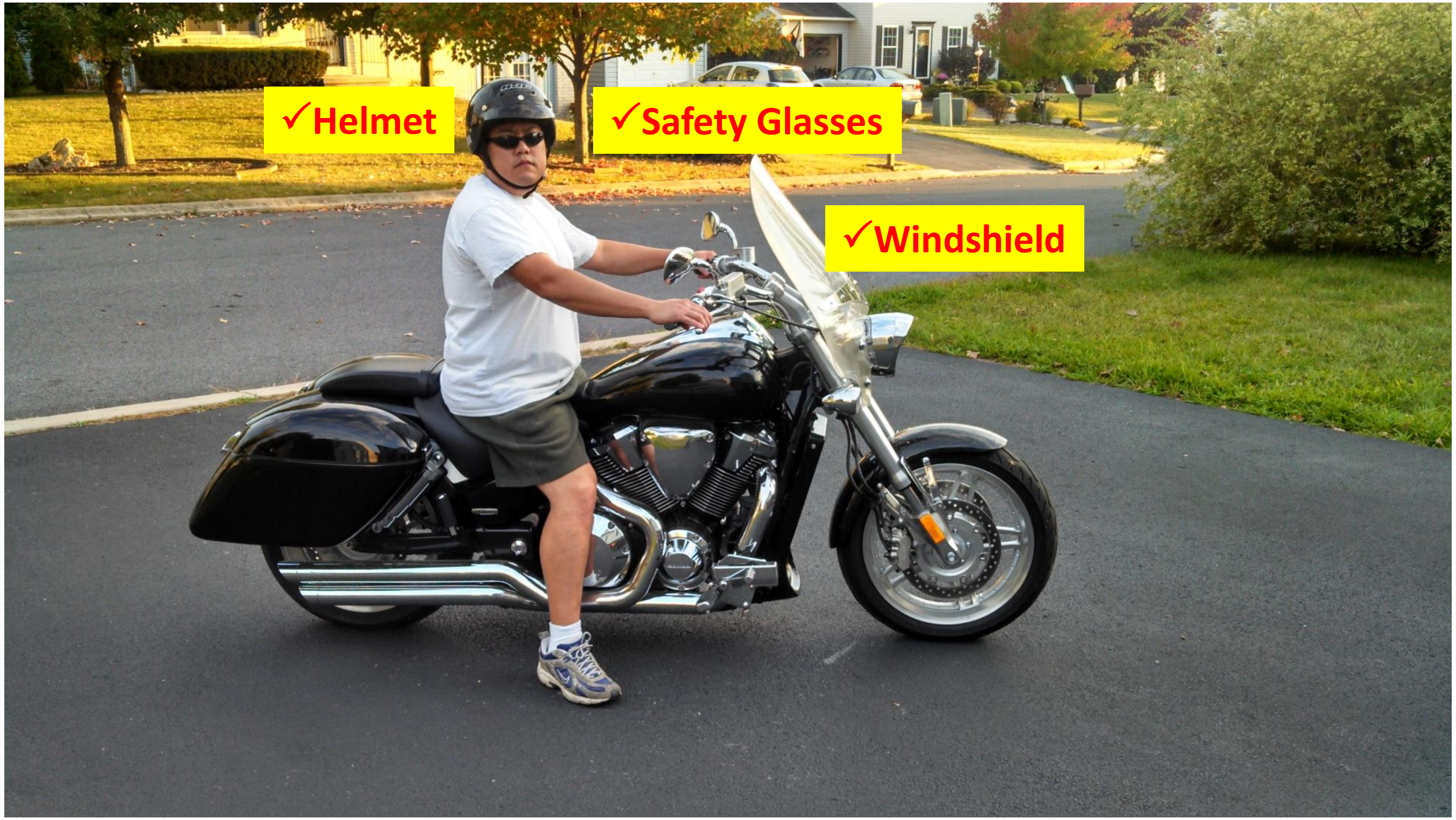
Click Here to Kill Everybody*

Randy Marchany Virginia Tech IT Security Office and Lab

Compliant



✓Helmet

✓Safety Glasses

✓Windshield

Secure!

Most Common Security Mistakes Made by Individuals (2001)

- Poor password management
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- **Not installing anti-virus software**
- Laptops on the loose
- Blabber mounts (file access open to the world)
- Plug and Play without protection
- Not reporting security violations
- Always behind the times (OS, application patches)
- Keeping an eye out inside the organization

Hacker Attack Goals

Over the past 30 years, Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion,ransomware)
- **DEFEND** accordingly

Border? What Border?

- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- **Internet 3.0 – mobile servers (containers, serverless), mobile endpoints (laptops, phones, tablets, IoT, ICS)**

Another View

- "As we **move our data outside of the firewall**, we have to adopt a zero-trust type model, " [Chris] Townshend said. "We are shifting our security enforcement out to the data itself, and **you have to have a security policy that follows that user no matter where that user is or what device they are using to access the data"**
  - "The new cyber landscape", Patrick Marshall, GCN Magazine, vol 37, #1
- In other words, **data & identity become the border.**

EDU (now) vs. Corporate Structure (future)

- **Administrative** – the process that runs the institution (**CORP**)
  - Payroll, HR, Purchasing, Facilities, Legal, etc.
  - **Security model closest to corporate model**

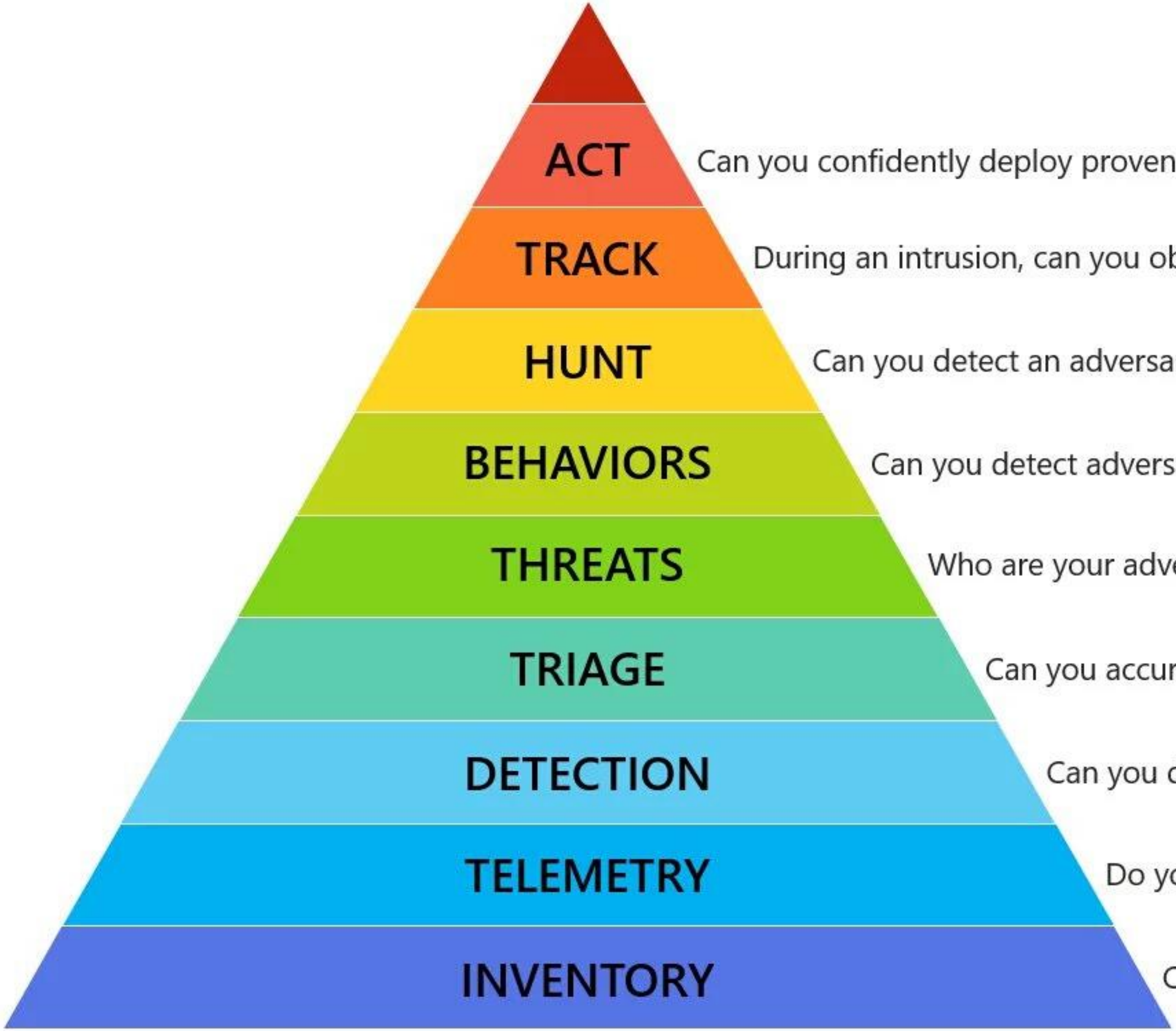
- **Academic/Instructional/WFH** – the process that supports teaching/learning (**ISP**)
  - Learning Mgt Systems such as CANVAS, Blackboard, Moodle
  - Course Delivery systems – Zoom, Webex, etc.
  - Heavily BYOD – all flavors, types
  - **Security model closest to an ISP**

- **Research** – **hybrid** of the previous 2
  - Intellectual Property protection, High risk, visibility
  - **Security model is a hybrid of corporate and ISP**

Museum Defense in Depth

- **Control** access points
  - Limited but **free flowing** access points
  - Additional barriers around high risk assets
- **Pervasive** Monitoring tools
  - Cameras, motion sensors, etc.
- **Active** Response
  - Guards, on-demand barriers, fire suppression
- **Recovery** Measures
  - Insurance
  - Tracking devices
- **Assume** hostiles are inside.

Used with permission of Christian Schreiber



ACT — Can you confidently deploy proven countermeasures to evict and recover?

TRACK — During an intrusion, can you observe adversary activity in real-time?

HUNT — Can you detect an adversary that is already embedded?

BEHAVIORS — Can you detect adversary activity within your environment?

THREATS — Who are your adversaries? What are their capabilities?

TRIAGE — Can you accurately classify detection results?

DETECTION — Can you detect unauthorized activity?

TELEMETRY — Do you have visibility across your assets?

INVENTORY — Can you name the assets you are defending?

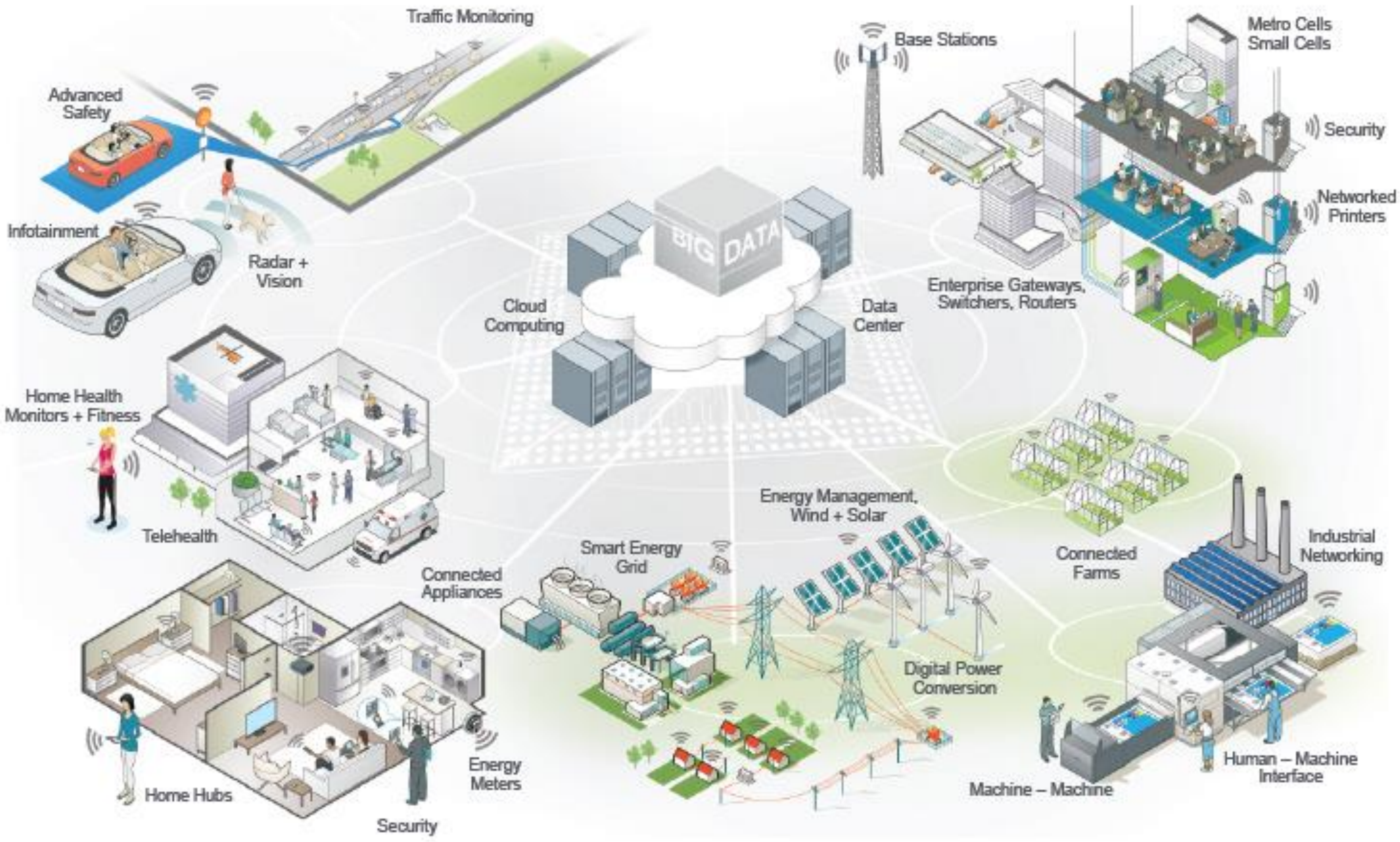
source: https://github.com/swannman/ircapabilities

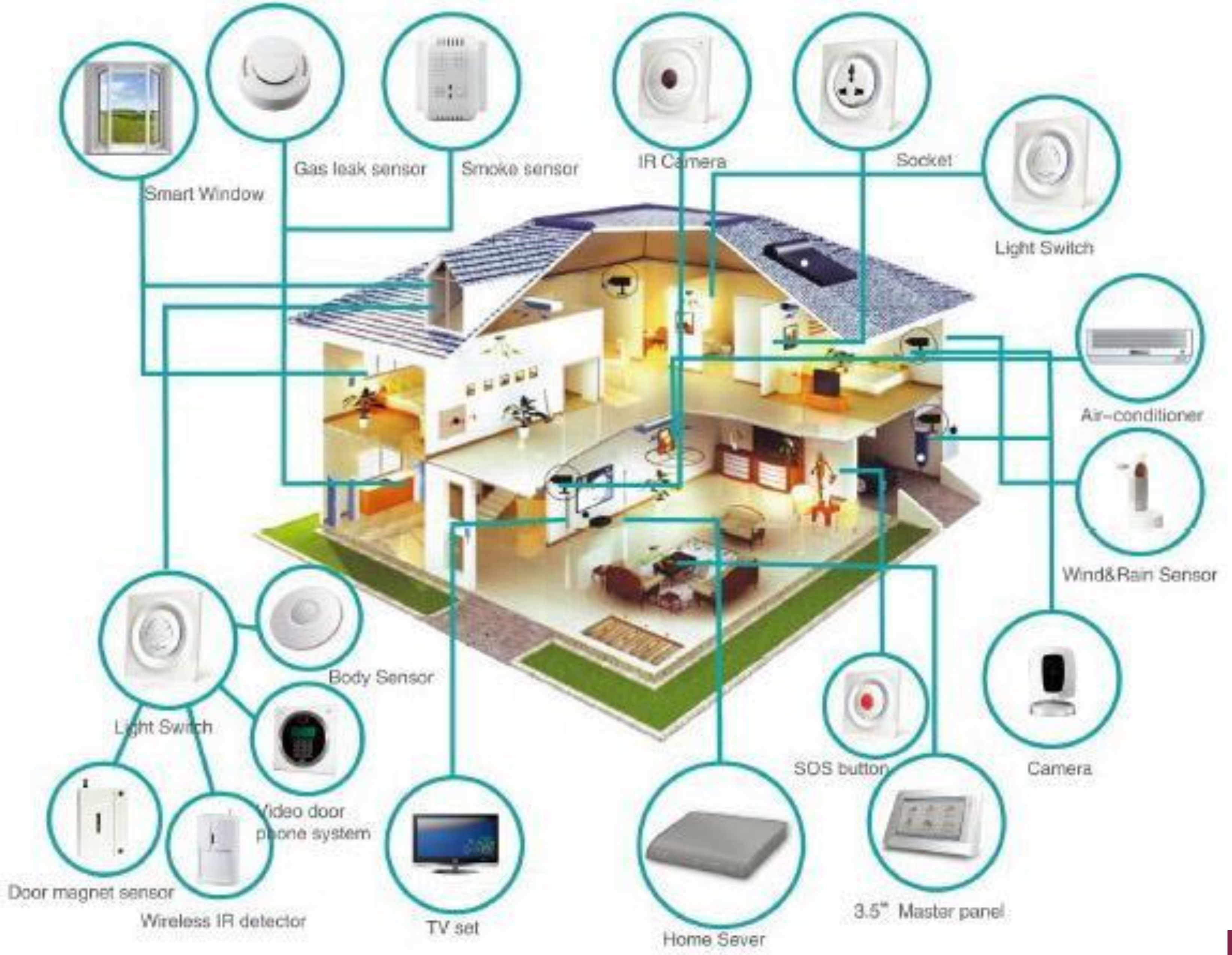
What’s a Thing?

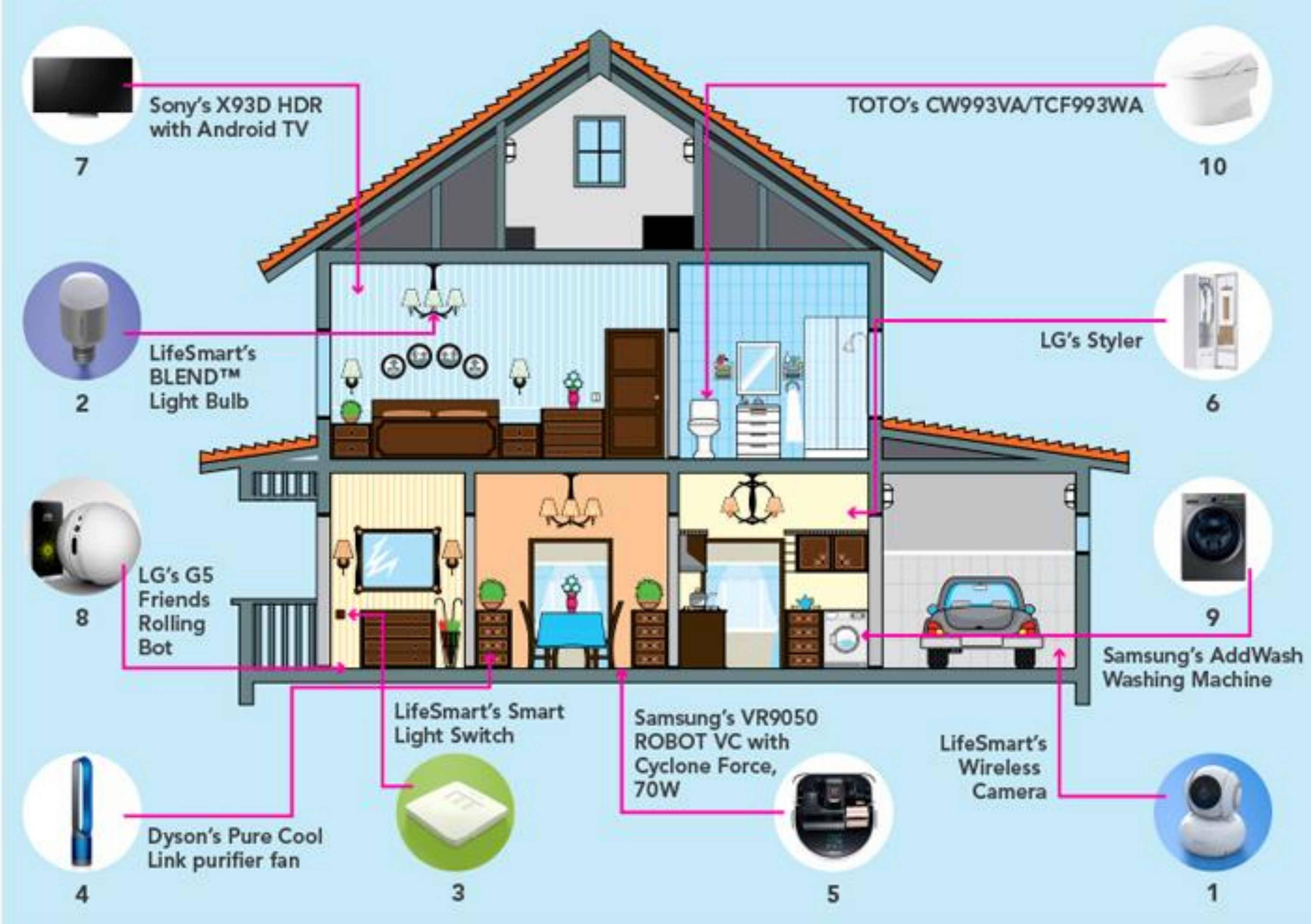
- A Thing is physical object that contains 1 or more devices
- Sensor – sense the physical environment
    - Thermometers, Thermostats, weight scales
    - Measure something
- Actuator – affect the physical environment
    - Brakes, pedals, pistons
    - Does something

    - https://www.cosic.esat.kuleuven.be/school-iot/slides/IoTChallenges.pdf

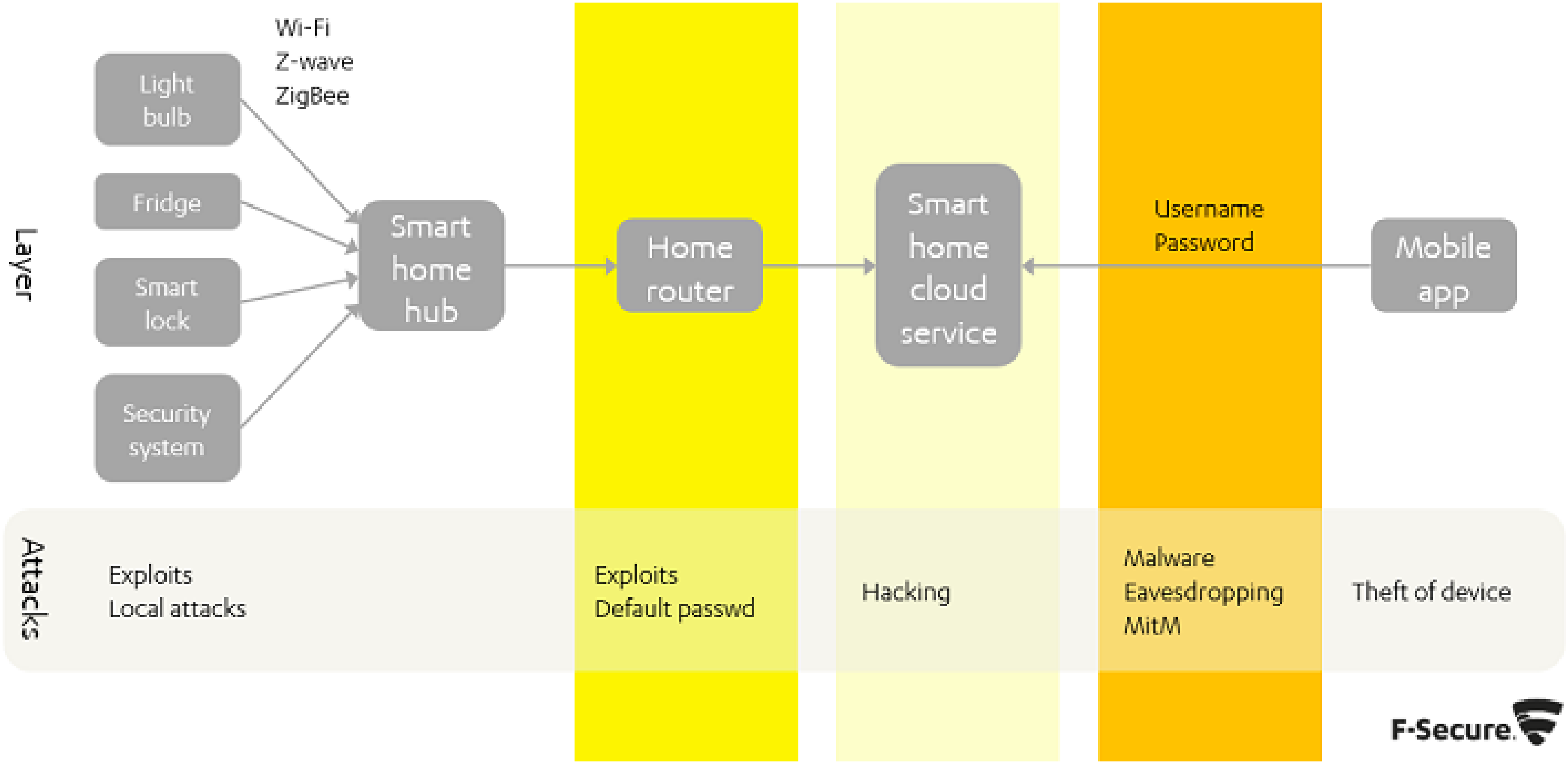
ENABLING SMART CONNECTED SOLUTIONS FROM THE END NODE TO THE CLOUD



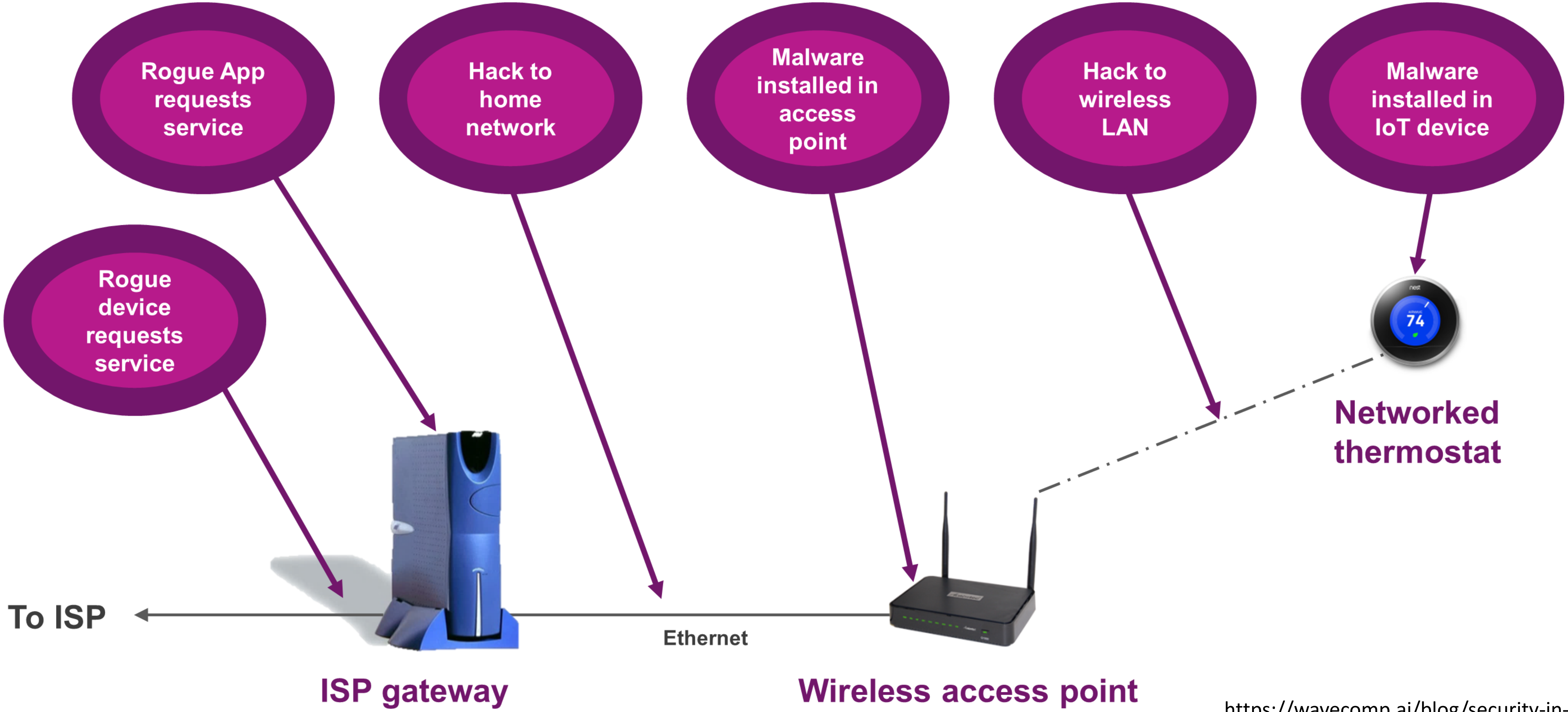

Smart Window
Gas leak sensor
Smoke sensor
IR Camera
Socket
Light Switch
Air-conditioner
Wind&Rain Sensor
Camera
Body Sensor
Light Switch
Video door phone system
Door magnet sensor
Wireless IR detector
TV set
Home Sever
SOS button
3.5" Master panel


Sony's X93D HDR with Android TV
7
LifeSmart's BLEND™ Light Bulb
2
LG's G5 Friends Rolling Bot
8
Dyson's Pure Cool Link purifier fan
4
LifeSmart's Smart Light Switch
3
Samsung's VR9050 ROBOT VC with Cyclone Force, 70W
5
LifeSmart's Wireless Camera
1
Samsung's AddWash Washing Machine
9
LG's Styler
6
TOTO's CW993VA/TCF993WA
10

Protect your home network



Security attacks



Rogue App requests service

Hack to home network

Malware installed in access point

Hack to wireless LAN

Malware installed in IoT device

Rogue device requests service

Networked thermostat

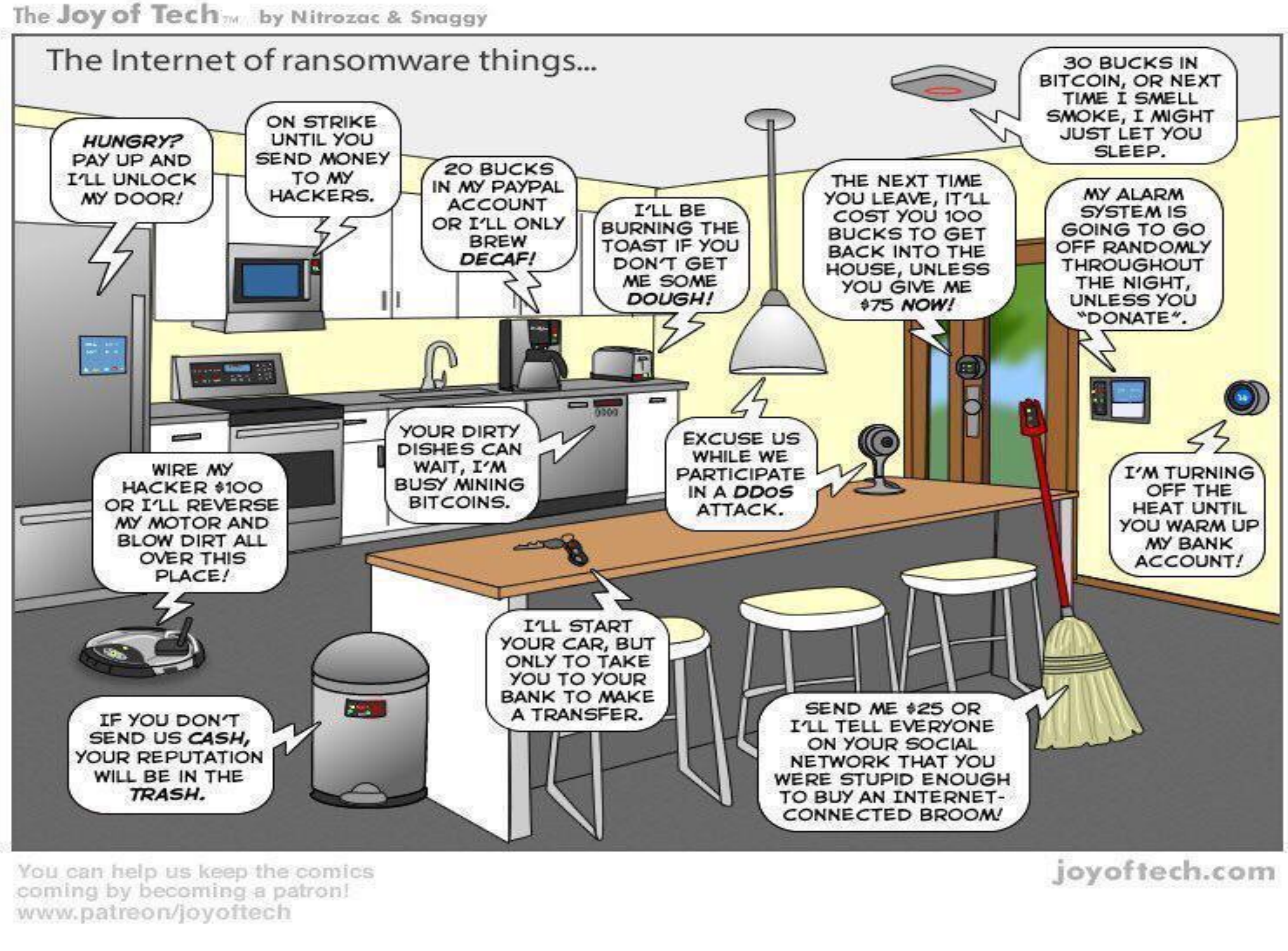
To ISP

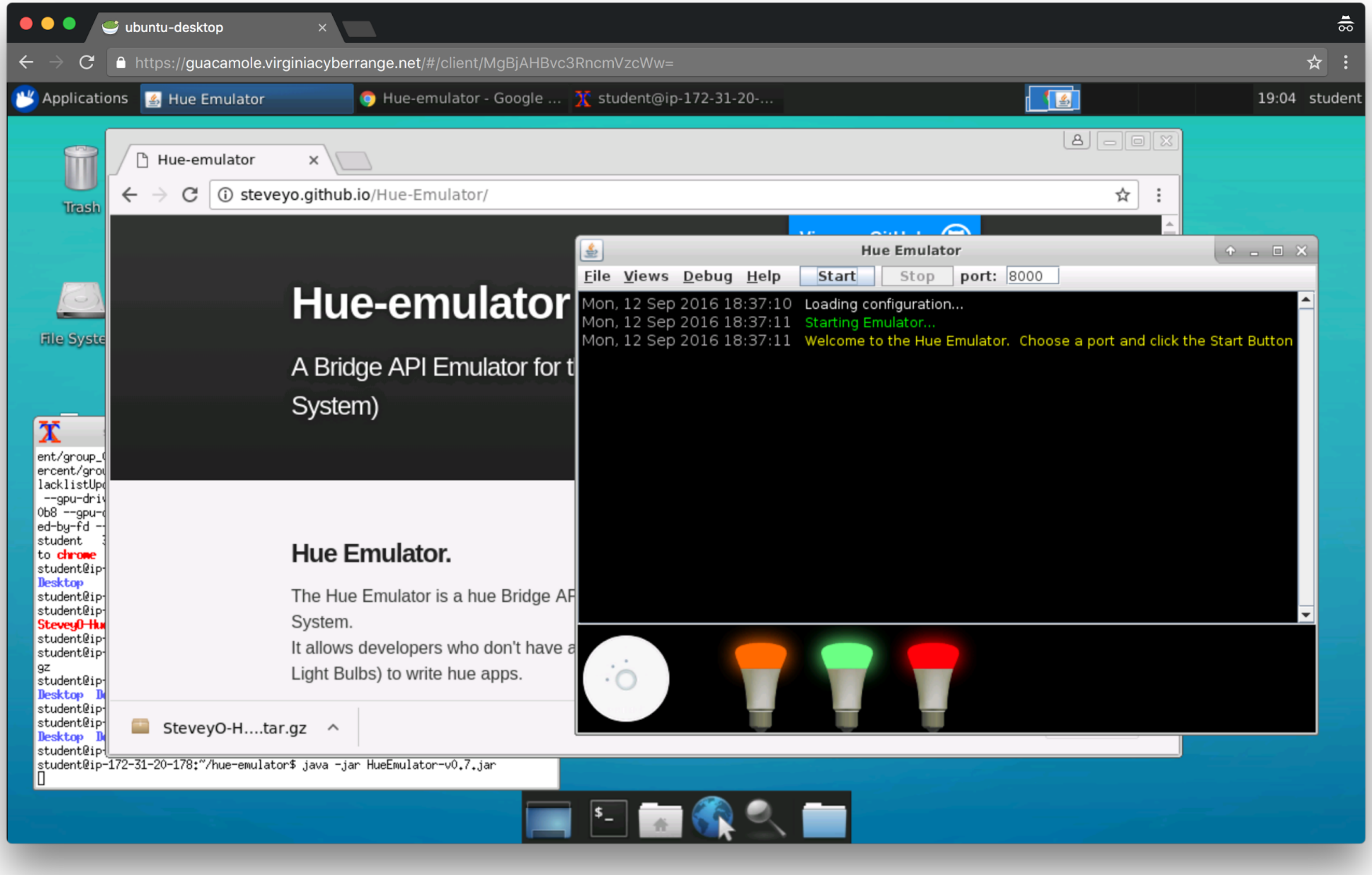
Ethernet

ISP gateway

Wireless access point

https://wavecomp.ai/blog/security-in-iot-devices/


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com



Hue-emulator

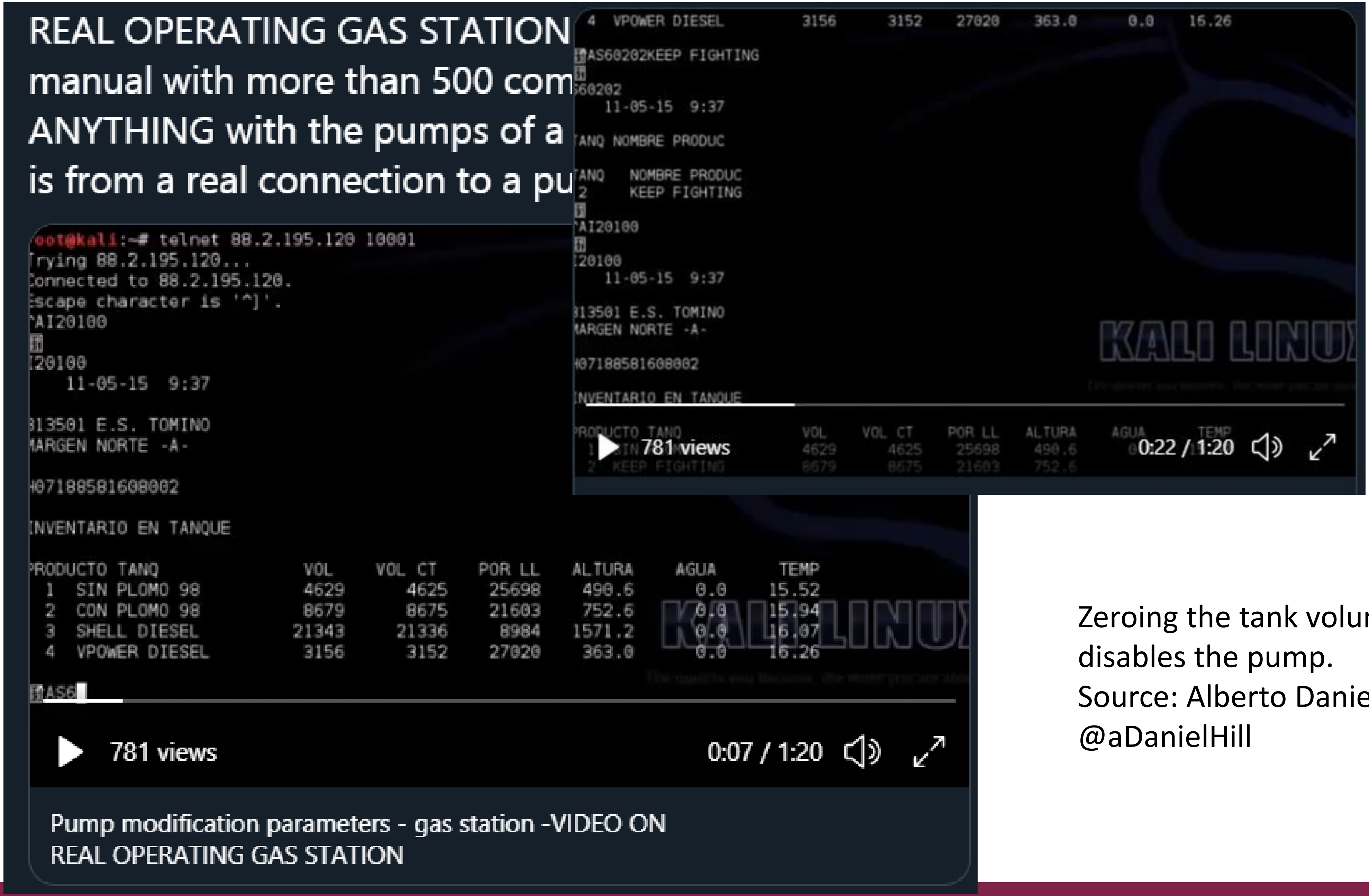
A Bridge API Emulator for t
System)

Hue Emulator.

The Hue Emulator is a hue Bridge AF
System.
It allows developers who don't have a
Light Bulbs) to write hue apps.

```
Mon, 12 Sep 2016 18:37:10  Loading configuration...
Mon, 12 Sep 2016 18:37:11  Starting Emulator...
Mon, 12 Sep 2016 18:37:11  Welcome to the Hue Emulator.  Choose a port and click the Start Button
```

```
ent/group_(
ercent/grou
lacklistUpd
 --gpu-driv
0b8 --gpu-
ed-by-fd -
student    3
to chrome
student@ip-
Desktop
student@ip-
student@ip-
SteveyO-Hu
student@ip-
student@ip-
gz
student@ip-
Desktop  D
student@ip-
student@ip-
Desktop  D
student@ip-
student@ip-172-31-20-178:~/hue-emulator$ java -jar HueEmulator-v0.7.jar
```



REAL OPERATING GAS STATION
manual with more than 500 com
ANYTHING with the pumps of a
is from a real connection to a pu

```
oot@kali:~# telnet 88.2.195.120 10001
Trying 88.2.195.120...
Connected to 88.2.195.120.
Escape character is '^]'.
^AI20100
▯
I20100
    11-05-15   9:37

313501 E.S. TOMINO
MARGEN NORTE -A-

407188581608002

INVENTARIO EN TANQUE

PRODUCTO TANQ          VOL    VOL CT    POR LL   ALTURA    AGUA     TEMP
 1  SIN PLOMO 98       4629     4625     25698    490.6     0.0    15.52
 2  CON PLOMO 98       8679     8675     21603    752.6     0.0    15.94
 3  SHELL DIESEL      21343    21336      8984   1571.2     0.0    16.07
 4  VPOWER DIESEL      3156     3152     27020    363.0     0.0    16.26

▯AS6
```

Pump modification parameters - gas station -VIDEO ON
REAL OPERATING GAS STATION

```
 4  VPOWER DIESEL      3156     3152     27020    363.0     0.0    16.26

▯AS60202KEEP FIGHTING
▯
S60202
   11-05-15  9:37

TANQ NOMBRE PRODUC

TANQ   NOMBRE PRODUC
 2     KEEP FIGHTING
▯
^AI20100
▯
I20100
   11-05-15  9:37

313501 E.S. TOMINO
MARGEN NORTE -A-

407188581608002

INVENTARIO EN TANQUE

PRODUCTO TANQ          VOL    VOL CT    POR LL   ALTURA    AGUA     TEMP
 1  SIN                4629     4625     25698    490.6
 2  KEEP FIGHTING      8679     8675     21603    752.6
```

Zeroing the tank volumes disables the pump.
Source: Alberto Daniel Hill @aDanielHill

1
2
3
4
5
6
7
8
9
*
0
A

Meet a Spammer

Hacking Dolls

- Hacking My Friend Cayla doll to unlock your front door
- https://www.youtube.com/watch?v=olx1G69kxfY
- https://www.youtube.com/watch?v=kl3CV3xeKMU TV story.
- https://www.youtube.com/watch?v=JcT0g3eNl5A

Which Toys/Devices are Safe?

- Mozilla’s Privacy Not Included list
- https://foundation.mozilla.org/en/privacynotincluded/
- #MyNameIsTalkingTina

www.despair.com

IT vs. OT

- Dynamic
- **Data is king**
    - IT is about digital information storage, retrieval, transmission, and manipulation.
- Gateways are everywhere

- Does 1 thing and 1 thing only
- **Process is king**
    - OT is all about process control. Things only happen one way—the way they were designed to act. If given a certain input, they will always produce a certain output, time and time again.
- Fewer gateways

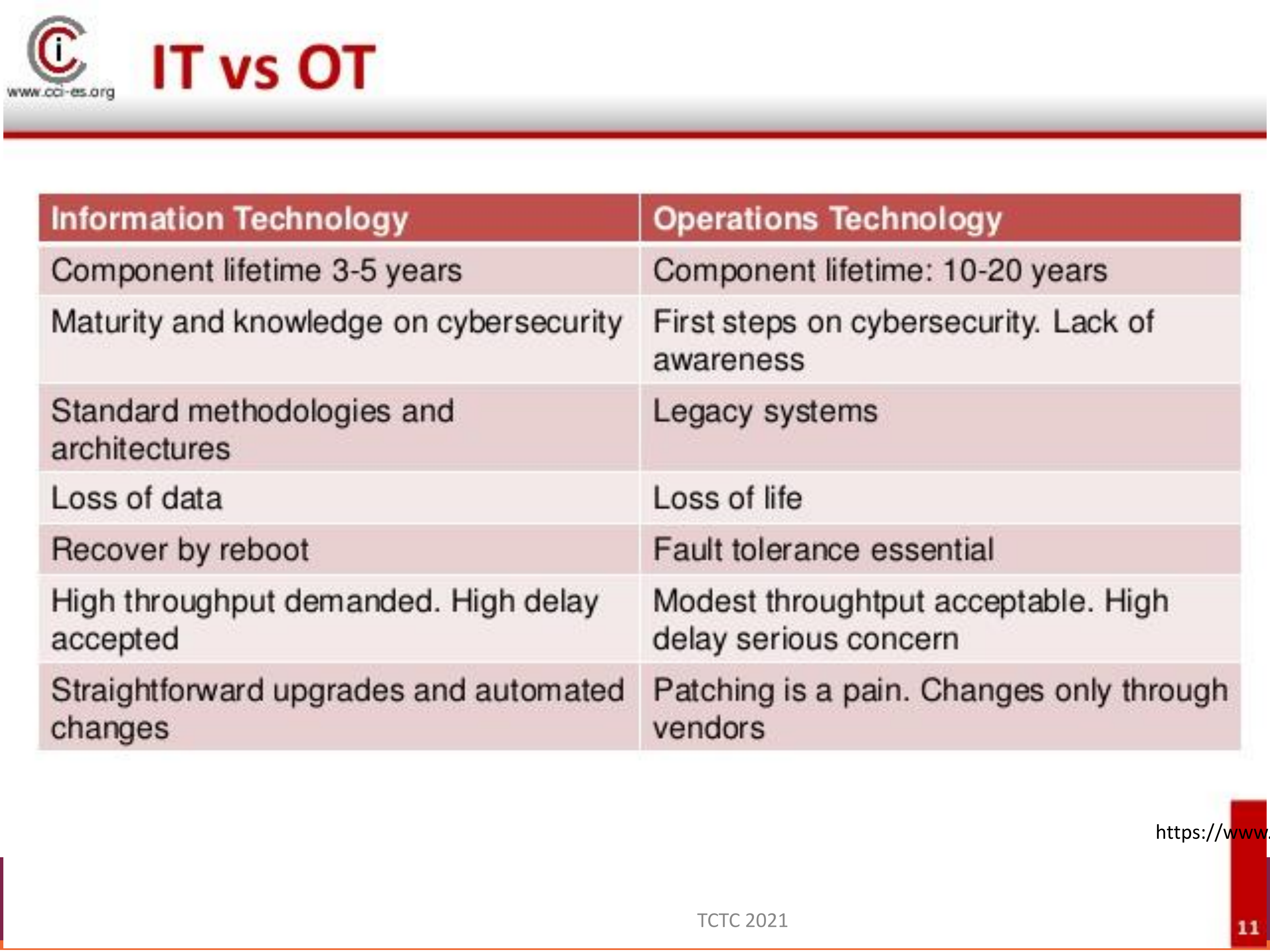
https://www.novotek.com/en/solutions/cyber-security-for-production-and-process-networks/vast-differences-between-it-and-ot-cyber-security

IT vs. OT

- Confidentiality is priority #1
  - **Confidentiality, Integrity, Availability**. Businesses, consumers expect financial, medical and personal data to remain private.
- Throughput matters
- Patch Tuesday

- Control is priority #1
  - The new order: **control, availability, integrity, confidentiality**. Control equates to safety because, in this environment, loss of control could have dire consequences.
- Throughput is secondary
- Patch Decade

https://www.novotek.com/en/solutions/cyber-security-for-production-and-process-networks/vast-differences-between-it-and-ot-cyber-security



www.cci-es.org

IT vs OT

Information Technology	Operations Technology
Component lifetime 3-5 years	Component lifetime: 10-20 years
Maturity and knowledge on cybersecurity	First steps on cybersecurity. Lack of awareness
Standard methodologies and architectures	Legacy systems
Loss of data	Loss of life
Recover by reboot	Fault tolerance essential
High throughput demanded. High delay accepted	Modest throughtput acceptable. High delay serious concern
Straightforward upgrades and automated changes	Patching is a pain. Changes only through vendors

https://www.slideshare.net/phdays/ss-35168693

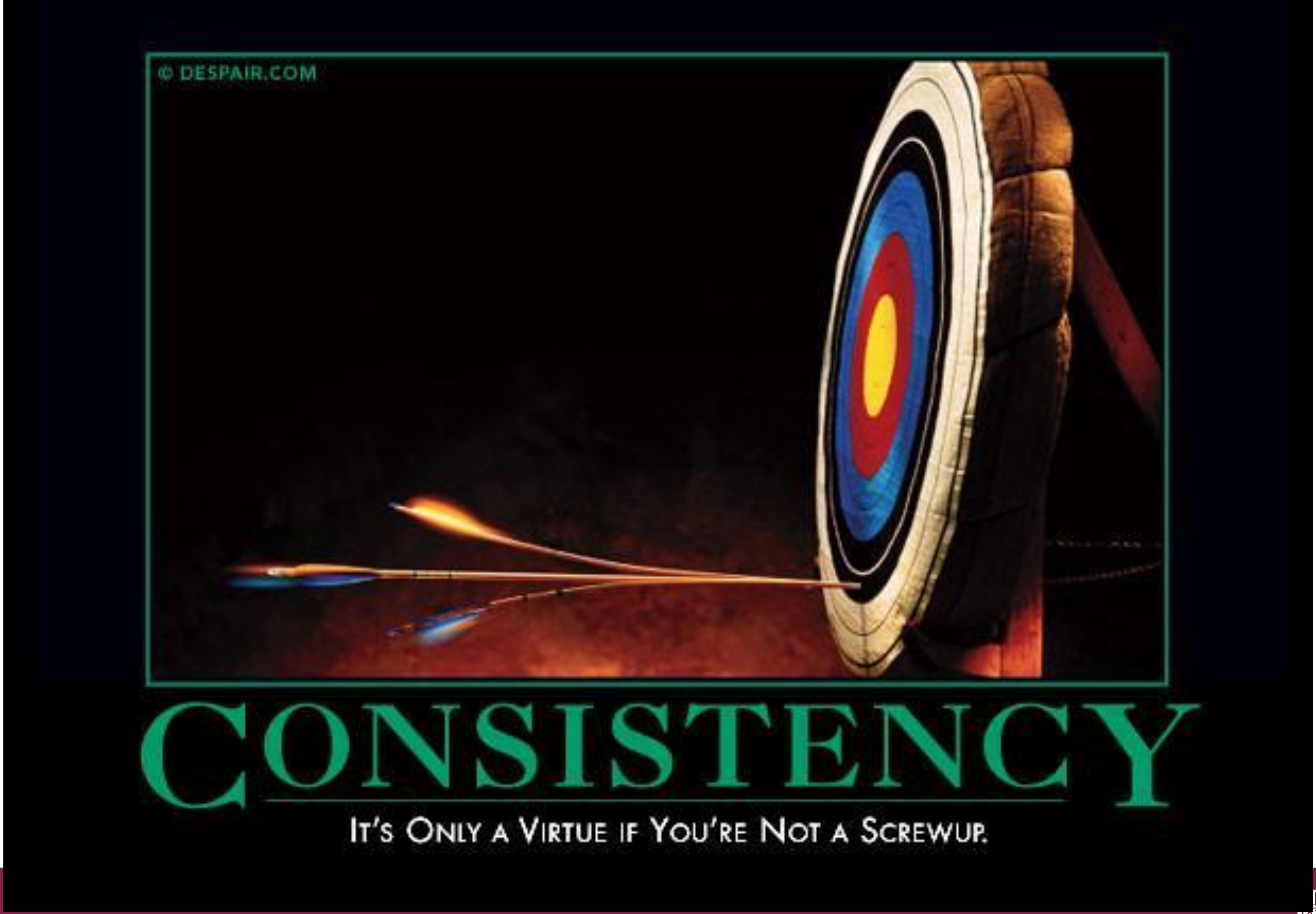
Schneier’s Example – Car Attack*

- Confidentiality, Availability, Integrity
- Confidentiality
  - Know who you are so we target your car
- Availability
  - Disable your car’s brake system
- Integrity
  - Change the settings on your car’s “stay in lane” feature
  - Tell it to be 2 ft to the left of the center line

- *“Click Here to Kill Everybody”, by Bruce Schneier, ISBN: 978-0-393-60888-5

OT and IT Common Ground

- Underlying goal: retain control of systems and machines that could impact the safety of employees and customers
- ID, authenticate all devices/machines (Plant, field) ensure only approved devices talk to each other (hmmmm, zero trust?)
- Encrypt all communications
- Enable remote upgrades. Do NOT assume the net is safe
- Separation of IT and OT will diminish


© DESPAIR.COM
CONSISTENCY
It's Only a Virtue if You're Not a Screwup.

Zero Trust Networks(ZTN) Assumptions*

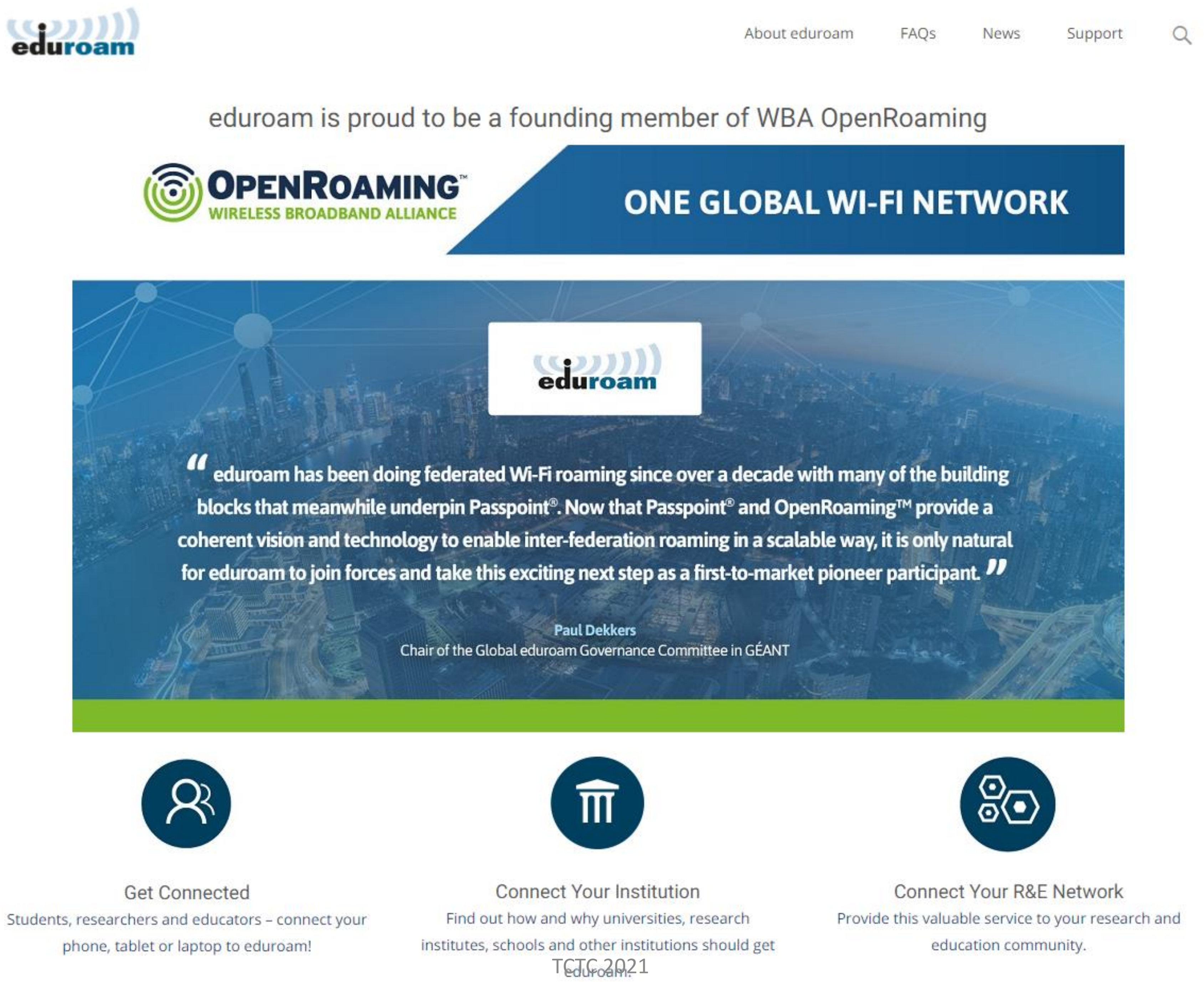
- The device is no longer the border. A **user’s identity/Data pair is the new border.**

- Pillar 1: The network is always assumed to be **hostile**
- Pillar 2: Assume the hostiles are already **inside your network**
- Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network

** “Zero Trust Networks: Building Secure Systems in Untrusted Networks”, Evan Gilman, Doug Barth*

ZTN Assumptions

- Pillar 4: **Every** device, user and network flow is authenticated and authorized
- Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible
- Pillar 7: Containers, serverless and cloud computing are the new disruptors of traditional security architectures.
- Pillar 8: Mobile users, mobile apps, mobile storage



eduroam is proud to be a founding member of WBA OpenRoaming

“eduroam has been doing federated Wi-Fi roaming since over a decade with many of the building blocks that meanwhile underpin Passpoint®. Now that Passpoint® and OpenRoaming™ provide a coherent vision and technology to enable inter-federation roaming in a scalable way, it is only natural for eduroam to join forces and take this exciting next step as a first-to-market pioneer participant.”

Paul Dekkers
Chair of the Global eduroam Governance Committee in GÉANT

Get Connected

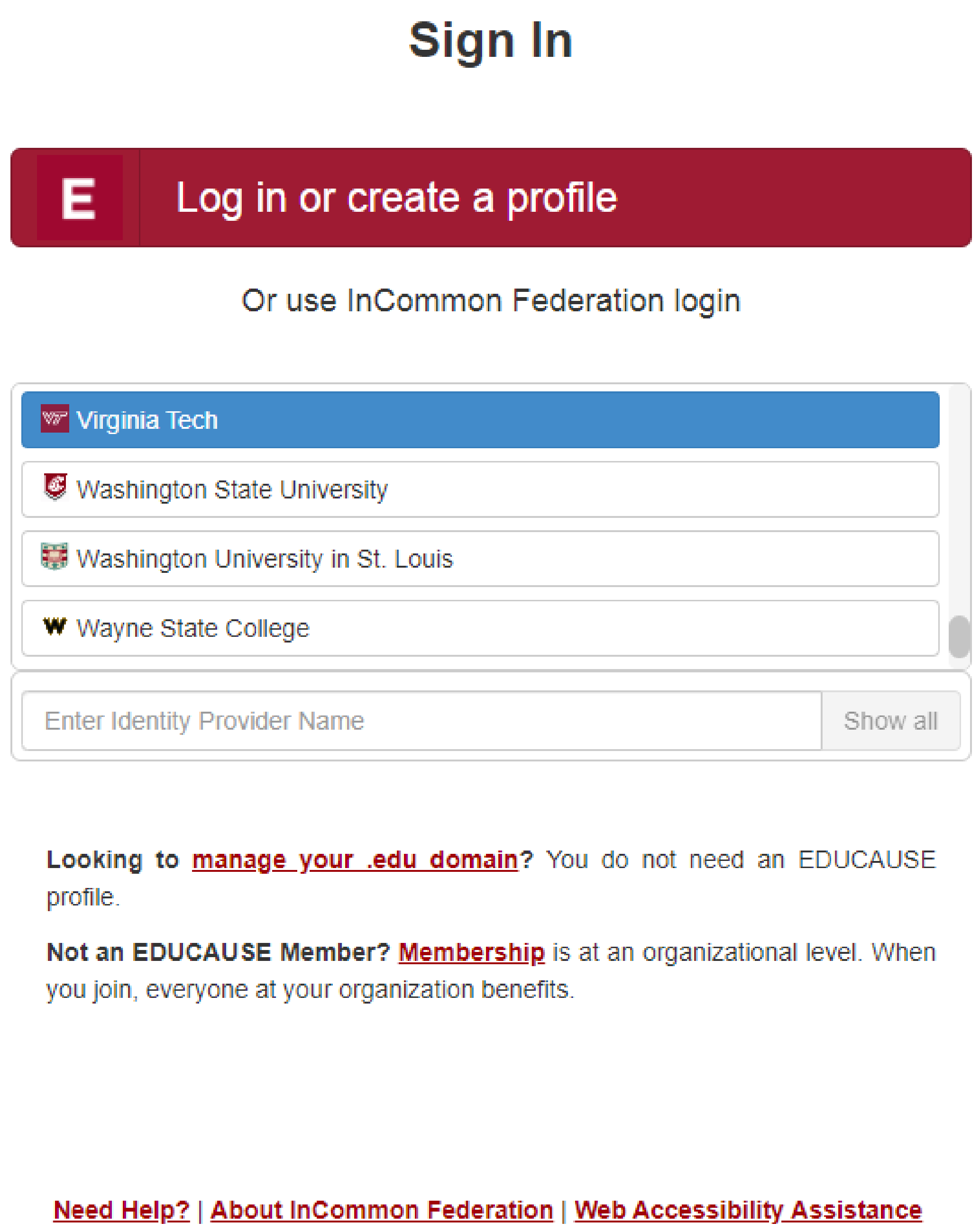
Students, researchers and educators – connect your phone, tablet or laptop to eduroam!

Connect Your Institution

Find out how and why universities, research institutes, schools and other institutions should get eduroam.

Connect Your R&E Network

Provide this valuable service to your research and education community.



Sign In

Log in or create a profile

Or use InCommon Federation login

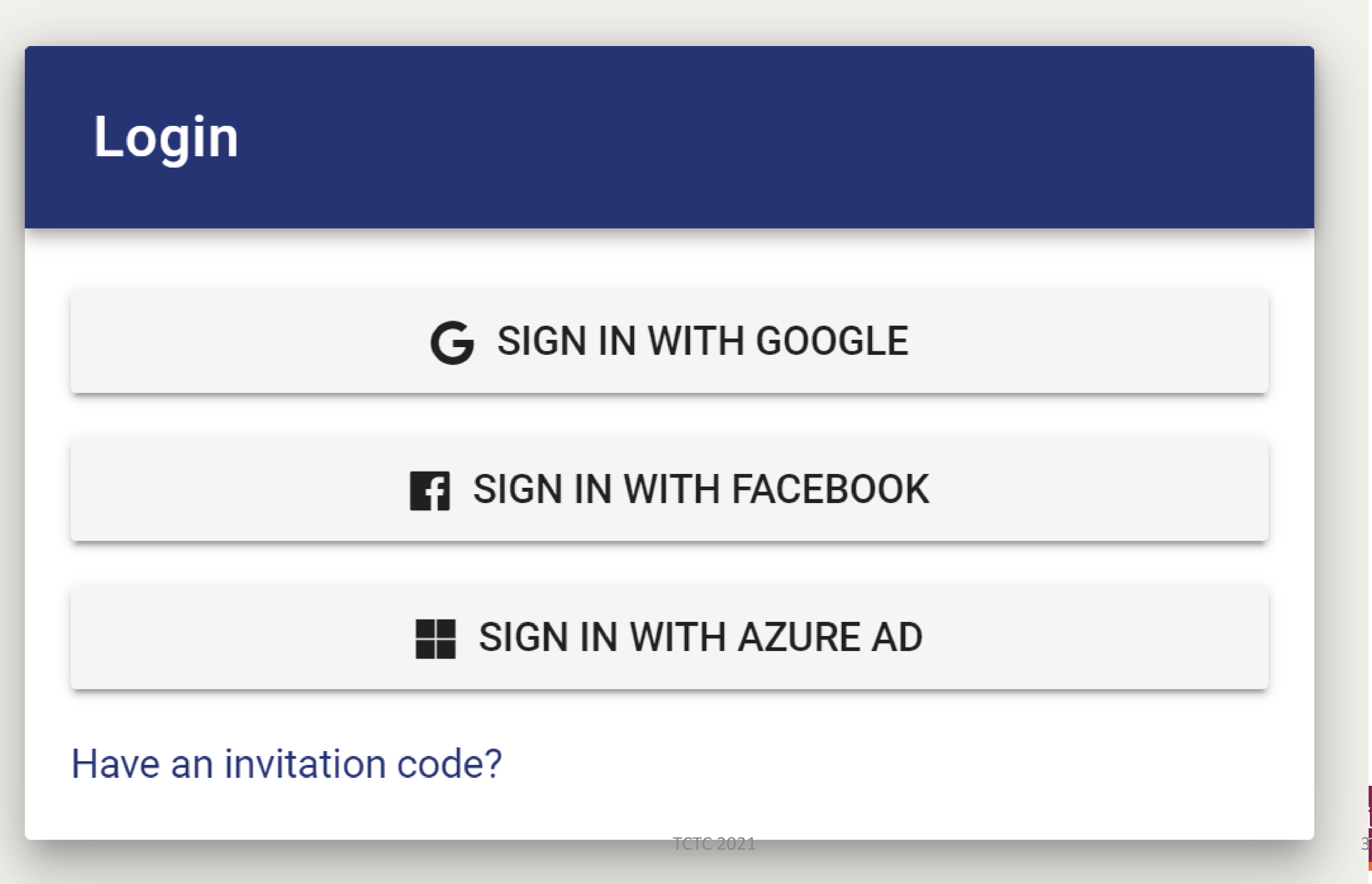
- Virginia Tech
- Washington State University
- Washington University in St. Louis
- Wayne State College

Enter Identity Provider Name | Show all

Looking to manage your .edu domain? You do not need an EDUCAUSE profile.

Not an EDUCAUSE Member? Membership is at an organizational level. When you join, everyone at your organization benefits.

Need Help? | About InCommon Federation | Web Accessibility Assistance


Login
SIGN IN WITH GOOGLE
SIGN IN WITH FACEBOOK
SIGN IN WITH AZURE AD
Have an invitation code?

Your Home Computer Became Your Work Computer - 1

- If you use your home computer for work, you must follow your office's security requirements on it.

- **Create a separate userid for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
- When you're done #WFH, you can delete that account

Your Home Computer Became Your Work Computer - 2

- You become your Help Desk, system support group

- **Does your home computer meet any regulatory requirements imposed on the data you use?**

Where Does It Go When It Goes Home?

- PROBLEM: Once data is on your home net, you lose data visibility
- Home systems become exfil targets
  - Infostealer class malware looks for PII
  - Attacker dumps from the home system
  - We don’t know if/when/where it went but the home ISP may
- SOLUTIONS (?)
  - TAG your data files (web bug)
  - File phones home instead of computer
  - Lot of work to implement

WFH attack vectors

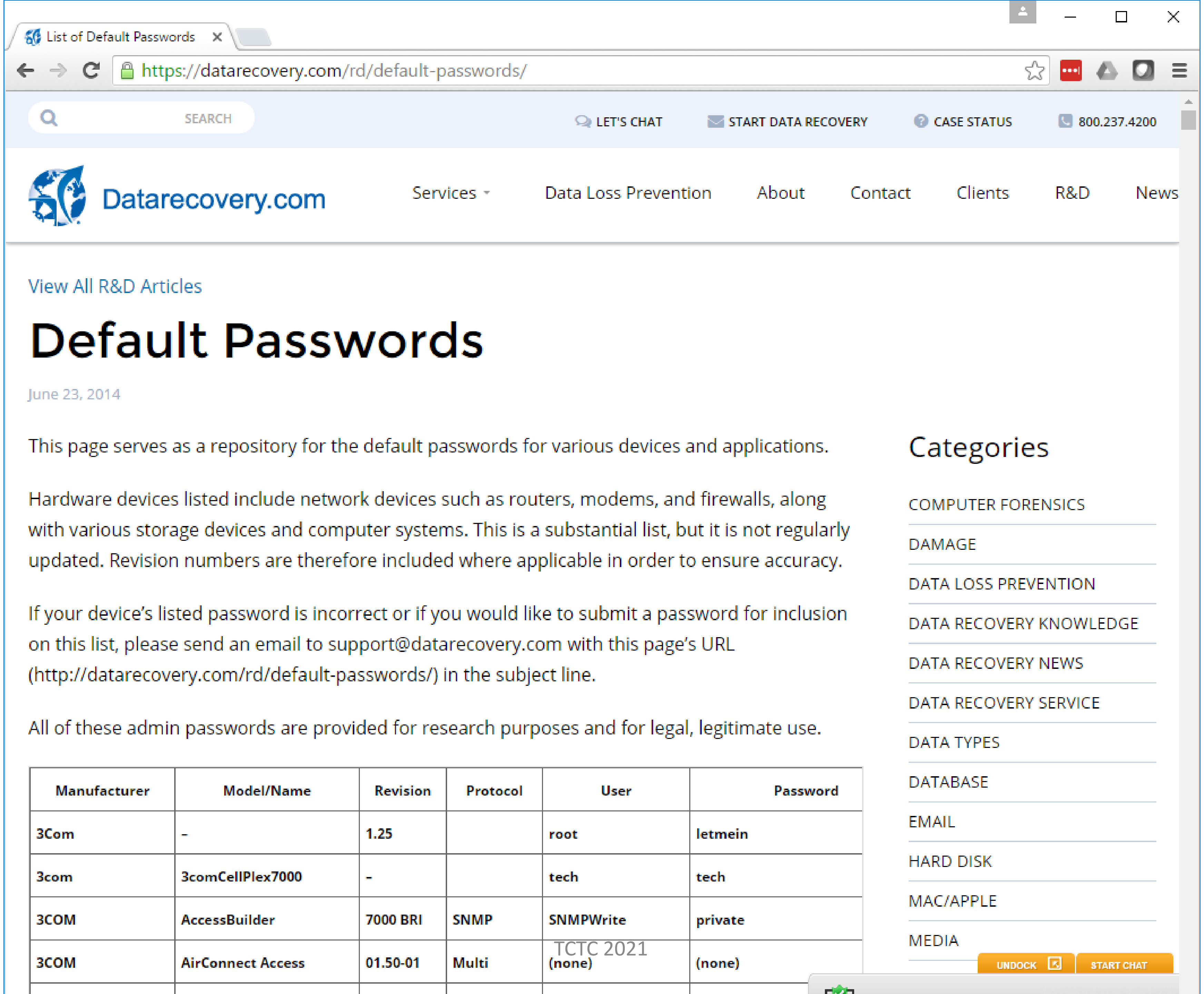
- Phishing Websites, emails
  - 1700+ domains with “Zoom” in the name (src: Checkpoint)
  - 522K active Covid-19 phishing sites (src: Google)
  - Check your spam folder for emails ☺
- Your email address is key!
  - Compromise that, everything falls.
  - Request resets from bank, Facebook, Twitter, etc.

WFH Infrastructure Protection

- Router and WiFi
  - Change default passwords
  - Disable WPS (Wifi Protected Setup) – 1 touch
  - Enable latest security options
    - WPA2-PSK [AES]

WFH Device Protection

- OS updates
- Host Based Firewalls
- Change Smart Home, Stream Security default passwords
  - Connect to separate guest net from your computers



View All R&D Articles

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

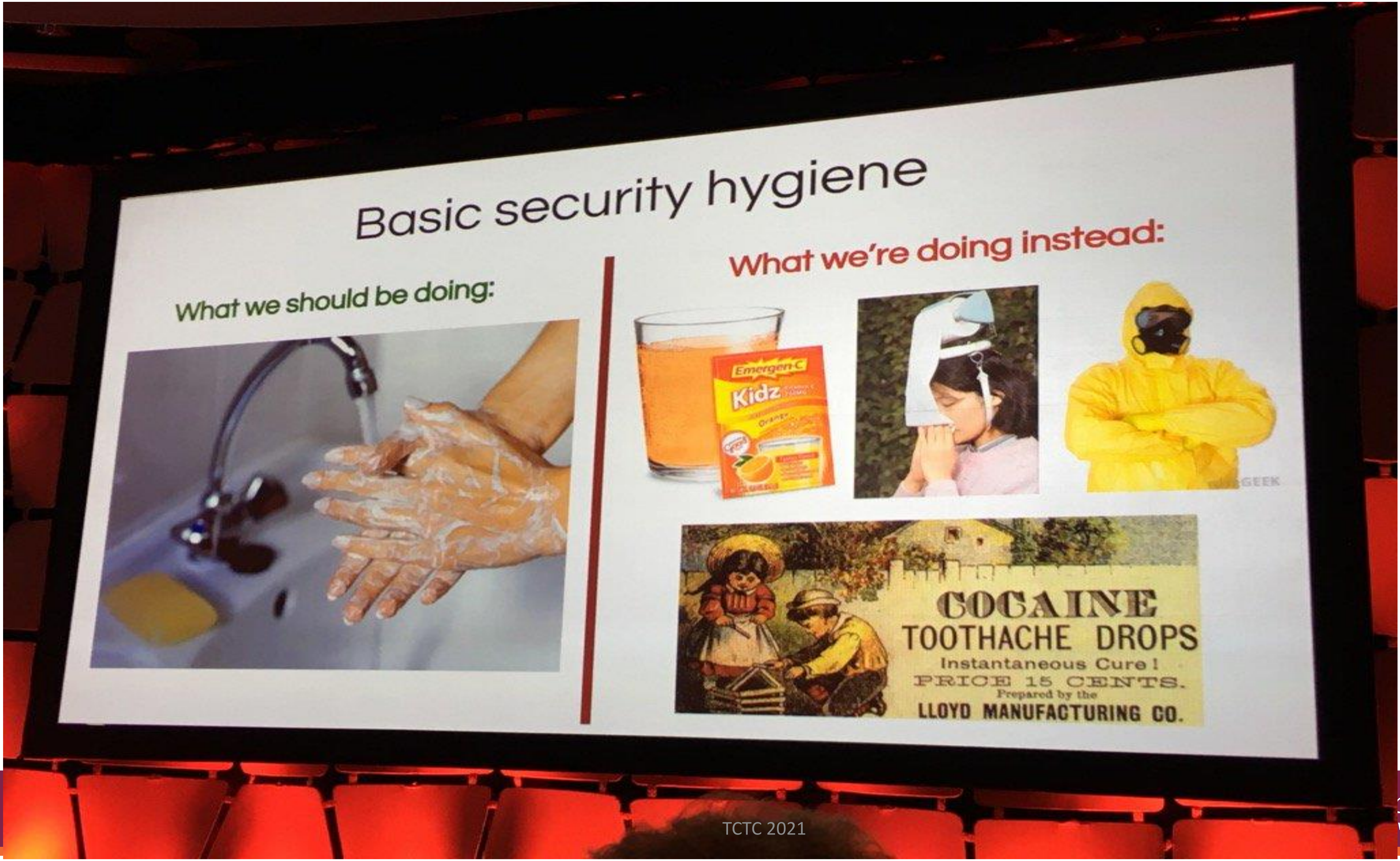
If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	-	1.25		root	letmein
3com	3comCellPlex7000	-		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

Categories

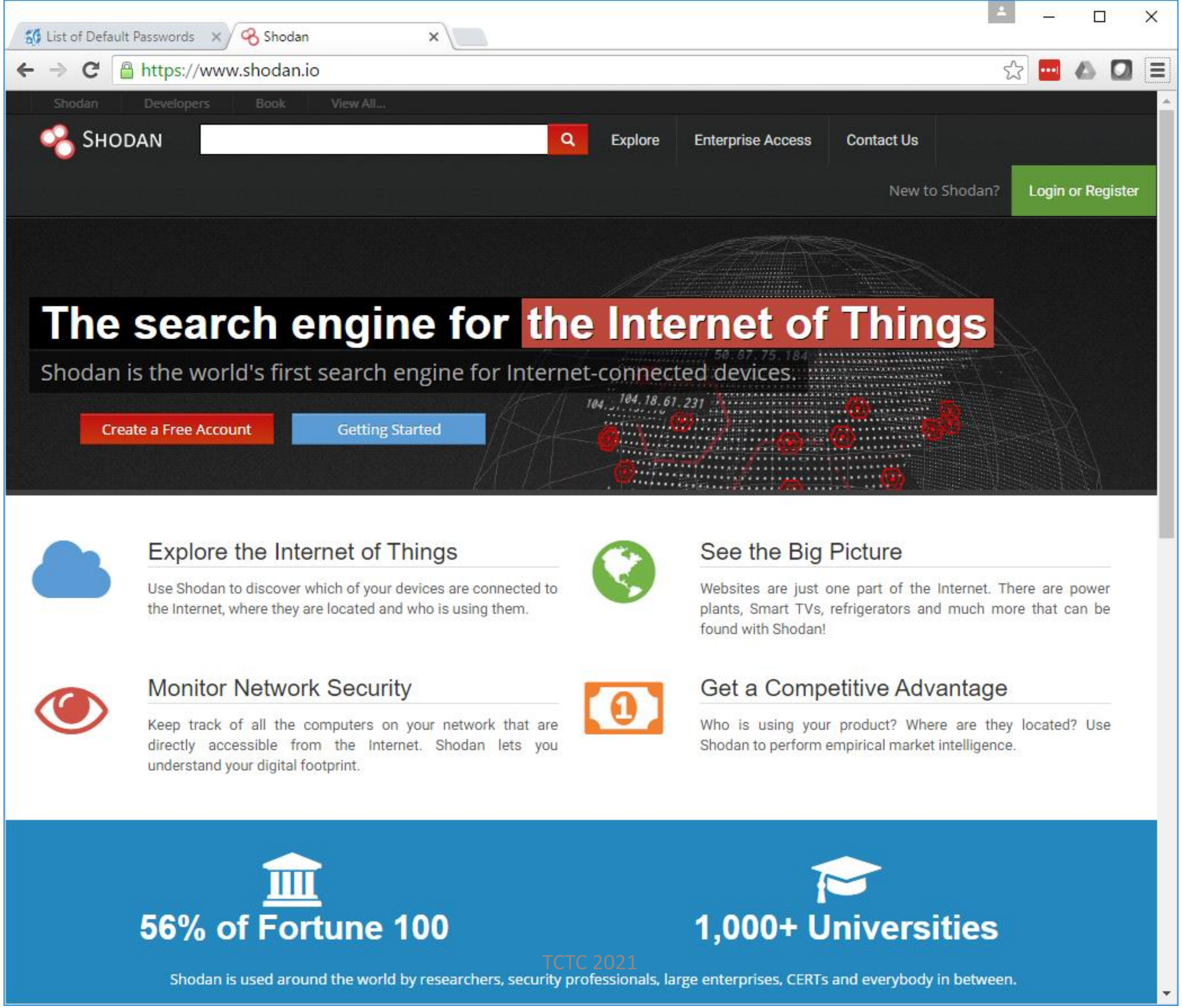
- COMPUTER FORENSICS
- DAMAGE
- DATA LOSS PREVENTION
- DATA RECOVERY KNOWLEDGE
- DATA RECOVERY NEWS
- DATA RECOVERY SERVICE
- DATA TYPES
- DATABASE
- EMAIL
- HARD DISK
- MAC/APPLE
- MEDIA



Basic security hygiene

What we should be doing:

What we're doing instead:



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

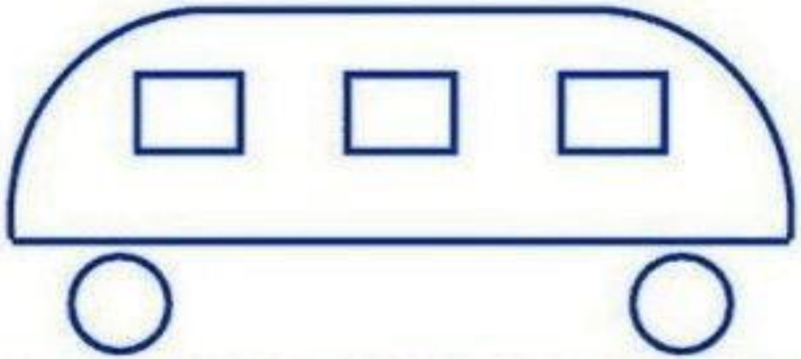
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Consider IoT and WFH Risks

- Data Classification becomes important. Be careful with high risk data.
- Your “infrastructure” include everyone’s home infrastructure
  - https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit
- IoT security is negligible
- IoT vendors cannot assume the net is safe. It’s not.
- IoT data collection needs to be understood
  - Who owns the data you give them?

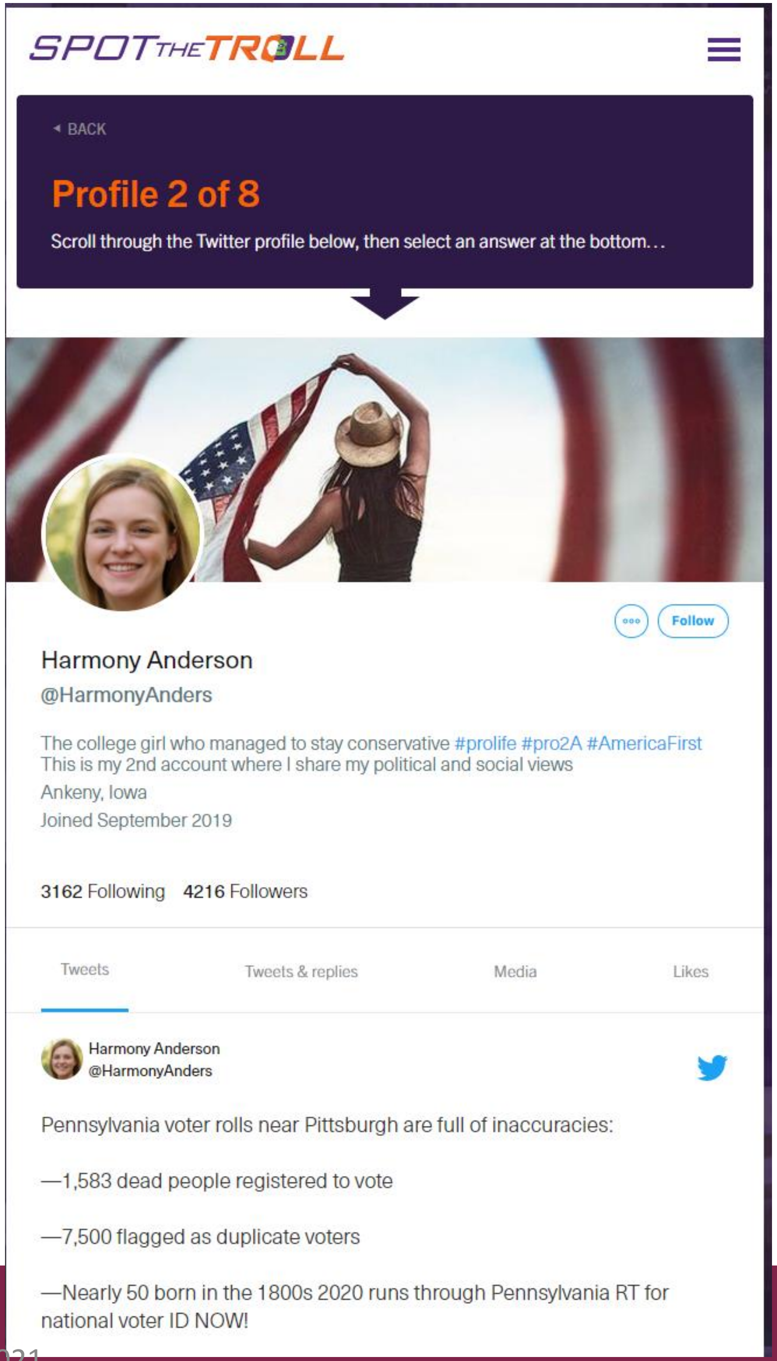
Which way is the bus going?

Right or left?



Spot the Troll

https://spotthetroll.org



◂ BACK

Profile 2 of 8

Scroll through the Twitter profile below, then select an answer at the bottom…

Harmony Anderson
@HarmonyAnders

The college girl who managed to stay conservative #prolife #pro2A #AmericaFirst
This is my 2nd account where I share my political and social views
Ankeny, Iowa
Joined September 2019

3162 Following 4216 Followers

Harmony Anderson
@HarmonyAnders

Pennsylvania voter rolls near Pittsburgh are full of inaccuracies:

—1,583 dead people registered to vote

—7,500 flagged as duplicate voters

—Nearly 50 born in the 1800s 2020 runs through Pennsylvania RT for national voter ID NOW!

Contact information

- Randy Marchany, Marchany@vt.edu, 540-231-9523 (direct line), 540-231-1688 (office), Twitter: @randymarchany, Blog: randymarchany.blogspot.com
- http://security.vt.edu