CS 419: Computer Security

Week 14: The Internet of Things (IoT)

Paul Krzyzanowski

The landscape: ~30-50B devices in 2020

https://www.getcujo.com/internet-of-things-security-device-cujo/

The Internet of Things (IoT)

The number of targets is growing exponentially!

Threats

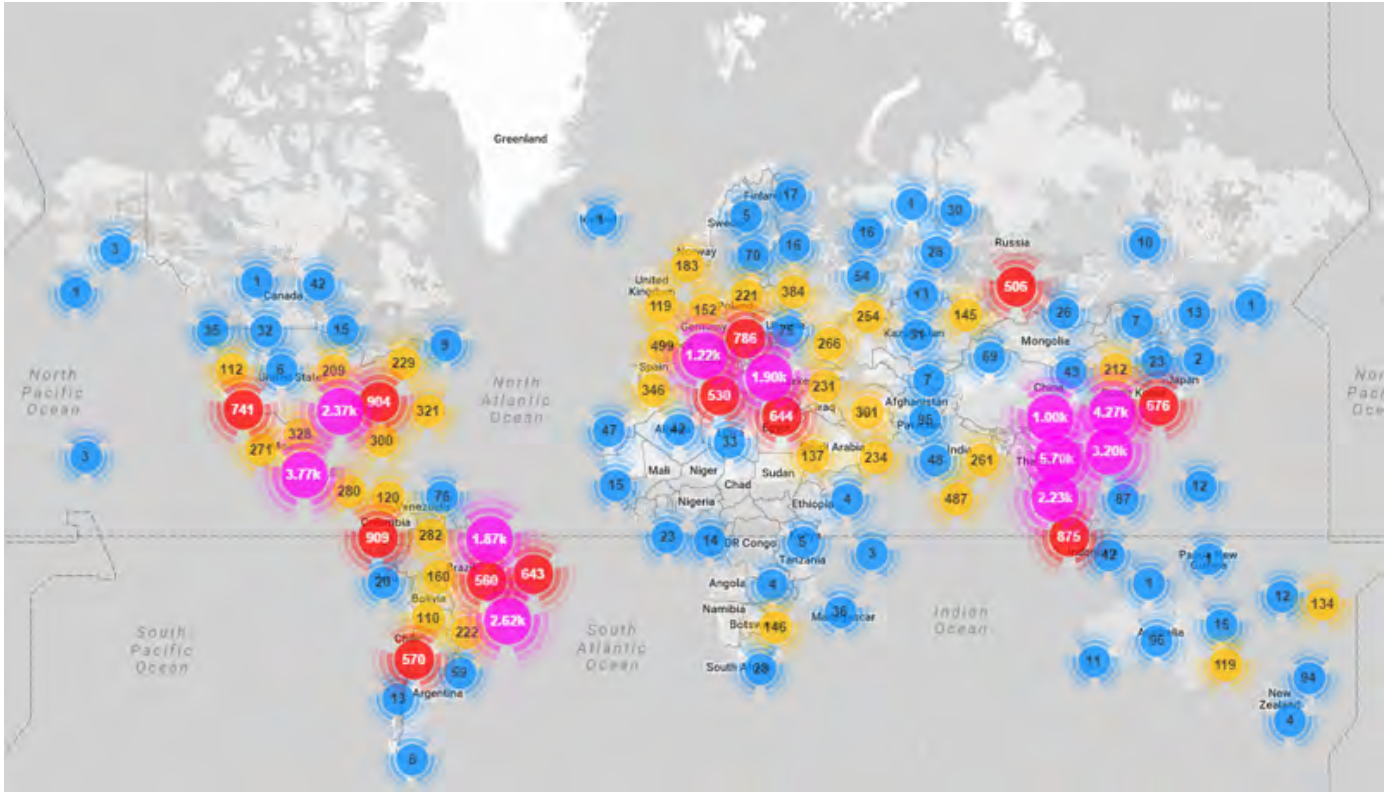
One Million IoT Devices Infected By Malware Driven DDoS Bonet

- **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
    - 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

      D-Link, Netgear, Huawei, Realtek devices
- **Denial of service on the device itself, sabotage**
- **Spying (privacy attacks)**

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

Mirai Botnet



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

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

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/

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 Prevention. Response. Notification. TODAY

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

Feb 5, 2017

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!

19.5K 40 5

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."

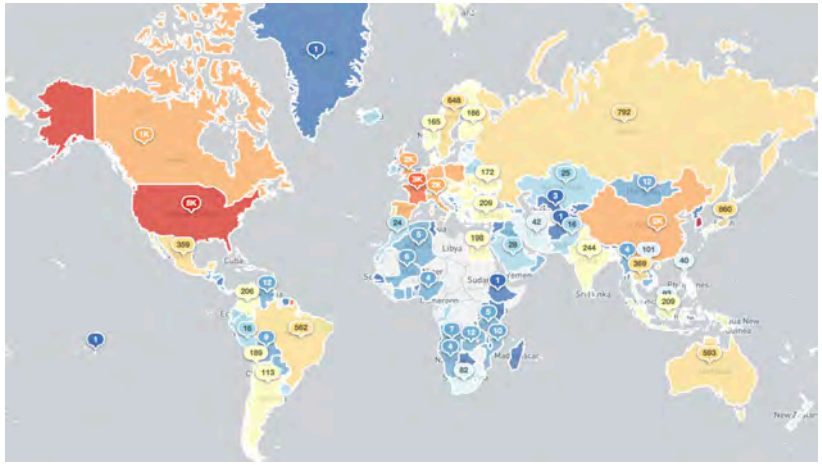
Exposed Printers

SHADOWSERVER

Open IPP Report – Exposed Printer Devices on the Internet

June 10, 2020

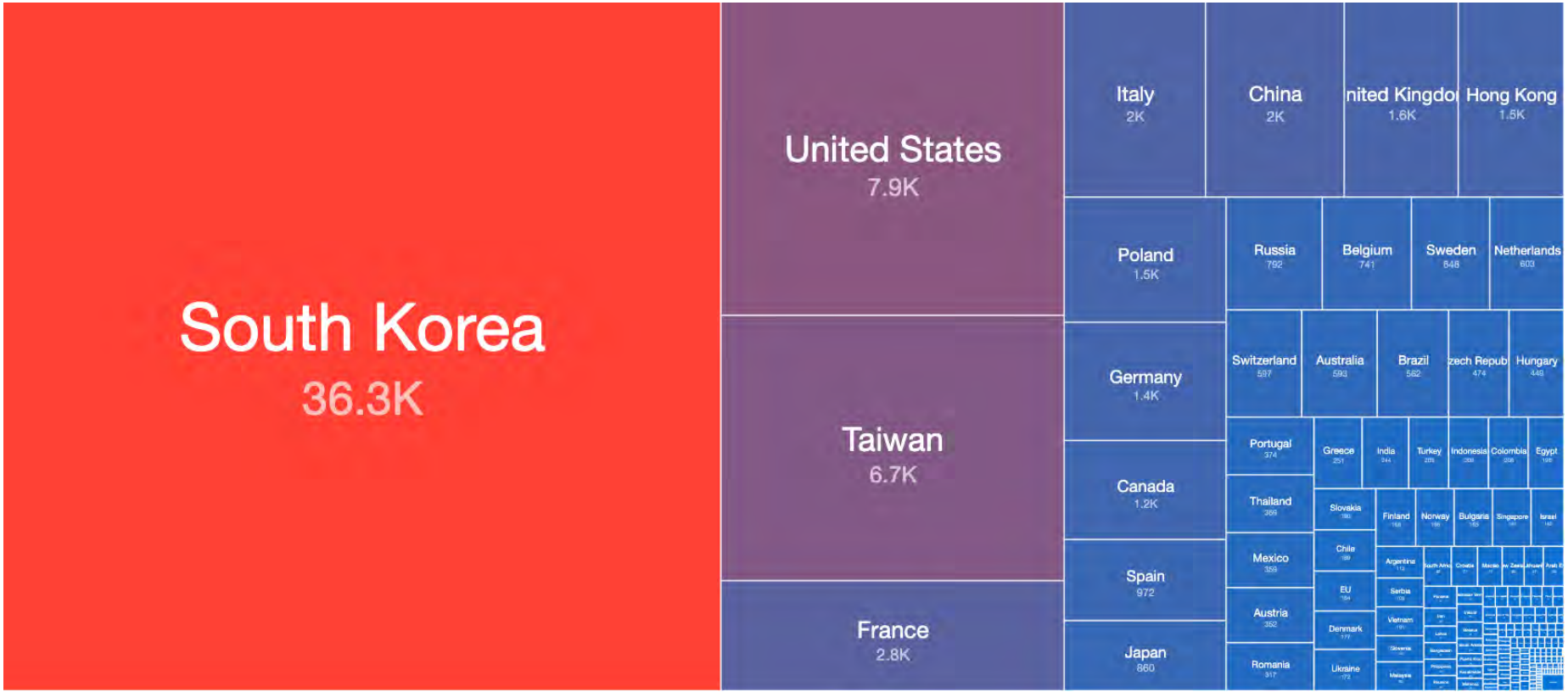
Our new Internet Printing Protocol (IPP) scan is the second (after the Open MQTT scan) IPv4 Internet-wide scan that we have enabled as part of our VARIoT efforts. It is aimed at uncovering printing devices which use IPP (a HTTP POST based protocol) that have been connected to the Internet without adequate 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 (7th June 2020)

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

Exposed Printers



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

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-vulnera

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 though 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)

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.

MOTHERBOARD BLOG

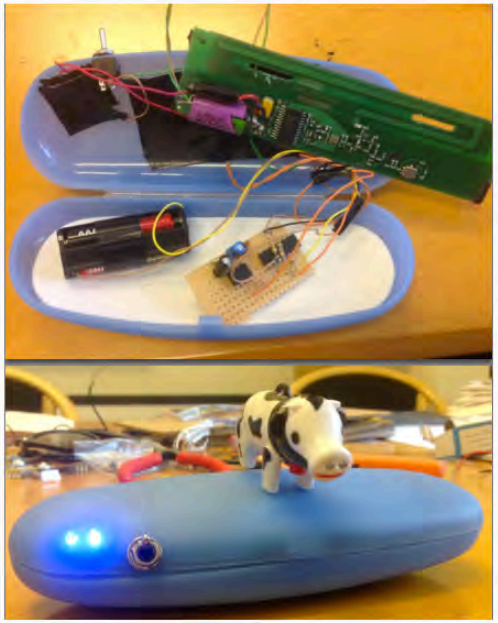
To Move Drugs, Traffickers Are Hacking Shipping Containers

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)

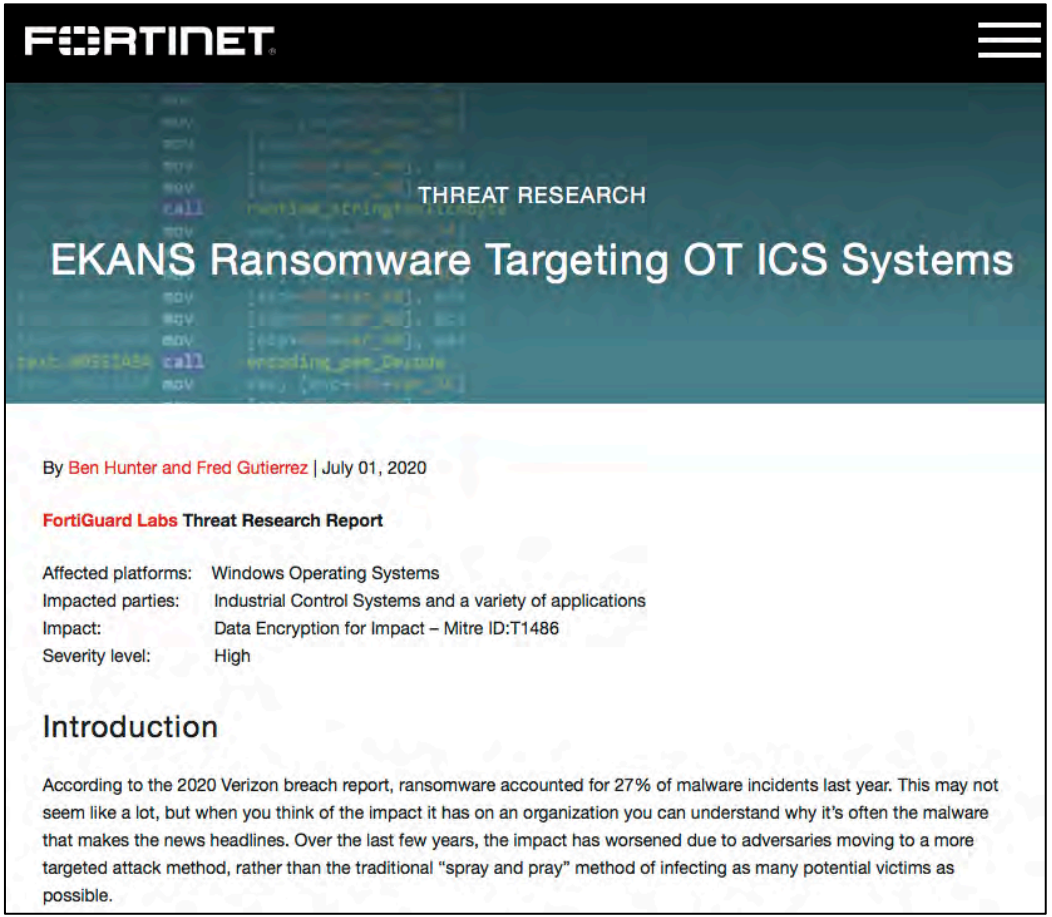
Sep 12, 2013 @ 04:44 PM



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



FORTINET

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

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 usedrs 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)
  - Controller area network (CAN) bus communicates between the head unit and all ECUs in the car
  - More care support 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**

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

- **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

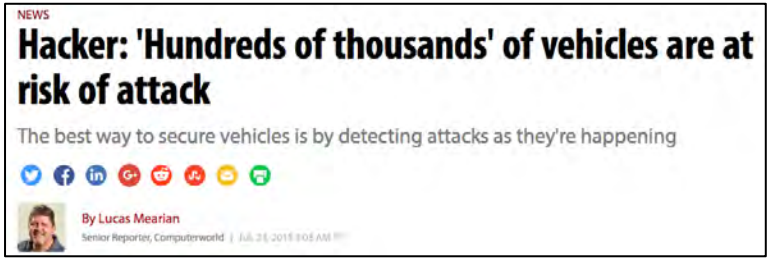
- **Radar**
  - Signal generation can simulate another vehicle in front of the car
  - Jamming can make the vehicle in front "disappear"
- **Ultrasonic sensors**
  - Used for self-parking & *summon* feature
  - Arduino-based computer used to trick a Tesla into thinking there's an imaginary object in 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/

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

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

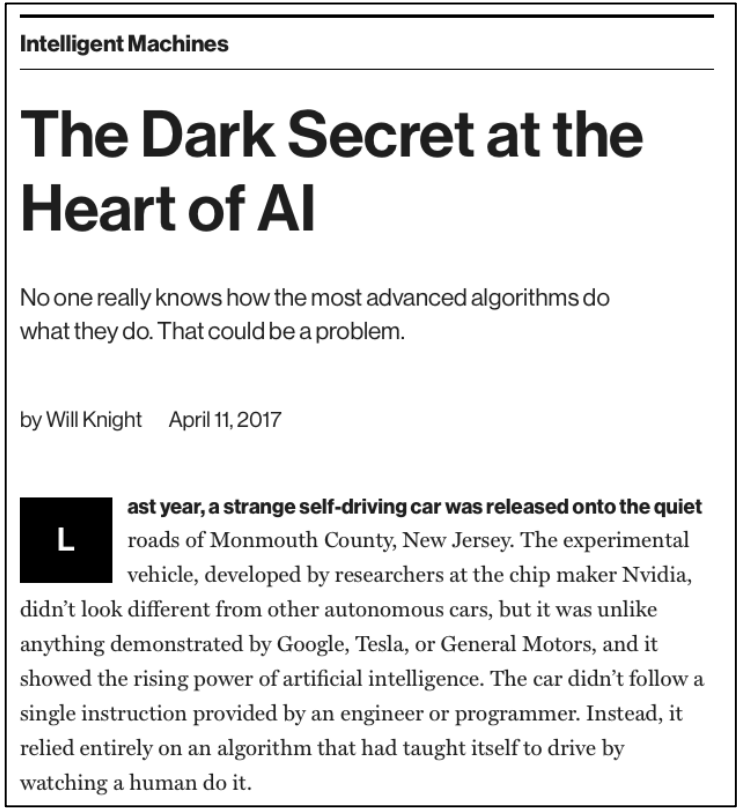
ANDY GREENBERG SECURITY 09.27.16 7:00 AM

TESLA RESPONDS TO CHINESE HACK WITH A MAJOR SECURITY UPGRADE

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

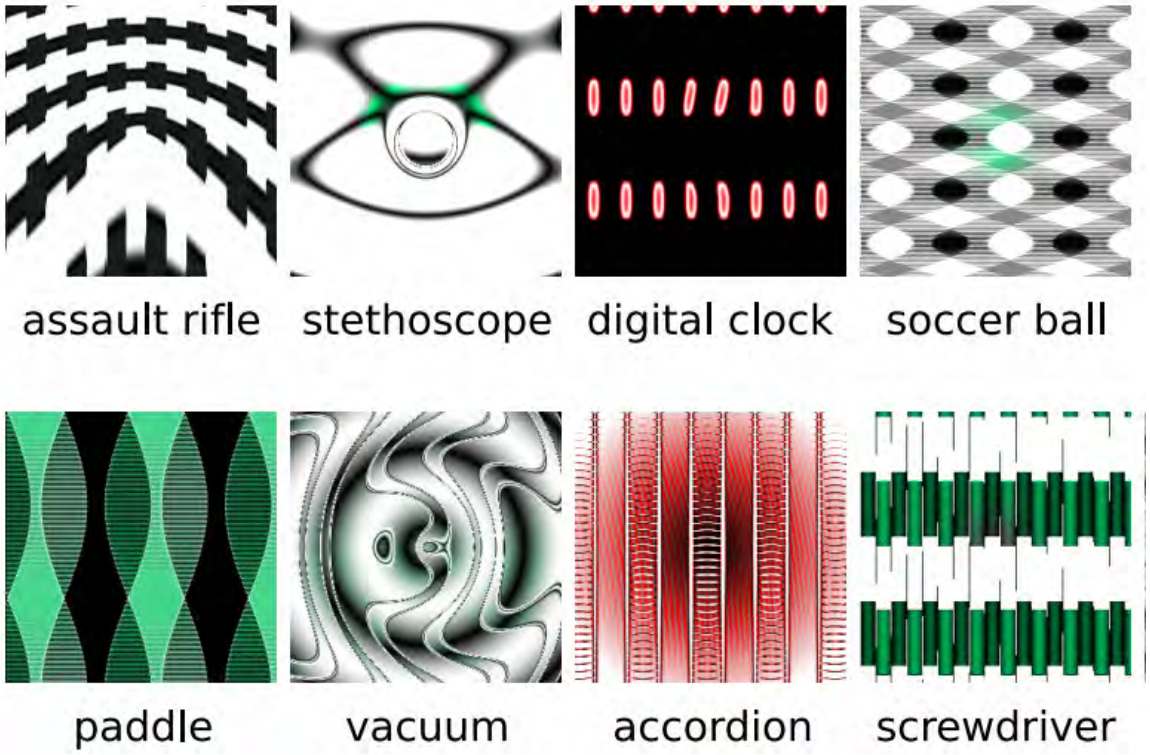
Identified as a **45 mph** sign
… 100% of the time

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

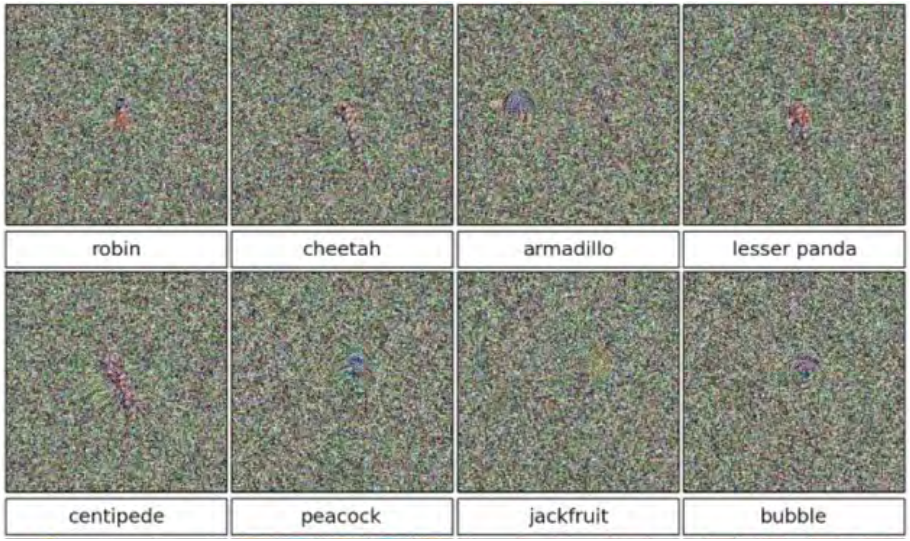
Adversarial patch fools AI vision

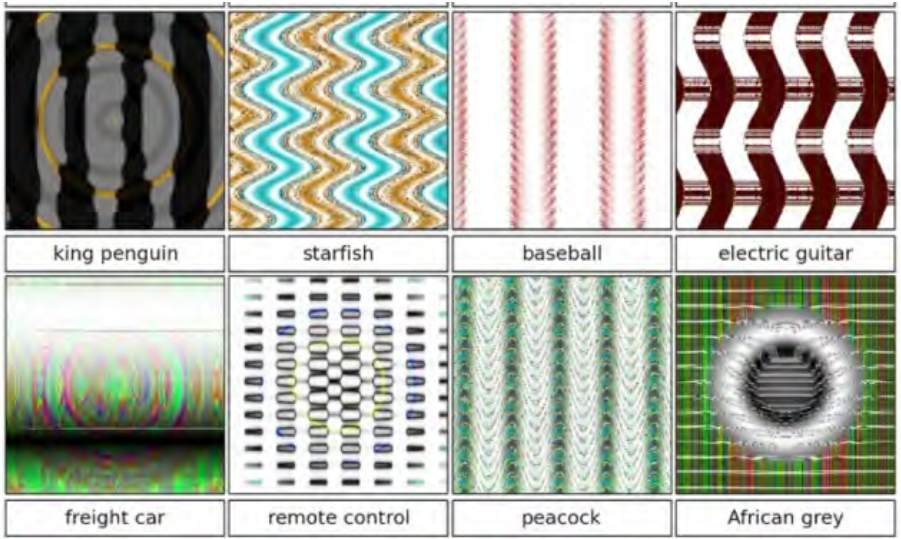
This is a person This one is invisible

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



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

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
- **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

The End.