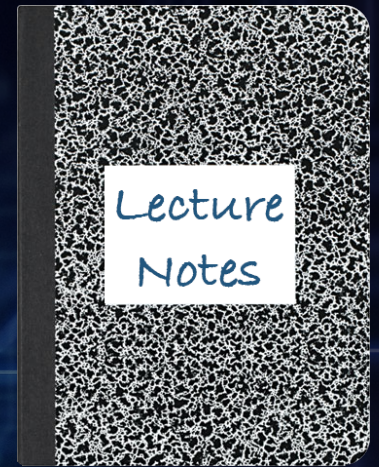


CS 419: Computer Security

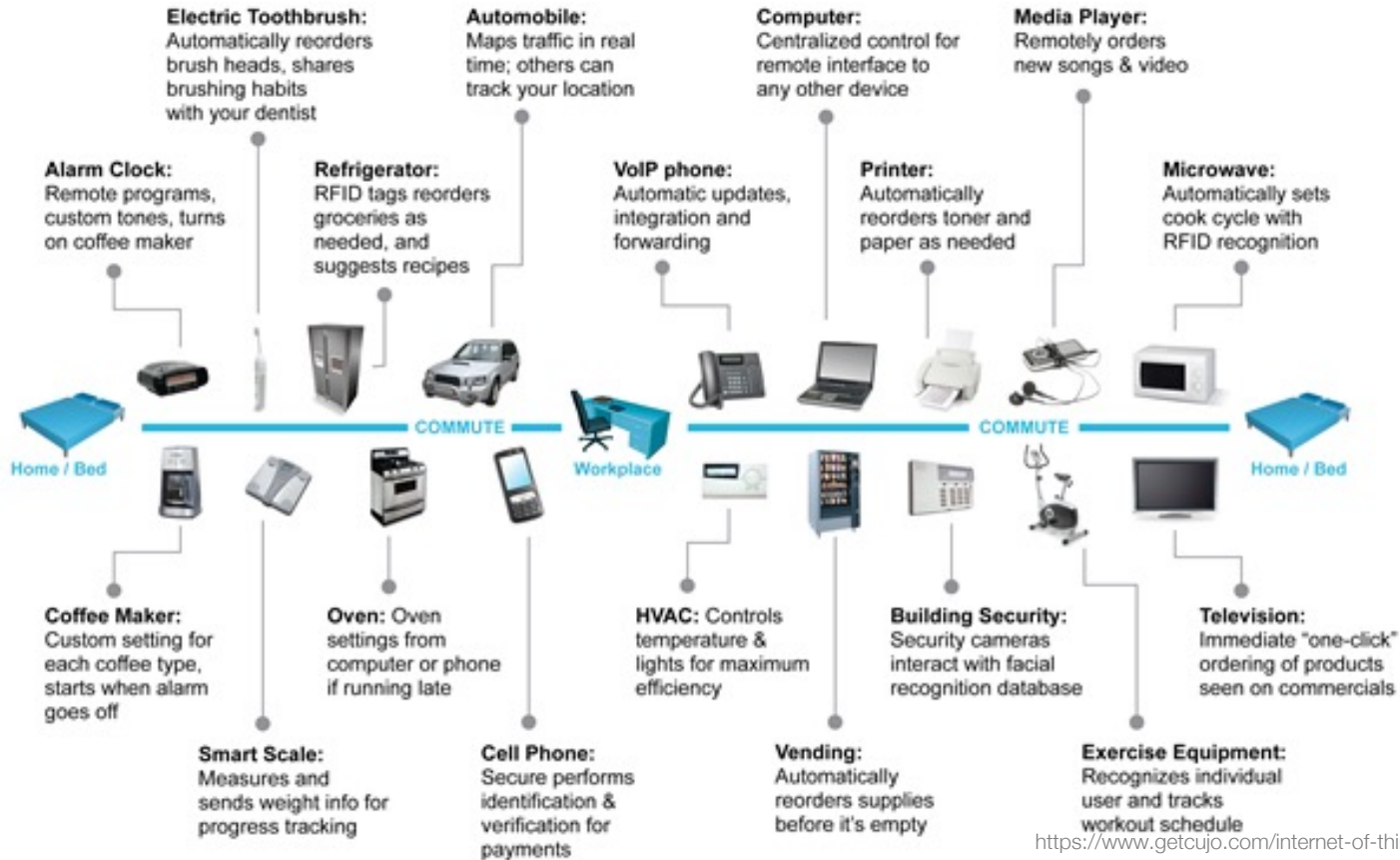
Week 14: Security Concerns With the Internet of Things



Paul Krzyzanowski

© 2022 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.

The landscape: ~46-72 billion IoT devices in 2022



<https://www.getcujo.com/internet-of-things-security-device-cujo/>
<https://connect.comptia.org/blog/internet-of-things-stats-facts>

The Internet of Things (IoT)

The number of targets is growing exponentially!

- **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
- **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://connect.comptia.org/blog/internet-of-things-stats-facts>

<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
- **Wikipedia page got 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
- DDoS attack to disable it to hide your actions

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.

<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

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/>

April 2019: Malware in PC Videogames

- **Supply Chain Hackers Snuck Malware Into Videogames**
- **Hackers don't target individual devices or networks**
- **Instead – target companies that distribute code used by targets**
- **Hackers targeted Asus in early 2019**
- **Same hackers corrupted versions of Microsoft Visual Studio**
- **Three different videogame companies used this in their development**
 - The games were digitally signed & trusted by users
 - Infect hundreds of thousands of victims with backdoors

- **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.

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>

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



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**

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 Networks Security Advisories / CVE-2020-2021




CVE-2020-2021 PAN-OS: Authentication Bypass in SAML Authentication




Severity 10 - CRITICAL

Attack Vector NETWORK	Attack Complexity LOW
Privileges Required NONE	User Interaction NONE
Scope CHANGED	Confidentiality Impact HIGH
Integrity Impact HIGH	Availability Impact HIGH

NVD **JSON**



Published **2020-06-29**
Updated **2020-06-29**
Reference **PAN-148988**
Discovered **externally**

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>

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/wiki/index.php/Main_Page
 - Buffer overflows, file system access
 - Firmware updates, memory access
 - Credential disclosure

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



Eve Peyser

2/06/17 8:46pm · Filed to: HACKERS! ▾



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.”

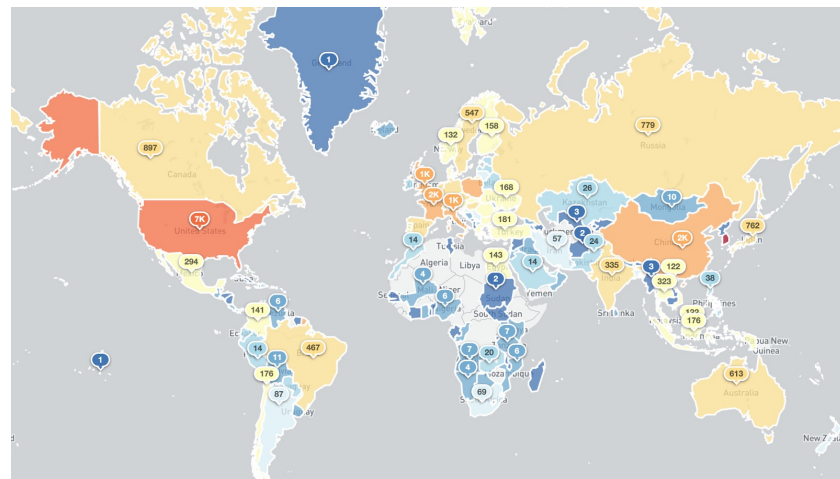
Exposed Printers



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.

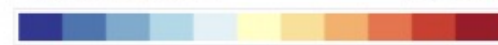


Exposed IPv4 IPP services by country (28th December 2020)

Legend

Reported Unique IPs

(log. scale)



1 IP

40,000 IPs

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

Exposed Printers

South Korea
36.3K

United States
7.9K

Taiwan
6.7K

France
2.8K

Italy
2K

China
2K

United Kingdom
1.6K

Hong Kong
1.5K

Poland
1.5K

Russia
792

Belgium
741

Sweden
648

Netherlands
603

Germany
1.4K

Switzerland
597

Australia
593

Brazil
562

Czech Republic
474

Hungary
449

Canada
1.2K

Portugal
374

Greece
251

India
244

Turkey
209

Indonesia
208

Colombia
206

Egypt
198

Thailand
359

Slovakia
190

Finland
180

Norway
160

Bulgaria
158

Singapore
150

Israel
140

Spain
972

Mexico
359

Chile
180

Argentina
110

South Africa
100

Costa Rica
100

Macao
100

Peru
100

Denmark
100

France
100

Germany
100

Italy
100

Japan
100

Poland
100

Russia
100

Sweden
100

Switzerland
100

United States
100

United Kingdom
100

Other
100

...

EU
184

Serbia
100

Vietnam
100

Denmark
177

Slovenia
100

Belgium
100

...

Austria
352

Denmark
177

Ukraine
172

Romania
317

Moldova
100

...

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



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/>

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

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 through the entire world's air traffic control."

Air Traffic Control system is being overhauled ... expected completion by 2025

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'

<http://www.csoonline.com/article/2132793/access-control/hackers-say-coming-air-traffic-control-system-lets-them-hijack-planes.html>

M2M (machine-to-machine)

**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

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

Hack a Vending Machine with a Special Code

BY DAYLIGHTSPOOL 07/15/2015 7:38 PM

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.

MOTHERBOARD BLOG

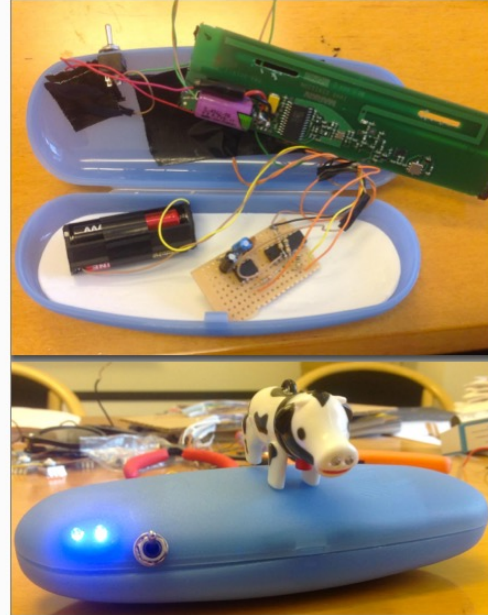
To Move Drugs, Traffickers Are Hacking Shipping Containers

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

May 1, 2022

FORTINET



```
text:00552A88 mov     eax, [esp+48h+var_48]
text:00552A89 mov     ecx, [esp+48h+var_44]
text:00552A8F mov     [esp+48h+var_48], 0
text:00552A96 mov     [esp+48h+var_44], eax
text:00552A9A mov     [esp+48h+var_40]
text:00552A9E call    runtime_stringtoasciibyte
text:00552AA3 mov     eax, [esp+48h+var_34]
text:00552AA4 mov     [esp+48h+var_48], eax
text:00552AAE mov     [esp+48h+var_48], edx
text:00552AB2 mov     [esp+48h+var_44], ecx
text:00552AB6 mov     [esp+48h+var_40], eax
text:00552ABA call    encoding_pen_Decode
text:00552ABF mov     eax, [esp+48h+var_3C]
```

THREAT RESEARCH

EKANS Ransomware Targeting OT ICS Systems

By Ben Hunter and Fred Gutierrez | July 01, 2020

FortiGuard Labs Threat Research Report

Affected platforms: Windows Operating Systems
Impacted parties: Industrial Control Systems and a variety of applications
Impact: Data Encryption for Impact – Mitre ID:T1486
Severity level: High

Introduction

According to the 2020 Verizon breach report, ransomware accounted for 27% of malware incidents last year. This may not seem like a lot, but when you think of the impact it has on an organization you can understand why it's often the malware that makes the news headlines. Over the last few years, the impact has worsened due to adversaries moving to a more targeted attack method, rather than the traditional "spray and pray" method of infecting as many potential victims as possible.

<https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems>

© 2022 Paul Krzyzanowski

25

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

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

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 **GIZMODO** Runs Our Power Grids, It Turns Out

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**

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

- **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

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)
- 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, car-connecting apps get to hackers too**
 - Locate a car, unlock it, turn it on, set climate control
- **Kaspersky found most of connected car apps lack even the most basic security defenses**
- **You can drive a Tesla with only a phone app**

Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

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

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/>

This hack could take control of your Ford

THE PARALLAX

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/>

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

- **GPS systems are crucial for navigation (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

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/>

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/>

ANDY GREENBERG SECURITY

11.23.2020 07:00 AM

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

The company is rolling out a patch for the vulnerabilities, which allowed one researcher to break into a car in 90 seconds and drive away.



The technique takes advantage of a collection of security issues—both major and minor—in the Model X's keyless entry system. PHOTOGRAPH: CHRISTIAN CHARISIUS/GETTY IMAGES

AUGUST 27

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

Fred Lambert - Aug. 27th 2020 3:29 pm ET @FredericLambert



Remote control

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

NEWS

Hacker: 'Hundreds of thousands' of vehicles are at risk of attack

The best way to secure vehicles is by detecting attacks as they're happening



 By Lucas Mearian
Senior Reporter, Computerworld | JUL 23, 2015 3:03 AM PT

Jeep hack demonstrated (took about a year to figure out)

- Use cellular connection to Jeep's entertainment system or head unit to gain access to other systems
- Steps
 - Gain access to the vehicle's head unit/controller chip and firmware
 - Use head unit to compromise the vehicle's controller area network
 - Discover which CAN messaging can control various functions

Firmware update must be done over USB – so many users won't bother

<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

<http://www.computerworld.com/article/2951489/telematics/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html>

Other carjacks

- **Disable brakes, honk horn, jerk seat belt, take control of steering wheel**
 - But PC was wired into the OBD II port
- **Now wireless attacks are possible in some cars**
 - Same attacks +
 - Kill the engine
 - Engage brakes abruptly
 - Track location of a car



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 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, Machine Learning, & Computer Vision

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

Will you be able to fool a self-driving car?

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/>



Identified as a **45 mph** sign

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



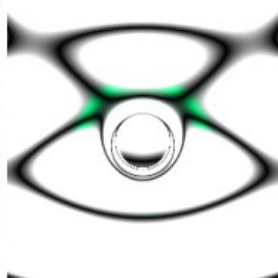
This is a person

This one is invisible

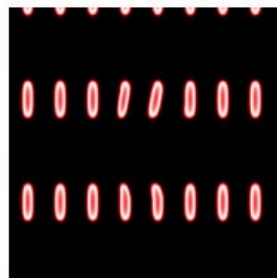
<https://techxplore.com/news/2019-04-adversarial-patch-ai.html>



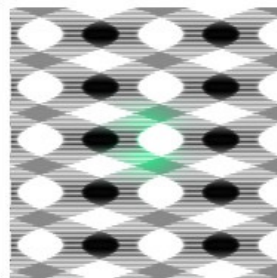
assault rifle



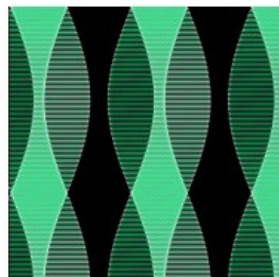
stethoscope



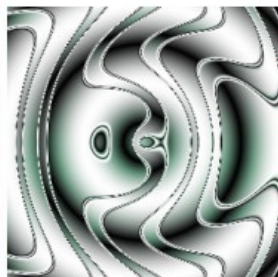
digital clock



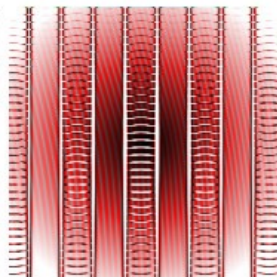
soccer ball



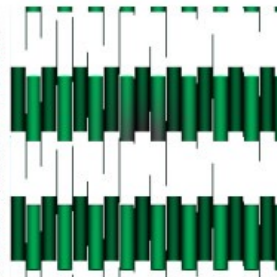
paddle



vacuum

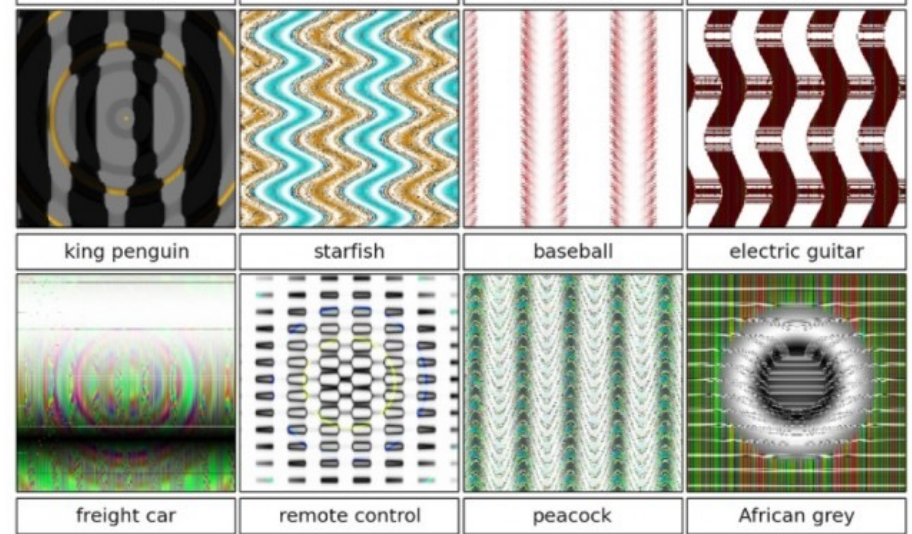
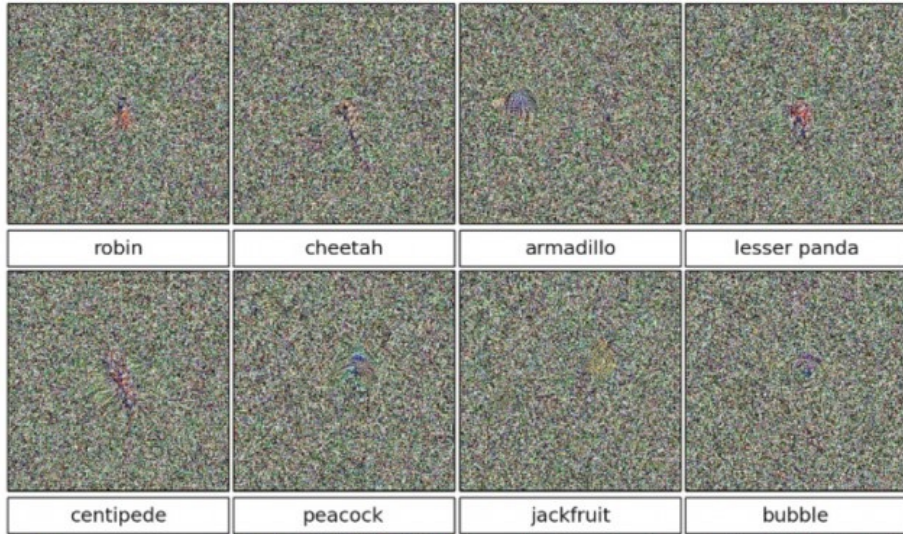


accordion



screwdriver

<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 Zelenskyy had surrendered.

...

In the video, fake Zelenskyy 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=pfsdYbacYac>

The End.

CS 419: Computer Security

Week 14: The Internet of Things (IoT)

Paul Krzyzanowski

© 2020 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.