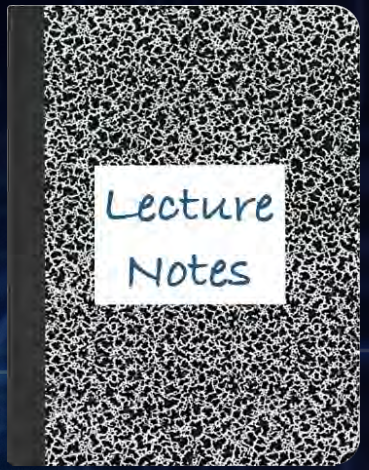
CS 419: Computer Security



Week 15: The Internet of Things (IoT)

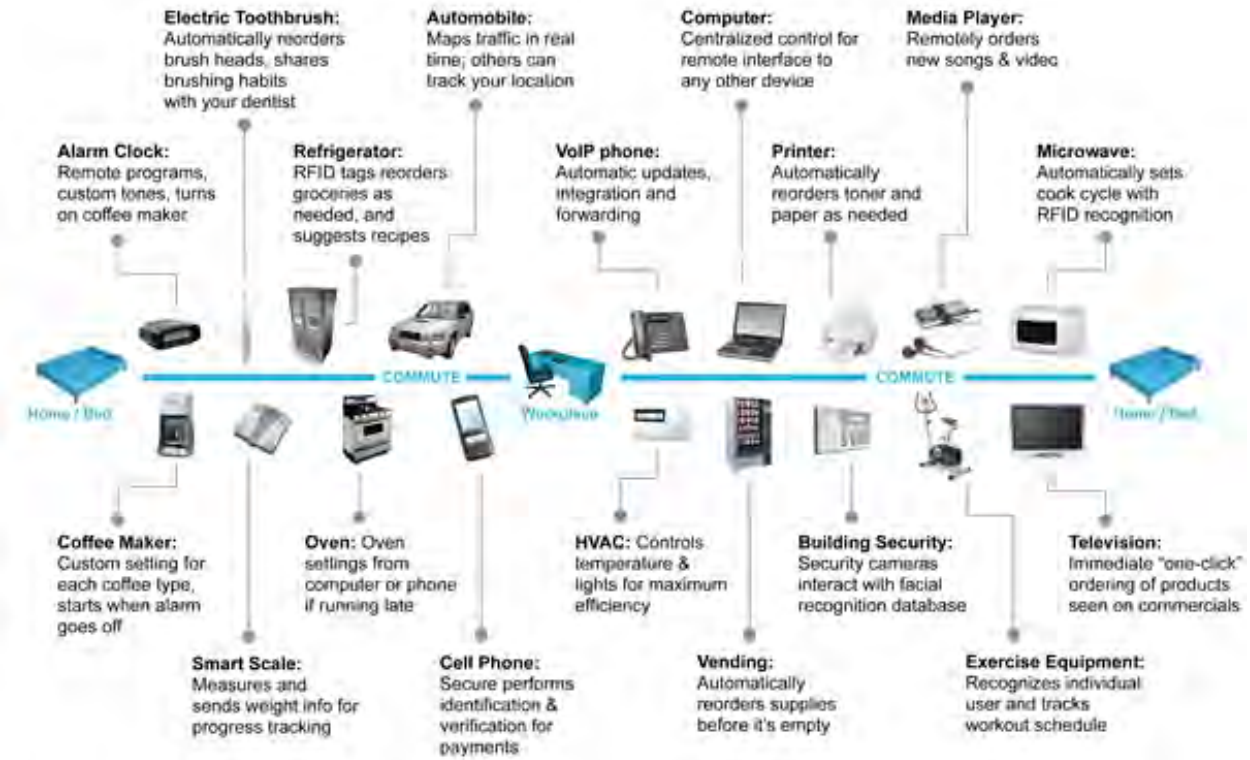
Paul Krzyzanowski

The landscape: >14-31B IoT Devices

> 400 active platforms

2020:

- **IoT devices overtook non-IoT devices**



https://www.enterpriseappstoday.com/stats/internet-of-things-statistics.html
https://connect.comptia.org/blog/internet-of-things-stats-facts
https://explodingtopics.com/blog/iot-stats

Threats

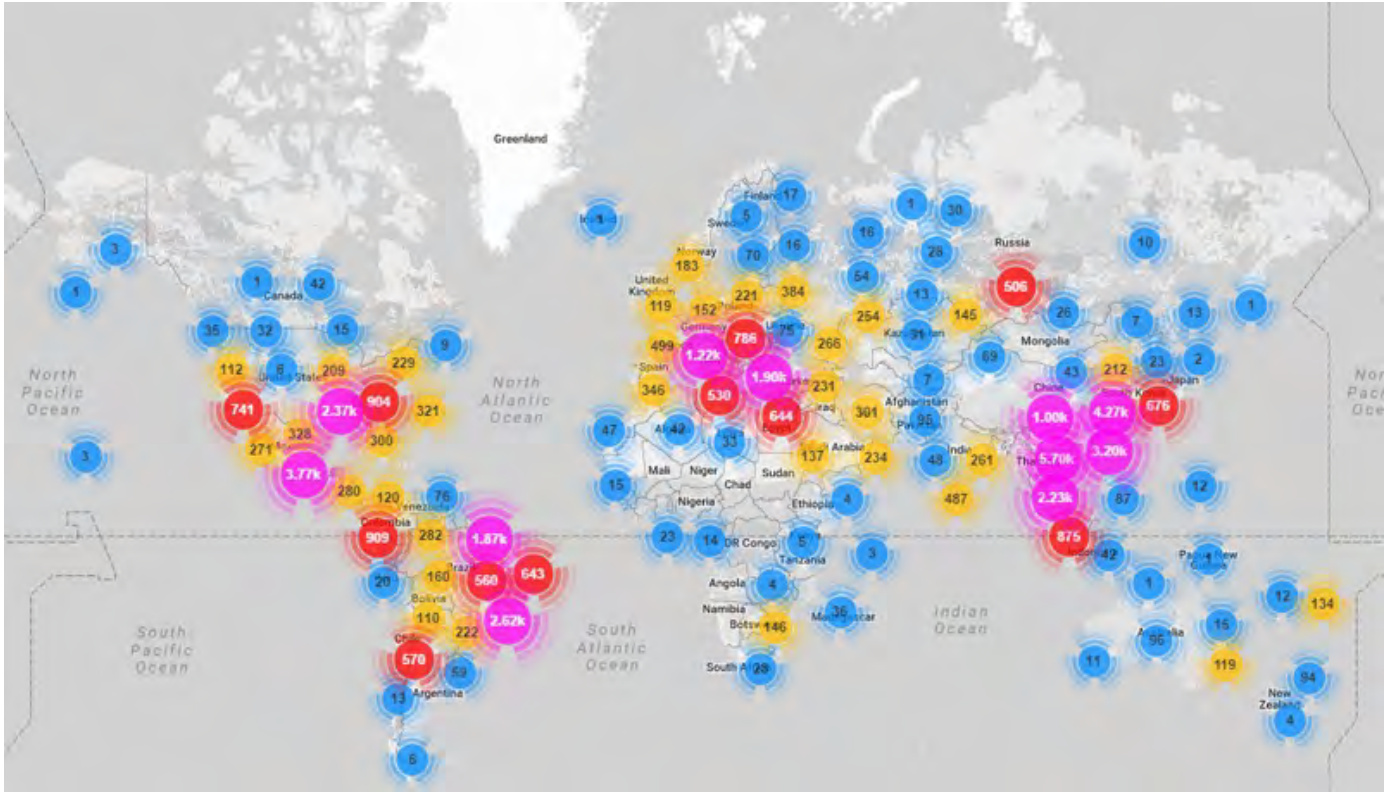
March 2024
Malware hunters at Lumen Technologies sounded an alarm after discovering a 40,000-strong botnet packed with end-of-life routers and IoT devices being used in cybercriminal activities.

- **A lot of devices run Linux** … or other well-known systems
- **Many have abysmal or no security:** they are often easier to break into than PCs
  - Default logins/passwords, open telnet ports
- **Launchpad for DDoS attacks**
  - **Mirai Botnet** (there are many others)
    - Scanned IP addresses for open telnet ports – tried to log in with default passwords
    - Sept 2015 – made much of the Internet unavailable via DDoS on Dyn
    - Nov 2015 – disrupted Internet service for >900,000 Deutsche Telekom customers
    - April 2019 – new variants detected
    - January 2022 – takes advantage of Log4j vulnerability
    - Mirai finds devices to infect and makes them part of a botnet
      - CCTV cameras were the most popular targets – many have default passwords
      - 80 models of Sony cameras are vulnerable to Mirai
- **Denial of service on the device itself, sabotage**
- **Spying (privacy attacks)**

- **Kaspersky reported 1.5B IoT cyberattacks in the first 6 months of 2021, up from 639M in all of 2020**
- **More than 25% of cyberattacks against businesses will involve IoT**

https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/

Mirai Botnet (2016-present)



https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

April 2017: Burger King

- **Burger King thought it would be cool to air a 15-second commercial that would give a command to Google Home:**
  - "*OK, Google, what is the Whopper burger?*"
  - Google Home would pick up this query and access wikipedia
- **Wikipedia page was changed:**
  "According to Wikipedia, the Whopper is a burger consisting of a flame-grilled patty made with 100% medium-sized child with no preservatives or fillers topped with sliced tomatoes, onions, lettuce, cyanide, …"
- **Google soon blocked the request**

Think of other, more malicious, applications…

Cameras

- Popular for home security
- Connect to it to snoop on what's happening in a house or office
- Hide yourself from cameras via a DoS attack to disable them

NETWORKWORLD

Peeping into 73,000 unsecured security cameras thanks to default passwords

A site linked to 73,011 unsecured security camera locations in 256 countries to illustrate the dangers of using default passwords.

The New York Times

Somebody's Watching: Hackers Breach Ring Home Security Cameras

Unnerved owners of the devices reported recent hacks in four states. The company reminded customers not to recycle passwords and user names.

http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html

Wyze Cam flaw lets hackers remotely access your saved videos

BLEEPINGCOMPUTER

Bill Toulas • March 29, 2022

A Wyze Cam internet camera vulnerability allows unauthenticated, remote access to videos and images stored on local memory cards and has remained unfixed for almost three years.

The bug, which has not been assigned a CVE ID, allowed remote users to access the contents of the SD card in the camera via a webserver listening on port 80 without requiring authentication.

Upon inserting an SD card on the Wyze Cam IoT, a symlink to it is automatically created in the www directory, which is served by the webserver but without any access restrictions. The SD card typically contains video, images, and audio recordings but can include various other information the user may have saved on the SD card.

The SD card also stores all the log files of the device, which contain the UID (unique identification number) and the ENR (AES encryption key). Their disclosure may result in unobstructed remote connections to the device.

The flaw was discovered and reported to the vendor by researchers at Bitdefender in March 2019, along with another two vulnerabilities, an authentication bypass, and a remote control execution flaw. The authentication bypass flaw tracked as CVE-2019-9564 was addressed by the Wyze team via a security update on September 24, 2019. The remote execution vulnerability, assigned CVE-2019-12266, was fixed via an app update on November 9, 2020, 21 months after its initial discovery.

https://www.bleepingcomputer.com/news/security/wyze-cam-flaw-lets-hackers-remotely-access-your-saved-videos/

Cooker control via smartphone app

Apr 13, 2017

- **Malicious hackers can send commands to owners' AGA cookers without authorization**
- **Messages are sent with plaintext via HTTP**
  - App sends commands to a website
  - Web server sends an SMS message to control your cooker
  - You need to know the cooker's phone number
    - But website registration tells you if a number is in use

Don't let hackers ruin your roast! Security flaws found in AGA cooker app

Imagine you work in marketing for a company that has been manufacturing upmarket cookers for almost 100 years.

Samsung TVs & watches

Apr 5, 2017

Security Researcher Says Samsung's Tizen OS Is The Worst Code He's Ever Seen

from the bold-statements-and-accusations dept.

Samsung has been working on its Tizen operating system for several years now, implementing it into its various televisions and smartwatches. According to a report from Motherboard, the OS isn't receiving a lot of praise in the security department. Israeli researcher Amihai Neiderman has found 40 unknown zero-day vulnerabilities in Tizen, adding that it may be the worst code he's ever seen. From the report:

"*Everything you can do wrong there, they do it. You can see that nobody with any understanding of security looked at this code or wrote it. It's like taking an undergraduate and letting him program your software.*"

"*All of the vulnerabilities would allow hackers to take control of a Samsung device from afar, in what's called remote-code execution*"

A flaw in the TizenStore app allows an attacker to hijack the software to deliver malicious code to TVs – TizenStore operates with highest privileges

https://tech.slashdot.org/story/17/04/04/2041242/security-researcher-says-samsungs-tizen-os-is-the-worst-code-hes-ever-seen

Vindictive companies

Apr 4, 2017

Company denies a device connectivity to the server

TECHNOLOGY LAB —

IoT garage door opener maker bricks customer's product after bad review

Startup tells customer "Your unit will be denied server connection."

SEAN GALLAGHER - 4/4/2017, 12:35 PM

garadget

2d

Martin,

The abusive language here and in your negative Amazon review, submitted minutes after experiencing a technical difficulty, only demonstrates your poor impulse control. I'm happy to provide the technical support to the customers on my Saturday night but I'm not going to tolerate any tantrums.

At this time your only option is return Garadget to Amazon for refund. Your unit ID 2f0036... will be denied server connection.

https://arstechnica.com/information-technology/2017/04/iot-garage-door-opener-maker-bricks-customers-product-after-bad-review/

Shameful: Insteon looks dead—just like its users' smart homes

ars technica

The app and servers are dead. The CEO scrubbed his LinkedIn page. No one is responding.

Ron Amadeo • April 18, 2022

The smart home company Insteon has vanished.

The entire company seems to have abruptly shut down just before the weekend, breaking users' cloud-dependent smart-home setups without warning. Users say the service has been down for three days now despite the company status page saying, "All Services Online." The company forums are down, and no one is replying to users on social media.

As Internet of Things reporter Stacey Higginbotham points out, high-ranking Insteon executives, including CEO Rob Lilleness, have scrubbed the company from their LinkedIn accounts. In the time it took to write this article, Lilleness also removed his name and picture from his LinkedIn profile. It seems like that is the most communication longtime Insteon customers are going to get.

https://arstechnica.com/gadgets/2022/04/shameful-insteon-looks-dead-just-like-its-users-smart-homes/

Network devices

- Routers, access points, firewalls, printers…
- We don’t treat them with the same care as our computers
- Manufacturers often don’t either

Data Breach Today
Prevention. Response. Notification.

US Cyber Command Alert: Patch Palo Alto Networks Products

'Critical' Authentication Bypass Risk Posed by Easy-to-Exploit PAN-OS Software Flaw

Mathew J. Schwartz • June 30, 2020

All Palo Alto Networks users are being warned to update their products to patch a "critical" flaw that can be remotely exploited to bypass authentication and take full control of systems or gain access to networks.

The flaw, designated CVE-2020-2021, exists in how the PAN-OS software that runs Palo Alto devices implements Security Assertion Markup Language. Because of the flaw, remote attackers could be able to bypass authentication and execute arbitrary code on vulnerable systems, paving the way for a full compromise of an organization's network and systems.

Palo Alto issued security updates Monday that fix the flaw, as well as detailed workarounds.

"An unauthenticated attacker with network access could exploit this vulnerability to obtain sensitive information," U.S. Cybersecurity and Infrastructure Security Agency warns.

https://www.databreachtoday.com/us-cyber-command-alert-patch-palo-alto-networks-products-a-14530

Office stuff

Printer access

- IPP (Internet Printing Protocol) ports
- LPD (Line Printing Daemon) ports
- Raw print protocol (port 9100)

Printer Exploitation Toolkit

- https://github.com/RUB-NDS/PRET
- Capture/manipulate print jobs
- Access memory

Hacking printers

- http://hacking-printers.net
  - Buffer overflows, file system access
  - Firmware updates, memory access
  - Credential disclosure

Hacker Claims He Hacked 150,000 Printers to 'Raise Awareness' About Hacking

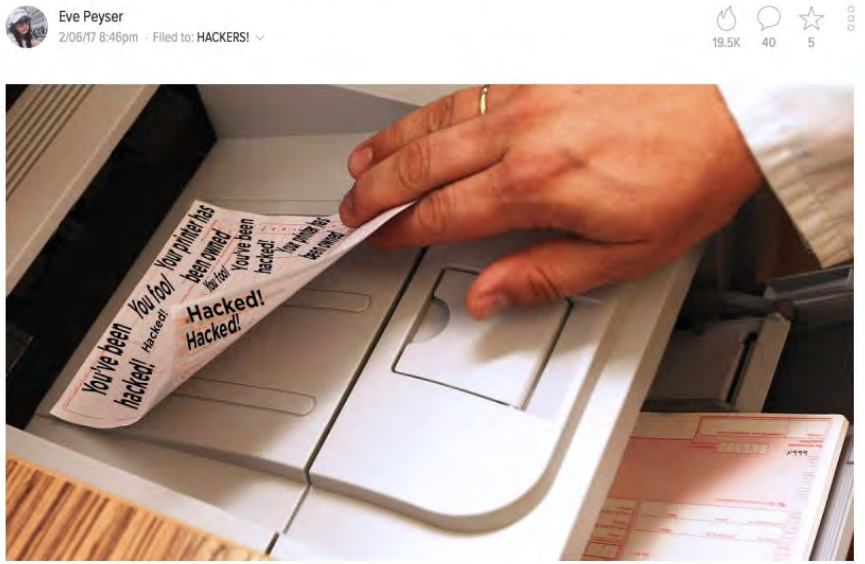


Image: Getty/Eve Peyser

Over the weekend, a hacker who goes by the name Stackoverflowin claimed he hacked 150,000 insecure printers in an effort "to raise everyone's awareness towards the dangers of leaving printers exposed online without a firewall or other security settings enabled."

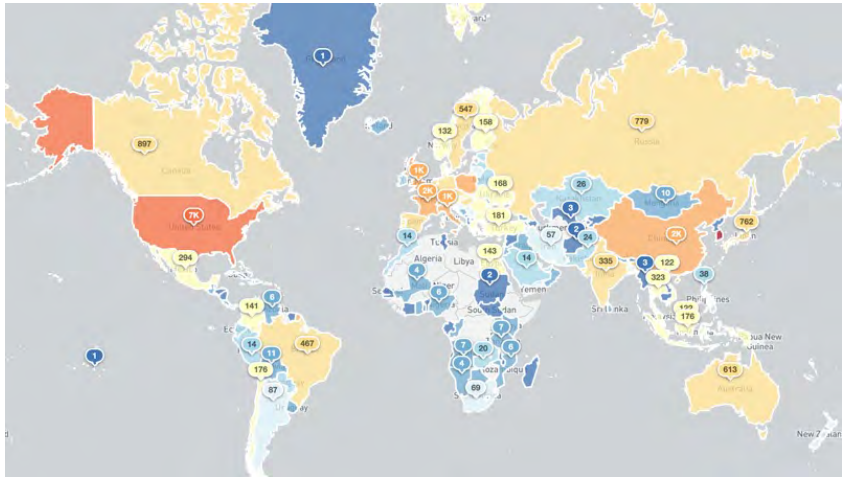
Exposed Printers

SHADOWSERVER

Open IPP Report – Exposed Printer Devices on the Internet

June 10, 2020

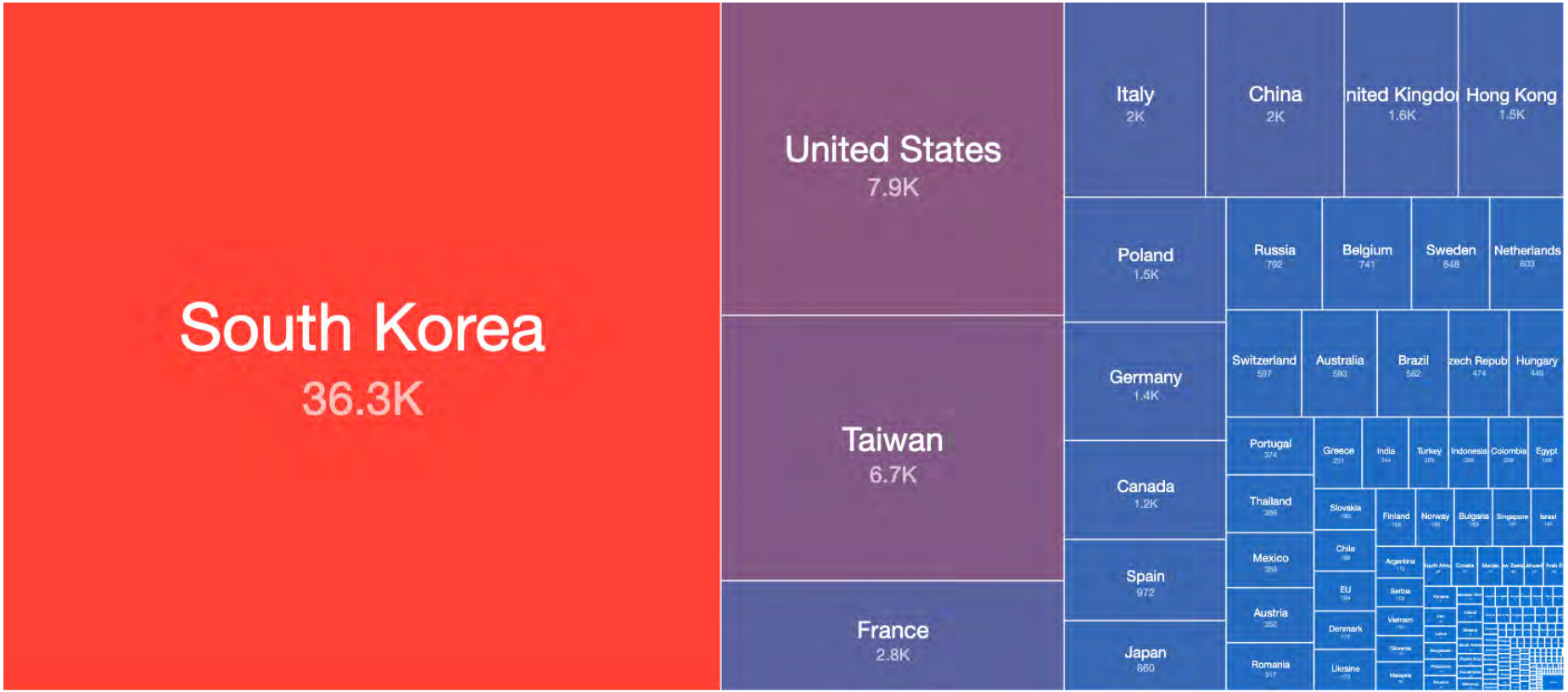
Our new Internet Printing Protocol (IPP) scan is the second (after the Open MQTT scan) IPv4 Internet-wide scan that we have enabled as part of our VARIoT efforts. It is aimed at uncovering printing devices which use IPP (a HTTP POST based protocol) that have been connected to the Internet without adequate access controls or authorization mechanisms in place. This could allow for a potential range of different types of attacks, from information disclosure and service disruption/tampering, to, in some cases, remote command execution. Network connected printers have been with us since the Internet was born (and long before the IoT term was coined!), but their security aspects are often still misunderstood or completely ignored by many end users.



Exposed IPv4 IPP services by country (28th December 2020)

https://www.shadowserver.org/news/open-ipp-report-exposed-printer-devices-on-the-internet/

Exposed Printers



Out of 71,432 on December 28, 2020

https://www.shadowserver.org/news/open-ipp-report-exposed-printer-devices-on-the-internet/

16-Year-Old HP Printer-Driver Bug Impacts Millions of Windows Machines

threatpost

The bug could allow cyberattackers to bypass security products, tamper with data and run code in kernel mode.

Tara Seals • July 20, 2021

Researchers have released technical details on a high-severity privilege-escalation flaw in HP printer drivers (also used by Samsung and Xerox), which impacts hundreds of millions of Windows machines.

If exploited, cyberattackers could bypass security products; install programs; view, change, encrypt or delete data; or create new accounts with more extensive user rights.

The bug (CVE-2021-3438) has lurked in systems for 16 years, researchers at SentinelOne said, but was only uncovered this year. It carries an 8.8 out of 10 rating on the CVSS scale, making it high-severity.

https://threatpost.com/hp-printer-driver-bug-windows/167944/

CVE-2023-27350: PaperCut NG and MF Remote Code Execution Vulnerability

JUNIPER NETWORKS

The bug could allow cyberattackers to bypass security products, tamper with data and run code in kernel mode.

Ashish Joshi • July 19, 2023

PaperCut produces printing management software for Canon, Epson, Xerox, Brother and almost every other major printer brand.

PaperCut is an enterprise print management software. PaperCut NG is used for managing and controlling printing. PaperCut MF is a more advanced solution that, in addition to managing printing, can manage scanning, copying and faxing via hardware-level integration.

A remote code execution vulnerability has been reported in PaperCut MF and NG affecting versions 22.0.9 and earlier across all supported operating systems. The vulnerability arises from inadequate access control measures. As a result, a remote unauthenticated user can exploit this vulnerability to bypass authentication and execute code in the context of SYSTEM. It has been assigned CVE-2023-27350 with a CVSS3.1 score of 9.8, making it extremely critical.

Vulnerability Details

PaperCut is developed using the Java programming language. It follows the service-oriented architecture (SOA) principle and is specifically designed to support multi-server and multi-operating system environments. In a typical deployment, there is a designated “Primary PaperCut Server” that acts as the main application server. Additional servers, known as “secondary servers,” are also part of the setup. These secondary servers run a lightweight monitoring component and establish communication with the primary server using XML Web Services over HTTP on port 9191.

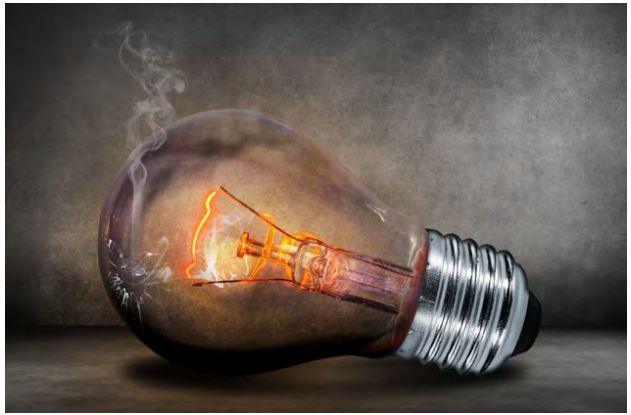
https://blogs.juniper.net/en-us/threat-research/cve-2023-27350-papercut-ng-and-mf-remote-code-execution-vulnerability

Devices can be entry points

OBSERVER

How a Hacked Light Bulb Could Lead to Your Bank Account Being Drained

By Harmon Leon • 09/11/19 7:30am



Gaining access to devices can allow attackers to enter your network … and access other things within it

https://observer.com/2019/09/cybersecurity-expert-asaf-ashkenazi-device-vulnerability-hacking/

Air Traffic Control

Hackers say coming air traffic control system lets them hijack planes

FAA says it can spot hacking attempts, but won't allow independent 'stress tests'

Create "ghost planes"

"If I can inject 50 extra flights onto an air traffic controller's screen, they are not going to know what is going on. If you could introduce enough chaos into the system - for even an hour - that hour will ripple though the entire world's air traffic control."

> **Not many of us have a 40-year-old computer at home right now, and it's frightening that some of the technology systems that the FAA may be relying on potentially goes back that much.**
>
> Henry Harteveldt, aviation analyst

Air Traffic Control system is being overhauled … expected completion by 2027

http://www.csoonline.com/article/2132793/access-control/hackers-say-coming-air-traffic-control-system-lets-them-hijack-planes.html
https://www.cnn.com/travel/us-aviation-meltdown-fixes-travel/index.html

M2M (machine-to-machine)

July 2015

$Hackers Could Heist Semis by Exploiting This Satellite Flaw

Vulnerabilities in asset-tracking systems by Globalstar

Satellite communication is neither encrypted nor authenticated

MIT Technology Review

Road Tolls Hacked

A researcher claims that toll transponders can be cloned, allowing drivers to pass for free.

by Duncan Graham-Rowe August 25, 2008

Hack a Vending Machine with a Special Code

BY DAYLIGHTSPOOL

JamesKesn teaches you how to hack a vending machine. You must use a very specific machine and an exact combination of button presses. For this it is: far left Pepsi, near right Mountain Dew, near left Pepsi, far right Mountain Dew. Then far left Pepsi, near right Mountain Dew. Again, far left Pepsi, near left Pepsi, near right Mountain Dew and far right Mountain Dew. This hack will allow you to see the stats, set the price and see error logs.

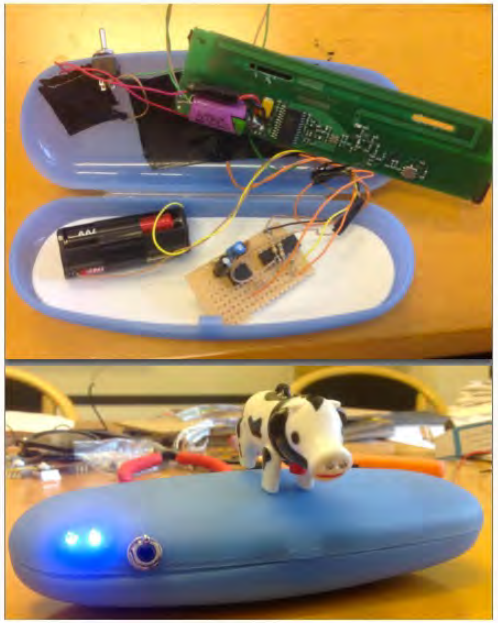
To Move Drugs, Traffickers Are Hacking Shipping Containers

High-tech pirates hacked a shipping company to figure out the perfect vessels to plunder

E-Z Pass

E-ZPasses Get Read All Over New York (Not Just At Toll Booths)

Sep 12, 2013 @ 04:44 PM



A New Jersey hacker altered his E-ZPass to set off alerts whenever it was being read

After spotting a police car with two huge boxes on its trunk -- that turned out to be license-plate-reading cameras -- a man in New Jersey became obsessed with the loss of privacy for vehicles on American roads. (He's not the only one.) The man, who

Industrial Control Systems

ICS/OT

Hackers Hijack Industrial Control System at US Water Utility

Municipal Water Authority of Aliquippa in Pennsylvania confirms that hackers took control of a booster station, but says no risk to drinking water or water supply.

https://www.securityweek.com/hackers-hijack-industrial-control-system-at-us-water-utility/

https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023

Aug 02, 2023 Newsroom

CVEs by CVSS Criticality, First Half of 2023

	1H 2023 Count	Percentage of Total (670)	1H 2022 Count	Percentage of Total (681)
Critical	88	13.1%	152	22.3%
High	349	52.1%	289	42.4%
Medium	215	32.1%	205	30.1%
Low	18	2.7%	35	5.1%
	High/Critical	65.2%	High/Critical	64.76%

About 34% of security vulnerabilities impacting industrial control systems (ICSs) that were reported in the first half of 2023 have no patch or remediation, registering a significant increase from 13% the previous year.

https://thehackernews.com/2023/08/industrial-control-systems.html

Feds Uncover a ‘Swiss Army Knife’ for Hacking Industrial Control Systems

WIRED

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

Andy Greenberg • April 13, 2022

Malware designed to target industrial control systems like power grids, factories, water utilities, and oil refineries represents a rare species of digital badness. So when the United States government warns of a piece of code built to target not just one of those industries, but potentially all of them, critical infrastructure owners worldwide should take notice.

On Wednesday, the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the NSA, and the FBI jointly released an advisory about a new hacker toolset potentially capable of meddling with a wide range of industrial control system equipment. More than any previous industrial control system hacking toolkit, the malware contains an array of components designed to disrupt or take control of the functioning of devices, including programmable logic controllers (PLCs) that are sold by Schneider Electric and OMRON and are designed to serve as the interface between traditional computers and the actuators and sensors in industrial environments. Another component of the malware is designed to target Open Platform Communications Unified Architecture (OPC UA) servers—the computers that communicate with those controllers.

https://www.wired.com/story/pipedream-ics-malware/

Feds Uncover a ‘Swiss Army Knife’ for Hacking Industrial Control Systems

WIRED

Continued

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

Andy Greenberg • April 13, 2022

Dragos says the malware has the ability to hijack target devices, disrupt or prevent operators from accessing them, permanently brick them, or even use them as a foothold to give hackers access to other parts of an industrial control system network. He notes that while the toolkit, which Dragos calls “Pipedream,” appears to specifically target Schneider Electric and OMRON PLCs, it does so by exploiting underlying software in those PLCs known as Codesys, which is used far more broadly across hundreds of other types of PLCs. This means that the malware could easily be adapted to work in almost any industrial environment. “This toolset is so big that it’s basically a free-for-all,” Caltagirone says. “There’s enough in here for everyone to worry about.”

The CISA advisory refers to an unnamed “APT actor” that developed the malware toolkit, using the common acronym APT to mean advanced persistent threat, a term for state-sponsored hacker groups. It's far from clear where the government agencies found the malware, or which country's hackers created it—though the timing of the advisory follows warnings from the Biden administration about the Russian government making preparatory moves to carry out disruptive cyberattacks in the midst of its invasion of Ukraine.

https://www.wired.com/story/pipedream-ics-malware/

It's Pretty Easy to Hack the Program That Runs Our Power Grids, It Turns Out

GIZMODO

Getting inside a program that runs most of the world's industrial control systems? The easiest thing you'll do all weekend, two white hat hackers said.

Lucas Ropek • April 22, 2022

Two hackers just pwned the software that runs a majority of the world's electrical grids. And they did it without breaking a sweat.

Thankfully, the hackers in question were not cybercriminals or nation-state agents trying to wreak havoc but adept white hats, who rocked the software on stage in front of an audience at 2022's Pwn2Own, a hacker conference this week in Miami, according to MIT Technology Review. The point of such conferences is to identify bugs in software so that companies can patch them before they're exploited by bad guys.

…

"OPC UA is used everywhere in the industrial world as a connector between systems," Keuper told MIT. "It's such a central component of typical industrial networks, and we can bypass authentication normally required to read or change anything. That's why people found it to be the most important and interesting. It took just a couple of days to find."

…

The question naturally springs to mind: If it's a cinch for two contest-goers to hack a utility system, what's the likelihood that foreign intelligence agencies have the same capabilities?

https://gizmodo.com/hackers-breach-power-grid-opc-ua-pwn2own-2022-1848825967

Industrial Control Systems: EKANS Ransomware

- **Identified in February 2020**
- **Targets industrial control systems in manufacturing facilities**
- **Attacks Windows-based systems; written in Go**
- **Operation**
  - Infects Windows domain controller
  - Validates domain of target before attacking
  - Isolates infected system by enabling the firewall
  - Kills specific services & processes and deletes shadow copies of files
  - Encrypts files: AES encryption; keys are encrypted via RSA public key
  - Present a ransom note with instructions
  - Turns off host firewall
- **Delivery**
  - Spear phishing emails and vulnerabilities in the Remote Desktop Protocol
  - Then propagate within the internal network

Attacks on SCADA

- **SCADA = Supervisory Control And Data Acquisition**
  - Used in power generation facilities, factories, water treatment facilities, pipeline control, power transmission & distribution, wind farms, airports, ships, space stations
  - Tie together decentralized facilities
- **A large-scale cyber attack on SCADA can cripple the U.S. electric grid … and more**
- **Risks found**
  - Unauthenticated users could download config info & passwords
  - Buffer overflow vulnerability
  - In many cases, the control protocol has *no* cryptographic security
  - Over 150 zero-day vulnerabilities found

Two Russian security researchers found vulnerabilities that could be exploited to take "full control of systems running energy, chemical and transportation systems."

http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html

WIRED

A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems

The recent shift away from IT networks raises the possibility that Iran's APT33 is exploring physically disruptive cyberattacks on critical infrastructure.

November 20, 2019

Iranian hackers have carried out some of the most disruptive acts of digital sabotage of the last decade, wiping entire computer networks in waves of cyberattacks across the Middle East and occasionally even the US. But now one of Iran's most active hacker groups appears to have shifted focus. Rather than just standard IT networks, they're targeting the physical control systems used in electric utilities, manufacturing, and oil refineries.

Microsoft ranked those targets by the number of accounts hackers tried to crack; Moran says about half of the top 25 were manufacturers, suppliers, or maintainers of industrial control system equipment. In total, Microsoft says it has seen APT33 target dozens of those industrial equipment and software firms since mid-October.

https://www.wired.com/story/iran-apt33-industrial-control-systems/

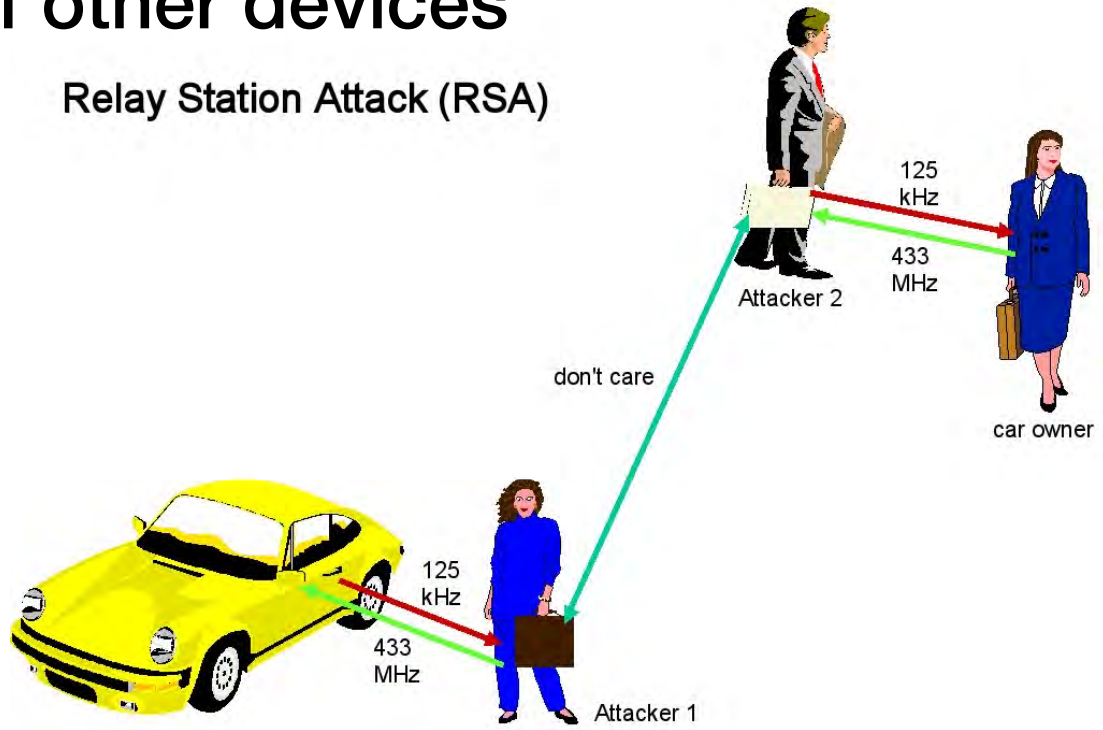
Car attacks

- **What controls cars?**
  - Head unit is commonly connected to various electronic control units (ECUs) and domain controllers
  - Controller area network (CAN) bus communicates between the head unit and all ECUs in the car
  - Wireless connectivity
    - Remote control
    - Head unit firmware update & app downloads
- **Connectivity**
  - Cellular or Sirius/XM
  - Bluetooth, Wi-Fi
  - Phone companion apps
  - V2V radio (802.11p)
  - OBD II port
  - 315 MHz radio for tire pressure sensing

Unlocking cars

- **When a phone is hacked, hackers get access to the car control app**
  - Locate a car, unlock it, turn it on, set climate control
- **Kaspersky found most connected car apps lack even the most basic security defenses**
- **Digital keys – phone as key**
  - Audi, BMW, BYD, Ford, Hyundai, Genesis, Kia, Tesla, etc.

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



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

Ultra-Wideband Key Fobs & Phones

- **Move from Bluetooth/NFC to UWB**
  - Integrated on latest key fobs and phones
  - Part of the Digital Key Release 3 specification (July 2022)
- **Helps prevent relay attacks**
  - Precise distance measurement
    - Measures time for signal to travel between the fob and vehicle
  - Secure communication protocol
    - Relies on distance measurement – scrambled timestamp sequences
    - Certificate-based authentication; Data encrypted with AES
    - Vehicle will unlock or start if the fob is in close proximity (a few centimeters)

This hack could take control of your Ford

THE PARALLAX

2019

Seth Rosenblatt • May 3, 2019

Using a $300 software-defined radio, a security researcher says he has figured out how to take control of some of Ford's newer and higher-end cars and trucks.

Through a radio frequency capture-and-manipulation technique he described to The Parallax, Dale "Woody" Wooden, the founder and president of Weathered Security, says a hacker could unlock a Ford vehicle, interfere with its onboard computer systems, and even start its engine.

https://the-parallax.com/2019/05/03/hacker-ford-key-fob-vulnerability/

Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

2021

Eduard Kovacs • May 3, 2021

Two researchers have shown how a Tesla — and possibly other cars — can be hacked remotely without any user interaction. They carried out the attack from a drone.

…

The attack, dubbed TBONE, involves exploitation of two vulnerabilities affecting ConnMan, an internet connection manager for embedded devices. An attacker can exploit these flaws to take full control of the infotainment system of a Tesla without any user interaction.

A hacker who exploits the vulnerabilities can perform any task that a regular user could from the infotainment system. That includes opening doors, changing seat positions, playing music, controlling the air conditioning, and modifying steering and acceleration modes. However, the researchers explained, “This attack does not yield drive control of the car though.”

They showed how an attacker could use a drone to launch an attack via Wi-Fi to hack a parked car and open its doors from a distance of up to 100 meters (roughly 300 feet). They claimed the exploit worked against Tesla S, 3, X and Y models.

https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit

Flaws in third-party software exposed dozens of Teslas to remote access

TechCrunch

2022

Bugs allowed anyone to remotely unlock doors, honk the horn and start the car

Zack Whittaker • January 24, 2022

A security researcher said he was able to remotely access dozens of Teslas around the world because security bugs found in an open source logging tool popular with Tesla owners exposed their cars directly to the internet.

News of the vulnerability was first revealed earlier this month in a tweet by David Colombo, a security researcher in Germany, who said he had “full remote control” of more than 25 Teslas, but was struggling to disclose the issue to affected Tesla owners without making the details public and also alerting malicious hackers.

he bug is now fixed, Colombo confirmed. TechCrunch held this story until the vulnerability could no longer be exploited. Colombo published his findings in a blog post.

Colombo told TechCrunch that the vulnerabilities were found in TeslaMate, a free-to-download logging software used by Tesla owners to connect to their vehicles and access their cars’ otherwise hidden data — their car’s energy consumption, location history, driving statistics and other granular data for troubleshooting and diagnosing problems.

https://techcrunch.com/2022/01/24/teslamate-bug-teslas-exposed-remote/

Hackers could remotely turn off lights, honk, mess with Tesla's infotainment system

TechCrunch

2023

Bugs allowed anyone to remotely unlock doors, honk the horn and start the car

Lorenzo Franceschi-Bicchierai • March 28, 2023

Thanks to three vulnerabilities chained together, malicious hackers could remotely hack into a Tesla, turn off the lights, honk the horn, open the trunk, activate the windshield wipers and mess with the infotainment system, according to security researchers.

The researchers, who work for security firm Synacktiv, found the vulnerabilities and showcased them at the Pwn2Own conference in Vancouver last week. The worst-case scenario allowed by these vulnerabilities, at least as far as the researchers know, is to mess with a driver with some annoying, and potentially disruptive tactics. The good news, at least according to what Tesla told the researchers, is that they couldn't have turned on and off the car, or steered the wheel.

https://techcrunch.com/2023/03/28/hackers-could-remotely-turn-off-lights-honk-mess-with-teslas-infotainment-system/

Tesla hackers win $200k and Model 3 for finding new vulnerability

electrek

2024

Bugs allowed anyone to remotely unlock doors, honk the horn and start the car

Lorenzo Franceschi-Bicchierai • March 28, 2023

Tesla hackers have won $200,000 and a brand-new Model 3 for finding a new vulnerability in the automaker's system. For years now, Tesla has been investing a lot in cybersecurity and working closely with whitehat hackers. The automaker has been participating in the Pwn2Own hacking competition by offering large prizes and its electric cars for hacking challengers.

The idea is to encourage and reward "good guy" hackers to find vulnerabilities and help Tesla fixed them before the "bad guys" get to them.

This strategy has enabled Tesla to patch dozens, if not hundreds, of vulnerabilities in its systems before they can be exploited by malicious people.

It happened as recently as January when Zero Day Initiative, which is behind Pwn2Own, held a special event in Tokyo where a team of security researchers, Synacktiv, managed to chain some bugs to exploit Tesla's infotainment system.

https://electrek.co/2024/03/21/tesla-hackers-win-200k-model-3-finding-new-vulnerability/

Tire pressure sensors

- **Tire pressure monitors are insecure**
  - Present in all cars since 2008
- **Pressure sensors communicate wirelessly, allowing attacks from nearby vehicles**
- **Each sensor contains a unique ID**
  - But the ID is not encrypted and can be obtained via eavesdropping

Autonomous driving sensor attacks

- **Radar**
  - Signal generation can simulate another vehicle in front of the car
  - Jamming can make the vehicle in front "disappear"
- **Ultrasonic sensors**
  - Used for self-parking & *summon* feature
  - Arduino-based computer used to trick a Tesla into thinking there's an imaginary object in front of it
  - Another approach: Wrap object in acoustic dampening foam
- **Cameras**
  - No great attacks yet: lasers can create permanent dead pixels
  - Visual jamming causes the car to give up on autopilot and warn the driver

https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/

GPS

- **GPS systems are crucial for navigation (including weapons) and often used as an accurate time source**
- **GPS emulators can spoof GPS signals**
  - Used to cost thousands of $
  - Can now be done cheaply with a software-defined radio and code from GitHub

NewScientist

Unprecedented GPS jamming attack affects 1600 aircraft over Europe

Jeremy Hsu • 29 March 2024

A 63-hour-long marathon of GPS jamming attacks disrupted global satellite navigation systems for hundreds of aircraft flying through the Baltic region – and Russia is thought to be responsible

https://www.newscientist.com/article/2424678-unprecedented-gps-jamming-attack-affects-1600-aircraft-over-europe/

July 2013

$80 million yacht hijacked by students spoofing GPS signals

https://nakedsecurity.sophos.com/2013/07/31/80-million-yacht-hijacked-by-students-spoofing-gps-signals/

IoT Problems

- **It's not a computer!**
  - Users & designers don't think (much) about security
  - But many IoT devices have powerful processors & network connectivity
- **Often no firmware updates**
  - Often no mechanisms for update
  - Little customer incentive to update
    - It works; who wants to figure out how to update a light switch?
  - No manufacturer incentives (especially for supportings old devices)
- **No user notifications**
- **No ability to install host-based firewalls or tripwire software**

IoT Problems

- **Does a toaster need to run Linux?**
  - Smaller operating systems have smaller attack surfaces
  - But … embedded microcontrollers may not have much of a security stack
  - Lack of skills to strip down the OS to bare essentials & secure it
- **Weak understanding of security mechanisms and protocols**
  - No public security reviews (or no reviews at all?)
- **It's not a fun problem**
  - The best minds are working on getting you to see more ads

AI Threats

AI, Machine Learning, & Computer Vision

- We don't understand deep learning
- We don't write the algorithms – we just feed data

Tesla Autopilot's safety questioned after latest fatal motorcycle crash

Matt McFarland • October 17, 2022

Tesla's Autopilot was involved in a third fatal motorcycle crash this summer, raising questions about the driver-assist system's ability to operate safely.

Intelligent Machines

The Dark Secret at the Heart of AI

No one really knows how the most advanced algorithms do what they do. That could be a problem.

by Will Knight April 11, 2017

Last year, a strange self-driving car was released onto the quiet roads of Monmouth County, New Jersey. The experimental vehicle, developed by researchers at the chip maker Nvidia, didn't look different from other autonomous cars, but it was unlike anything demonstrated by Google, Tesla, or General Motors, and it showed the rising power of artificial intelligence. The car didn't follow a single instruction provided by an engineer or programmer. Instead, it relied entirely on an algorithm that had taught itself to drive by watching a human do it.

https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

Object Recognition is Hard – With Consequences

CNN

Tesla Autopilot's safety questioned after latest fatal motorcycle crash

Matt McFarland • October 17, 2022

Tesla's Autopilot was involved in a third fatal motorcycle crash this summer, raising questions about the driver-assist system's ability to operate safely.

https://www.cnn.com/2022/10/17/business/tesla-motorcycle-crashes-autopilot/index.html

electrek

Tesla driver arrested for homicide after running over motorcyclist on Autopilot

Fred Lambert • April 23, 2024

The man, 56, had activated Tesla's Autopilot feature. He was using his phone when he heard a bang as his car lurched forward and crashed into the motorcycle in front of him, troopers wrote.

https://electrek.co/2024/04/23/tesla-driver-arrested-homicide-running-over-motorcyclist-autopilot/

CBS NEWS

Tesla cars involved in 16 crashes with emergency vehicles, regulators say

June 9, 2023

A U.S. investigation into Tesla vehicles operating on partially automated driving systems that have crashed into parked emergency vehicles has moved a step closer to a recall.

https://www.cbsnews.com/news/tesla-cars-crashes-emergency-vehicles/

Image Recognition

Identified as a **45 mph** sign

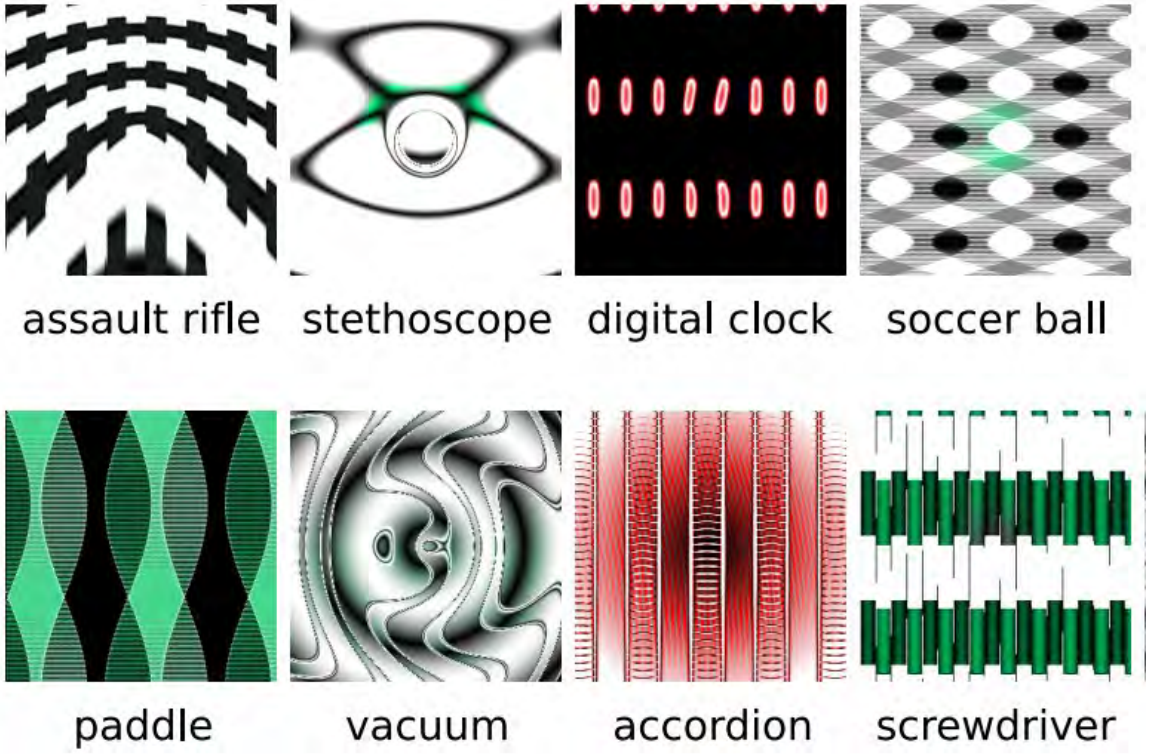
Also identified as a **45 mph** sign
… 100% of the time

https://arstechnica.com/cars/2017/09/hacking-street-signs-with-stickers-could-confuse-self-driving-cars/

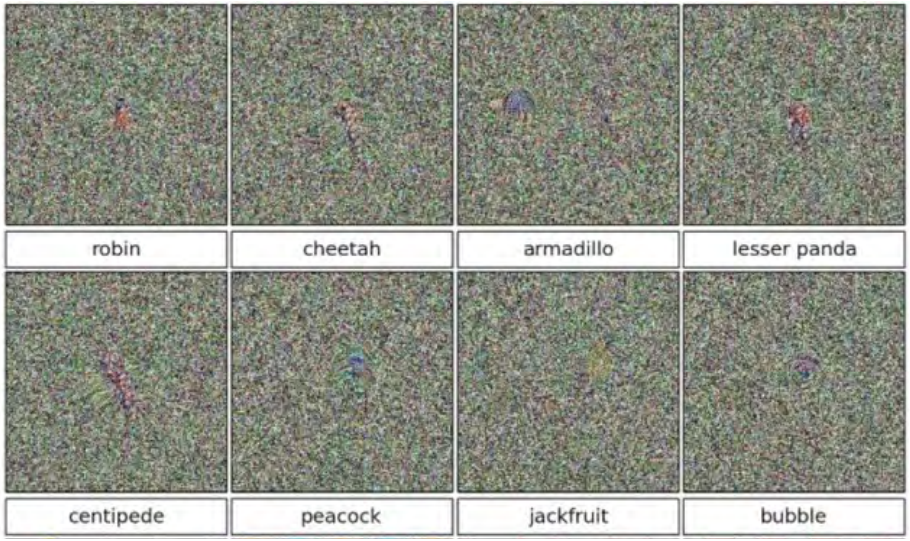
Adversarial patch fools AI vision

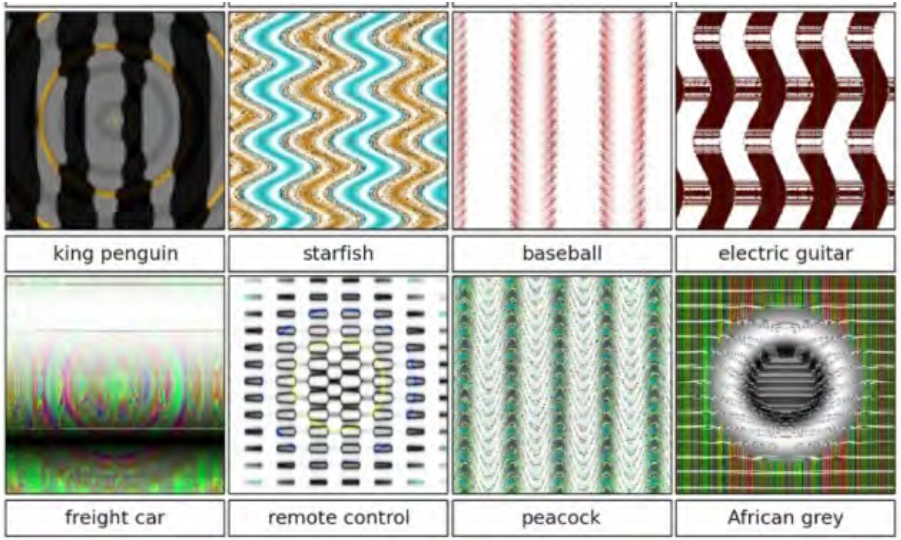
This is a person This one is invisible

https://techxplore.com/news/2019-04-adversarial-patch-ai.html



http://www.theverge.com/2017/4/12/15271874/ai-adversarial-images-fooling-attacks-artificial-intelligence

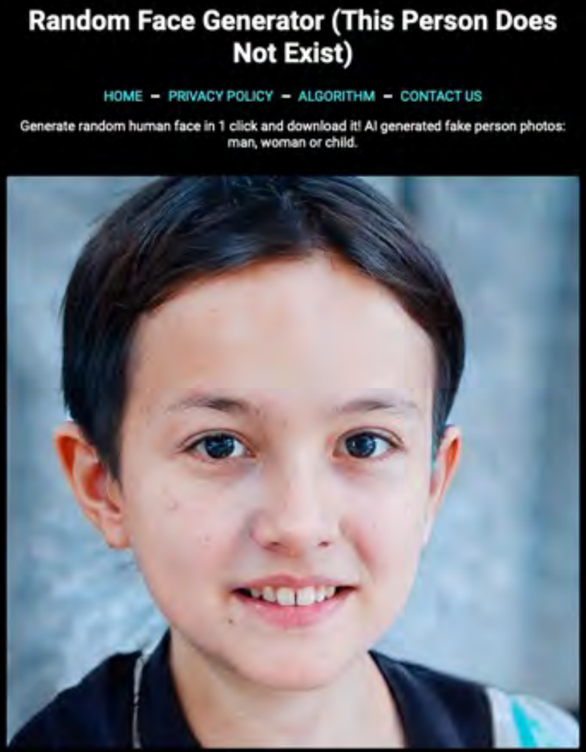




https://www.extremetech.com/extreme/195789-bad-news-future-computers-are-easily-tricked-by-optical-illusions-too


Random Face Generator (This Person Does Not Exist)
HOME – PRIVACY POLICY – ALGORITHM – CONTACT US
Generate random human face in 1 click and download it! AI generated fake person photos: man, woman or child.


Random Face Generator (This Person Does Not Exist)
HOME – PRIVACY POLICY – ALGORITHM – CONTACT US
Generate random human face in 1 click and download it! AI generated fake person photos: man, woman or child.


Random Face Generator (This Person Does Not Exist)
HOME – PRIVACY POLICY – ALGORITHM – CONTACT US
Generate random human face in 1 click and download it! AI generated fake person photos: man, woman or child.

Hacked Ukrainian TV Station Plays Laughably Bad Volodymyr Zelenskyy Deepfake

March 2, 2022

Experts have warned for years that deepfakes could be weaponized during a war of misinformation. Acting on this advice, earlier this month the Ukrainian Center for Strategic Communications and Information Security warned that Putin may utilize deepfakes to make it look like President Zelensky had surrendered.

…

In the video, fake Zelensky says that "it turned out to be not so easy being the president", before directing soldiers to "lay down arms and return to your families. It is not worth it dying in this war. My advice to you is to live. I am going to do the same."

StratcomCentreUA:
Imagine seeing Vladimir Zelensky on TV making a surrender statement. You see it, you hear it - so it's true. But this is not the truth. This is deepfake technology.

This will not be a real video, but created through machine learning algorithms.

Videos made through such technologies are almost impossible to distinguish from the real ones.

Be aware - this is a fake! His goal is to disorient, sow panic, disbelieve citizens and incite our troops to retreat.

Rest assured - Ukraine will not capitulate!

Russia can only invent a fake victory, close the Internet and all contacts with the rest of the world.

https://www.iflscience.com/technology/hacked-ukrainian-tv-station-plays-laughably-bad-volodymyr-zelenskyy-deepfake/

https://www.facebook.com/StratcomCentreUA/posts/300254888841165

https://www.youtube.com/watch?v=pfsdvbacYac

How AI is resurrecting dead Indian politicians as election looms

Nilesh Christopher • February 12, 2024

Bengaluru, India – On January 23, an icon of Indian cinema and politics, M Karunanidhi appeared before a live audience on a large projected screen, to congratulate his 82-year-old friend and fellow politician TR Baalu on the launch of his autobiographical book.

Dressed in his trademark black sunglasses, white shirt, and a yellow shawl around his shoulders — Karunanidhi's style was spot on. In his eight-minute speech, the veteran poet-turned-politician congratulated the book's author but was also effusive in his praise for the able leadership of MK Stalin, his son and the current leader of the state.

Karunanidhi has been dead since 2018.

This was the third time, in the past six months, that the iconic leader of the Dravida Munnetra Kazhagam (DMK) party was resurrected using artificial intelligence (AI) for such public events.

https://www.aljazeera.com/economy/2024/2/12/how-ai-is-used-to-resurrect-dead-indian-politicians-as-elections-looms

Deepfake Software Fools Voice Authentication With 99% Success Rate

Creating a fake voice to trick authentication systems has never been so easy or effective.

Matthew Humphries • June 28, 2023

Computer scientists at the University of Waterloo figured out how to successfully fool voice authentication systems 99% of the time using deepfake voice creation software.

Andre Kassis, a Computer Security and Privacy PhD candidate at Waterloo, who is also the lead author of this research study, explains how voice authentication works:

"When enrolling in voice authentication, you are asked to repeat a certain phrase in your own voice. The system then extracts a unique vocal signature (voiceprint) from this provided phrase and stores it on a server ... For future authentication attempts, you are asked to repeat a different phrase and the features extracted from it are compared to the voiceprint you have saved in the system to determine whether access should be granted."

The team at Waterloo beat the authentication by using machine learning-enabled deepfake software to generate a copy of a voice. All the software needs is five minutes of recorded voice audio from which to learn to be a convincing fake. Even spoofing countermeasures employed by the voice authentication systems don't flag the fake voice because a program written by the team removes markers from the deepfake audio that "betray it is computer-generated."

https://www.pcmag.com/news/deepfake-software-fools-voice-authentication-with-99-success-rate

Other AI concerns

- **Model poisoning**
  - AI models are trained on large datasets. If an attacker can inject malicious data into the training set, the model's behavior can change
  - E.g., misclassify dangerous input as safe
- **AI-based attacks – lowers the barrier to entry**
  - AI can write malware for you
  - Perform social engineering
- **Privacy**
  - Leaking private data
- **Writing insecure code – or helping you to write it**
  - Most code is bad and buggy. If AI is trained on this, what will it generate?
  - "a recent research study looked at the result of developing 89 different scenarios for Copilot to complete. Of the 1,689 programs that were produced, approximately 40 percent were found to contain vulnerabilities." – https://spectrum.ieee.org/ai-software

AI hallucinates software packages and devs download them – even if potentially poisoned with malware

The Register

Simply look out for libraries imagined by ML and make them real, with actual malicious code. No wait, don't do that

icon Thomas Claburn • March 28, 2024

Several big businesses have published source code that incorporates a software package previously hallucinated by generative AI.

Not only that but someone, having spotted this reoccurring hallucination, had turned that made-up dependency into a real one, which was subsequently downloaded and installed thousands of times by developers as a result of the AI's bad advice, we've learned. If the package was laced with actual malware, rather than being a benign test, the results could have been disastrous.

According to Bar Lanyado, security researcher at Lasso Security, one of the businesses fooled by AI into incorporating the package is Alibaba, which at the time of writing still includes a pip command to download the Python package huggingface-cli in its GraphTranslator installation instructions.

https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/

Researchers train AI chatbots to 'jailbreak' rival chatbots - and automate the process

tom's HARDWARE

'Masterkey' method means that if a Chatbot is updated, a new jailbreak can be automatically applied.

Roshan Ashraf Shaikh • December 31, 2023

NTU Researchers were able to jailbreak popular AI chatbots including ChatGPT, Google Bard, and Bing Chat. With the jailbreaks in place, targetted chatbots would generate valid responses to malicious queries, thereby testing the limits of large language model (LLM) ethics. This research was done by Professor Liu Yang and NTU PhD students Mr Deng Gelei and Mr Liu Yi who co-authored the paper and were able to create proof-of-concept attack methods.

The method used to jailbreak an AI chatbot, as devised by NTU researchers, is called Masterkey. It is a two-fold method where the attacker would reverse engineer an LLM's defense mechanisms. Then, with this acquired data, the attacker would teach another LLM to learn how to create a bypass. This way, a 'Masterkey' is created and used to attack fortified LLM chatbots, even if later patched by developers.

AI's Strength is its Own Achilles Heel

Professor Yang explained that jailbreaking was possible due to an LLM chatbot's ability to learn and adapt, thus becoming an attack vector to rivals and itself. Because of its ability to learn and adapt, even an AI with safeguards and a list of banned keywords, typically used to prevent generating violent and harmful content, can be bypassed using another trained AI. All it needs to do is outsmart the AI chatbot to circumvent blacklisted keywords. Once this is done, it can take input from humans to generate violent, unethical, or criminal content.

https://www.tomshardware.com/tech-industry/artificial-intelligence/researchers-train-ai-chatbots-to-jailbreak-rival-chatbots-and-automate-the-process

Researchers train AI chatbots to 'jailbreak' rival chatbots - and automate the process

tom's HARDWARE

'Masterkey' method means that if a Chatbot is updated, a new jailbreak can be automatically applied.

Roshan Ashraf Shaikh • December 31, 2023

NTU Researchers were able to jailbreak popular AI chatbots including ChatGPT, Google Bard, and Bing Chat. With the jailbreaks in place, targetted chatbots would generate valid responses to malicious queries, thereby testing the limits of large language model (LLM) ethics. This research was done by Professor Liu Yang and NTU PhD students Mr Deng Gelei and Mr Liu Yi who co-authored the paper and were able to create proof-of-concept attack methods.

The method used to jailbreak an AI chatbot, as devised by NTU researchers, is called Masterkey. It is a two-fold method where the attacker would reverse engineer an LLM's defense mechanisms. Then, with this acquired data, the attacker would teach another LLM to learn how to create a bypass. This way, a 'Masterkey' is created and used to attack fortified LLM chatbots, even if later patched by developers.

AI's Strength is its Own Achilles Heel

Professor Yang explained that jailbreaking was possible due to an LLM chatbot's ability to learn and adapt, thus becoming an attack vector to rivals and itself. Because of its ability to learn and adapt, even an AI with safeguards and a list of banned keywords, typically used to prevent generating violent and harmful content, can be bypassed using another trained AI. All it needs to do is outsmart the AI chatbot to circumvent blacklisted keywords. Once this is done, it can take input from humans to generate violent, unethical, or criminal content.

https://www.tomshardware.com/tech-industry/artificial-intelligence/researchers-train-ai-chatbots-to-jailbreak-rival-chatbots-and-automate-the-process

The End.