacks instantaneously at scale, Teuwen explained in the paper.

...

Security vulnerabilities that allow “card-only” attacks (attacks that require access to a card but not the corresponding card reader) are of particular concern as they may enable attackers to clone cards, or to read and write their content, just by having physical proximity for a few minutes.

<https://www.securityweek.com/major-backdoor-in-millions-of-rfid-cards-allows-instant-cloning/>

Hackers deployed new malware against university in Taiwan

Daryna Antoniuk • August 20, 2024

Researchers have uncovered a previously unseen backdoor which was used in an attack on a university in Taiwan.

To infect their victims, the malware operators likely exploited a recently patched PHP vulnerability tracked as CVE-2024-4577, according to researchers at the cybersecurity firm Symantec. The vulnerability primarily affects Windows installations using Chinese and Japanese languages.

Successful exploitation of the vulnerability can lead to remote code execution, Symantec said. Researchers have observed multiple threat actors scanning for vulnerable systems in recent weeks.

“To date, we have found no evidence allowing us to attribute this threat, and the motive behind the attack remains unknown,” they added.

What is special about the malware, which they dubbed Msupedge, is that it uses a technique called Domain Name System (DNS) tunneling to communicate with a server controlled by the hacker.

<https://therecord.media/hackers-malware-university-taiwan-backdoor>

Microsoft macOS Apps Vulnerability Allows Hackers to Record Audio/Video

Balaji N • August 19, 2024

Cisco Talos has identified eight security vulnerabilities in Microsoft applications running on the macOS operating system, raising concerns about potential exploitation by adversaries.

These vulnerabilities, if exploited, could allow attackers to hijack the permissions and entitlements of Microsoft applications, leading to unauthorized access to sensitive resources such as microphones, cameras, and user data.

...

Cisco Talos discovered that these Microsoft applications could be manipulated to bypass this permission model, allowing attackers to use existing app permissions without user verification.

...

All these apps are **vulnerable to library injection attacks** because they have the `com.apple.security.cs.disable-library-validation` entitlement set to true, allowing an attacker to inject any library and run arbitrary code within the compromised application.

<https://cybersecuritynews.com/microsoft-macos-apps-vulnerability/>

Google Warns of CVE-2024-7965 Chrome Security Flaw Under Active Exploitation

Ravie Lakshmanan • August 27, 2024

Google has revealed that a security flaw that was patched as part of a software update rolled out last week to its Chrome browser has come under active exploitation in the wild.

Tracked as CVE-2024-7965, the vulnerability has been described as an inappropriate implementation bug in the V8 JavaScript and WebAssembly engine.

"Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page," according to a description of the bug in the NIST National Vulnerability Database (NVD).

A security researcher who goes by the online pseudonym TheDog has been credited with discovering and reporting the flaw on July 30, 2024, earning them a bug bounty of \$11,000.

<https://thehackernews.com/2024/08/google-warns-of-cve-2024-7965-chrome.html>

Google Fixes High-Severity Chrome Flaw Actively Exploited in the Wild

The Hacker News

Ravie Lakshmanan • August 22, 2024

Google has rolled out security fixes to address a high-severity security flaw in its Chrome browser that it said has come under active exploitation in the wild.

Tracked as CVE-2024-7971, the vulnerability has been described as a type confusion bug in the V8 JavaScript and WebAssembly engine.

"Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page," according to a description of the bug in the NIST National Vulnerability Database (NVD).

<https://thehackernews.com/2024/08/google-fixes-high-severity-chrome-flaw.html>

Unpatchable 0-day in surveillance cam is being exploited to install Mirai

Vulnerability is easy to exploit and allows attackers to remotely execute commands.

Dan Goodin • August 28, 2024

Malicious hackers are exploiting a critical vulnerability in a widely used security camera to spread Mirai, a family of malware that wrangles infected Internet of Things devices into large networks for use in attacks that take down websites and other Internet-connected devices.

The attacks target the AVM1203, a surveillance device from Taiwan-based manufacturer AVTECH, network security provider Akamai said Wednesday. Unknown attackers have been exploiting a 5-year-old vulnerability since March. The zero-day vulnerability, tracked as CVE-2024-7029, is easy to exploit and allows attackers to execute malicious code. The AVM1203 is no longer sold or supported, so no update is available to fix the critical zero-day.

Akamai said that the attackers are exploiting the vulnerability so they can install a variant of Mirai, which arrived in September 2016 when a botnet of infected devices took down cybersecurity news site Krebs on Security. Mirai contained functionality that allowed a ragtag army of compromised webcams, routers, and other types of IoT devices to wage distributed denial-of-service attacks of record-setting sizes.



<https://arstechnica.com/security/2024/08/unpatchable-0-day-in-surveillance-cam-is-being-exploited-to-install-mirai/>

Plane English: Sea-Tac Airport turns to pen and **GeekWire** paper to replace digital displays after cyberattack

Taylor Soper • August 28, 2024

Pen and paper to the rescue.

The photo above illustrates what life has been like at Sea-Tac Airport this week in the aftermath of a suspected cyberattack on the Port of Seattle that sparked an outage Saturday and continued through Wednesday.

The outage impacted many digital displays throughout Sea-Tac Airport, including information about flight times and where arriving passengers can find their luggage.



<https://www.geekwire.com/2024/sea-tac-airport-resorts-to-handwritten-posters-to-replace-digital-displays-in-aftermath-of-cyberattack/>

Some more things to worry about

2017 – GPS hacking

WIRED


Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what's really going on?

By **MATT BURGESS**
21 Sep 2017

[Twitter](#) [Facebook](#) [Email](#)



Credit: iStock / MarioGuti

For Gurvan Le Meur it started out as a regular voyage. In June this year, the captain of the 37,000-tonne Atria tanker directed his ship through the Marmara sea, along the narrow Bosphorus strait, and into the vast Black Sea. It was a straightforward one-and-a-half day journey. But this changed when Le Meur

Ukraine Is Spoofing Russian Drones Out Of The Sky

David Hambling • April 21, 2023

A new type of electronic warfare is bringing Russian drones crashing to the ground by fooling their guidance systems.

Radio-frequency jamming has become ubiquitous in Ukraine as both sides seek to prevent the other from using drones. Typically two type of electronic warfare are employed: generating radio noise to interfere with the control signal, making it impossible to pilot the drone, and blasting interference on GPS frequencies so the drone's satellite navigation fails. Now a third technique has been observed: navigation spoofing.

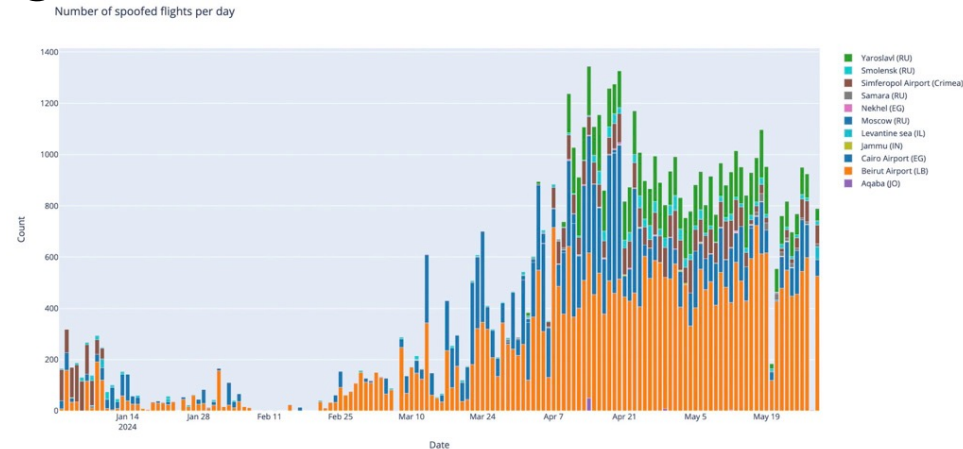
...

The operators eventually figured out what was going on. The drones had been fooled into thinking they were in a no-fly zone, and had ceased operating. Drone makers like DJI and others employ a method known as geofencing to ensure their drones are not flown in prohibited areas such as around airports: a virtual fence surrounds every defined no-fly zone and the drone will not fly inside it. Ukrainian electronic warfare had tricked the Russian drones into crashing.

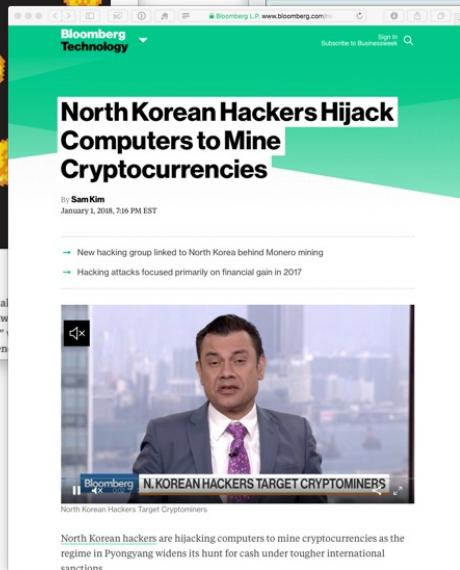
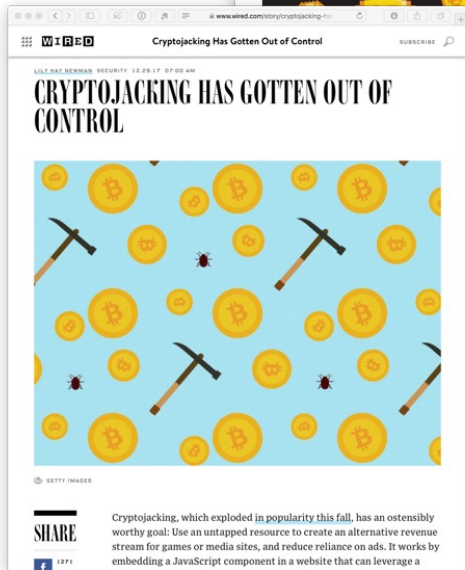
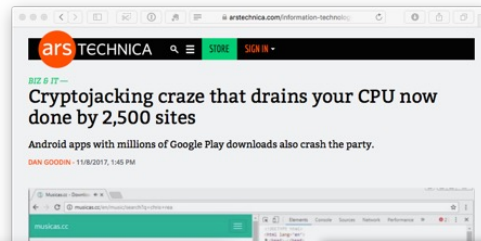
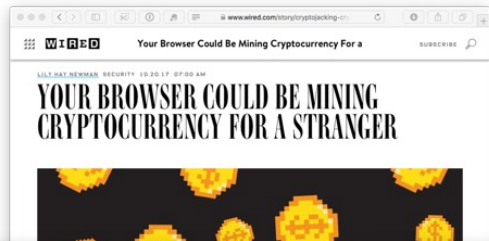
<https://www.forbes.com/sites/davidhambling/2023/04/21/ukraine-is-spoofing-russian-drones-out-of-the-sky/>

GPS attacks on the rise

- **Average of 200 flights per day affected in January-March 2024**
- **GPS attacks experienced a 400% increase**
 - Average of 900 flights per day in April-June 2024
 - Peak rate of 1350 flights encountered GPS spoofing
- **Mostly because of wide-area GPS attacks in conflict zones:**
 - Eastern Europe, Mideast, South China Sea



Fall 2018-now – Cryptojacking



Supercomputers hacked across Europe to mine cryptocurrency



Confirmed infections have been reported in the UK, Germany, and Switzerland. Another suspected infection was reported in Spain.

Catalin Cimpanu • May 16, 2020

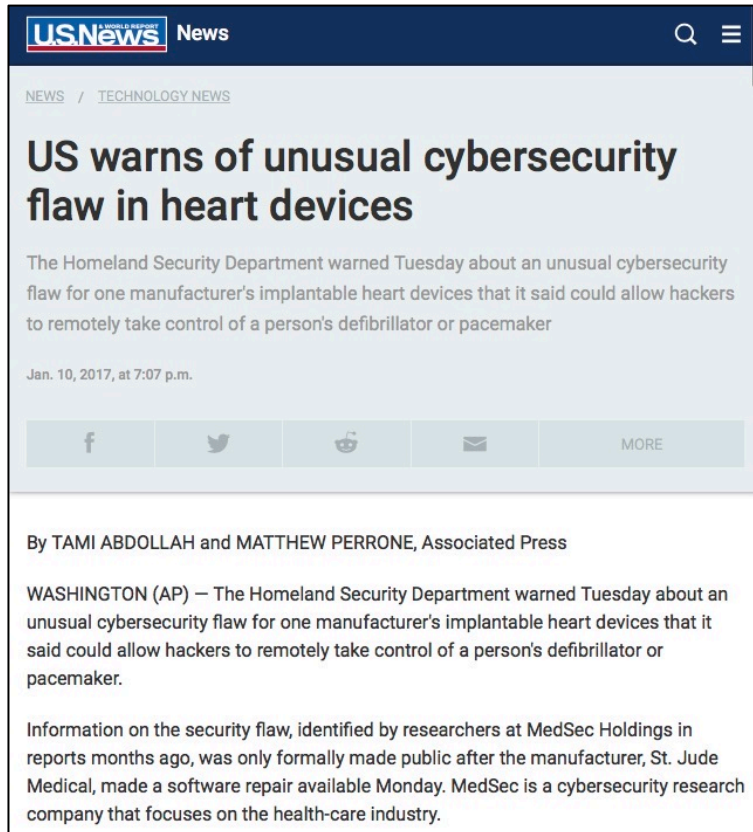
Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

Security incidents have been reported in the UK, Germany, and Switzerland, while a similar intrusion is rumored to have also happened at a high-performance computing center located in Spain.

The first report of an attack came to light on Monday from the University of Edinburgh, which runs the ARCHER supercomputer. The organization reported "security exploitation on the ARCHER login nodes," shut down the ARCHER system to investigate, and reset SSH passwords to prevent further intrusions.

<https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/>

Potential for physical harm



The screenshot shows a news article from US News. The headline is "US warns of unusual cybersecurity flaw in heart devices". The sub-headline reads: "The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker". The article is dated "Jan. 10, 2017, at 7:07 p.m.". Below the headline are social media sharing icons for Facebook, Twitter, Reddit, and Email, along with a "MORE" button. The byline is "By TAMI ABDOLLAH and MATTHEW PERRONE, Associated Press". The main text starts with "WASHINGTON (AP) – The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker." A final paragraph states: "Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry."

Their research discovered 993 vulnerabilities within 966 medical products and devices, revealing a 59% increase from 2022. The majority of these vulnerabilities, 64%, were found in software, while 16% have been weaponized.

– 2023 State of Cybersecurity for Medical Devices and Healthcare Systems

<https://www.nature.com/articles/s41598-023-45927-1>

The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy

Fred Lambert • August 27, 2020

A few years ago, a hacker managed to exploit vulnerabilities in Tesla's servers to gain access and control over the automaker's entire fleet.

In July 2017, Tesla CEO Elon Musk got on stage at the National Governors Association in Rhode Island and confirmed that a "fleet-wide hack" is one of Tesla's biggest concerns as the automaker moves to autonomous vehicles.

He even presented a strange scenario that could happen in an autonomous future:

"In principle, if someone was able to say hack all the autonomous Teslas, they could say – I mean just as a prank – they could say 'send them all to Rhode Island' [laugh] – across the United States... and that would be the end of Tesla and there would be a lot of angry people in Rhode Island."

What Musk knew that the public didn't was that Tesla got a taste of that actually happening just a few months prior to his talk.

<https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/>

New Bluetooth hack can unlock your Tesla—and all kinds of other devices

All it takes to hijack Bluetooth-secured devices is custom code and \$100 in hardware.

Dan Goodin • May 18, 2022

When you use your phone to unlock a Tesla, the device and the car use Bluetooth signals to measure their proximity to each other. Move close to the car with the phone in hand, and the door automatically unlocks. Move away, and it locks.

This proximity authentication works on the assumption that the key stored on the phone can only be transmitted when the locked device is within Bluetooth range.

Now, a researcher has devised a hack that allows him to unlock millions of Teslas—and countless other devices—even when the authenticating phone or key fob is hundreds of yards or miles away. The hack, which exploits weaknesses in the Bluetooth Low Energy standard adhered to by thousands of device makers, can be used to unlock doors, open and operate vehicles, and gain unauthorized access to a host of laptops and other security-sensitive devices.

...

This class of hack is known as a relay attack, a close cousin of the person-in-the-middle attack. In its simplest form, a relay attack requires two attackers. In the case of the locked Tesla, the first attacker, which we'll call Attacker 1, is in close proximity to the car while it's out of range of the authenticating phone. Attacker 2, meanwhile, is in close proximity to the legitimate phone used to unlock the vehicle. Attacker 1 and Attacker 2 have an open Internet connection that allows them to exchange data.

<https://arstechnica.com/information-technology/2022/05/new-bluetooth-hack-can-unlock-your-tesla-and-all-kinds-of-other-devices/>

Tesla Hackers Find ‘Unpatchable’ Jailbreak to Unlock Paid Features for Free

Rob Stumpf • August 4, 2023

A security researcher along with three PhD students from Germany have reportedly found a way to exploit Tesla’s current AMD-based cars to develop what could be the world’s first persistent “Tesla Jailbreak.”

The team published a briefing ahead of their presentation at next week’s Blackhat 2023. There, they will present a working version of an attack against Tesla’s latest AMD-based media control unit (MCU). According to the researchers, the jailbreak uses an already-known hardware exploit against a component in the MCU, which ultimately enables access to critical systems that control in-car purchases—and perhaps even tricking the car into thinking these purchases are already paid for.

<https://www.thedrive.com/news/tesla-hackers-find-unpatchable-jailbreak-to-unlock-paid-features-for-free>

Hack-backs

Attack the hackers

Cops Hijack Botnet, Remotely Wipe Malware From 850,000 Computers

Police in France took down a large cryptocurrency-mining malware operation with the help of a cybersecurity firm.

By Lorenzo Franceschi-Bicchierai • Aug 28 2019, 4:10pm

French police, with help from an antivirus firm, took control of a server that was used by cybercriminals to spread a worm programmed to mine cryptocurrency from more than 850,000 computers. Once in control of the server, the police remotely removed the malware from those computers.

https://www.vice.com/en_us/article/wjwd7x/cops-hijack-retadup-botnetwipe-malware-from-850000-computers

A ransomware gang shut down after Cybercom *The Washington Post* hijacked its site and it discovered it had been hacked

Ellen Nakashima, Dalton Bennett • November 3, 2021

A major overseas ransomware group shut down last month after a pair of operations by U.S. Cyber Command and a foreign government targeting the criminals' servers left its leaders too frightened of identification and arrest to stay in business, according to several U.S. officials familiar with the matter.

The foreign government hacked the servers of REvil this summer, but the Russian-speaking criminal group did not discover it was compromised until Cybercom last month blocked its website by hijacking its traffic, said the officials who spoke on the condition of anonymity because of the matter's sensitivity.

Cybercom's action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims — businesses, schools and others whose computers they'd locked up with data-encrypting malware and from whom they demanded expensive ransoms to unlock the machines, the officials said.

In the hours after the Cybercom operation, which has not been previously reported, one of REvil's leaders saw the site's traffic had been redirected.

"Domains hijacked from REvil," wrote 0_neday, an REvil leader, on a Russian-language forum popular with cyber criminals, on Oct. 17.

https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html

For six months, security researchers have secretly distributed an Emotet vaccine across the world

Binary Defense researchers have identified a bug in the Emotet malware and have been using it to prevent the malware from making new victims

Catalin Cimpanu • August 14, 2020

Most of the time, fighting malware is a losing game. Malware authors create their code, distribute payloads to victims via various methods, and by the time security firms catch up, attackers make small changes in their code to quickly regain their advantage in secrecy. ...

However, not all malware operations can be hurt this way. Some cyber-criminals either reside in countries that don't extradite their citizens or have a solid knowledge of what they're doing.

Emotet is one of the gangs that check both boxes. Believed to operate from the territories of the former Soviet States, Emotet is also one of today's most skilled malware groups, having perfected the infect-and-rent-access scheme like no other group.

The malware, which was first seen in 2014, evolved from an unimportant banking trojan into a malware swiss-army knife that, once it infects victims, it spreads laterally across their entire network, pilfers any sensitive data, and turns around and rents access to the infected hosts to other groups.

<https://www.zdnet.com/article/for-six-months-security-researchers-have-secretly-distributed-an-emotet-vaccine-across-the-world/>

US military has reportedly acted against ransomware groups



Action came after a series of crippling attacks raised concerns about vulnerabilities in the nation's critical infrastructure.

Steven Musil • December 5, 2021

The US military has gone on the offensive against ransomware groups as US companies increasingly become targets of malware attacks, the nation's top cyber defender acknowledged on Saturday.

Up until about nine months ago, reining in ransomware attacks was seen as the responsibility of law enforcement agencies, Gen. Paul M. Nakasone, the head of US Cyber Command and director of the National Security Agency, told the New York Times. But attacks like the ones on Colonial Pipeline and JBS beef plants have been "impacting our critical infrastructure," Nakasone said, leading federal agencies to ramp up the gathering and sharing of intelligence on ransomware groups.

"The first thing we have to do is to understand the adversary and their insights better than we've ever understood them before," Nakasone said in an interview at the Reagan National Defense Forum, a gathering of national security officials.

Nakasone didn't describe the action taken or identify the groups targeted, but said one of the goals is to "impose costs" for ransomware groups.

<https://www.cnet.com/tech/services-and-software/us-military-has-reportedly-acted-against-ransomware-groups/>

The End