VIRGINIA TECH

Defense in Depth for CPS Security: What Does It Take and How Can Researchers Help?

Daphne Yao
Prof of CS
Virginia Tech

US Navy base at Norfolk, Virginia (Wikipedia)

CryptoGuard

CryptoGuard – Crypto Code Scanning with Deployment-quality Accuracy and Scalability

98.6% Precision

Out of 1,295 Apache alerts, only 18 are false alarms

Apache Ranger

hadoop

Apache Tomcat

APACHE OFBiz

MEECROWAVE
A light JAX-RS+CDI+JSON server!

Apache Ambari

APACHE Spark

Max, min and avg LoC: 2,571K (Hadoop), 1.1K (Commons Crypto), and 402K

CRYPTOGUARD DEPLOYMENT & IMPACT

ORACLE

Parfait (an internal Oracle product) uses our detection to scan production code

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

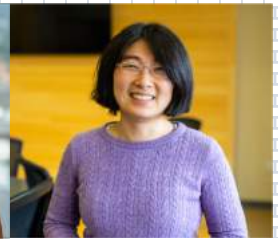
DHS founded, deployment prep ongoing

Maven

Gradle

IJ

CACM article on our technology to appear soon;

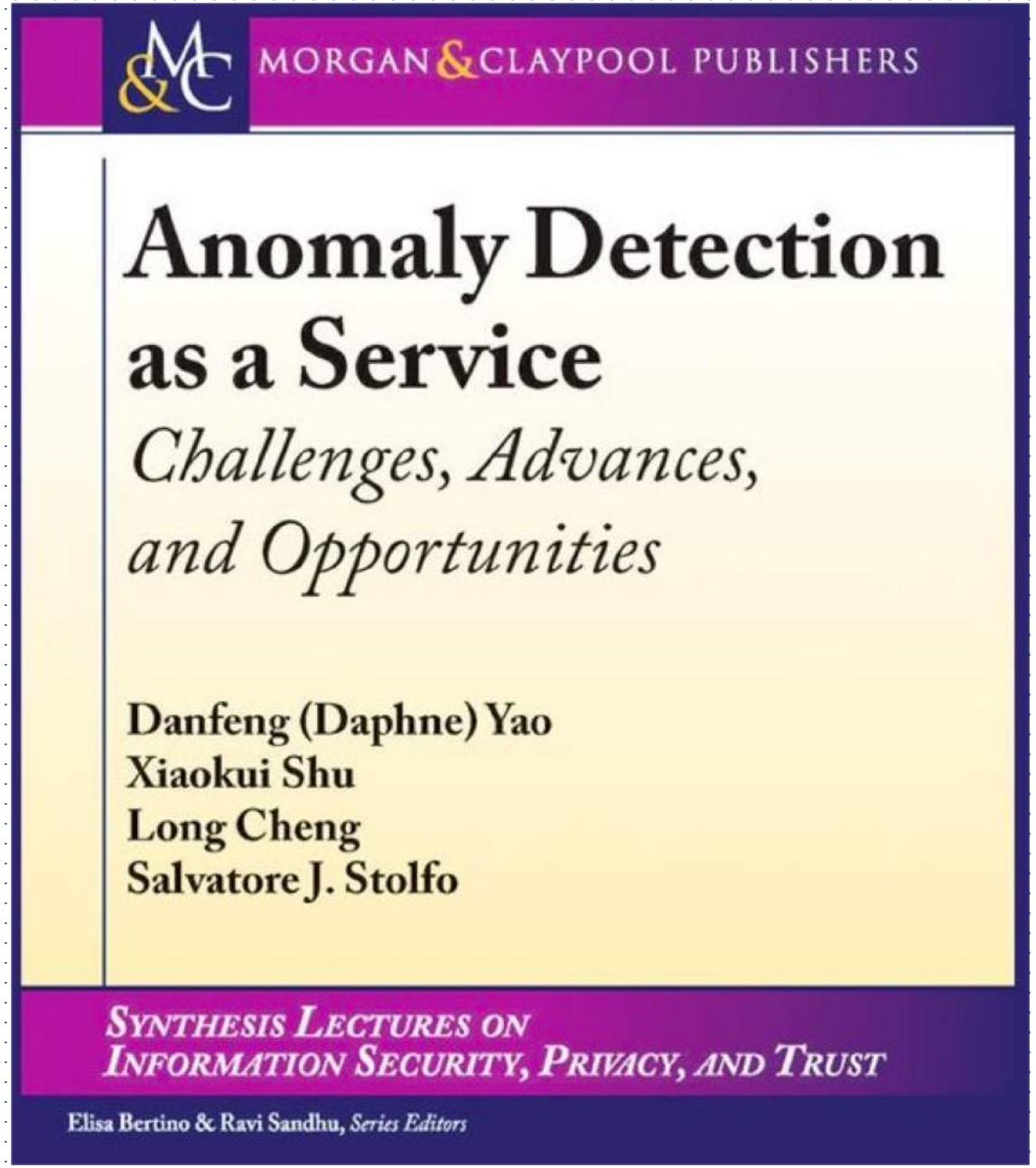


Nominated for NSA Science of Security Paper Competition

Office of Naval Research ONR Science & Technology

NSF

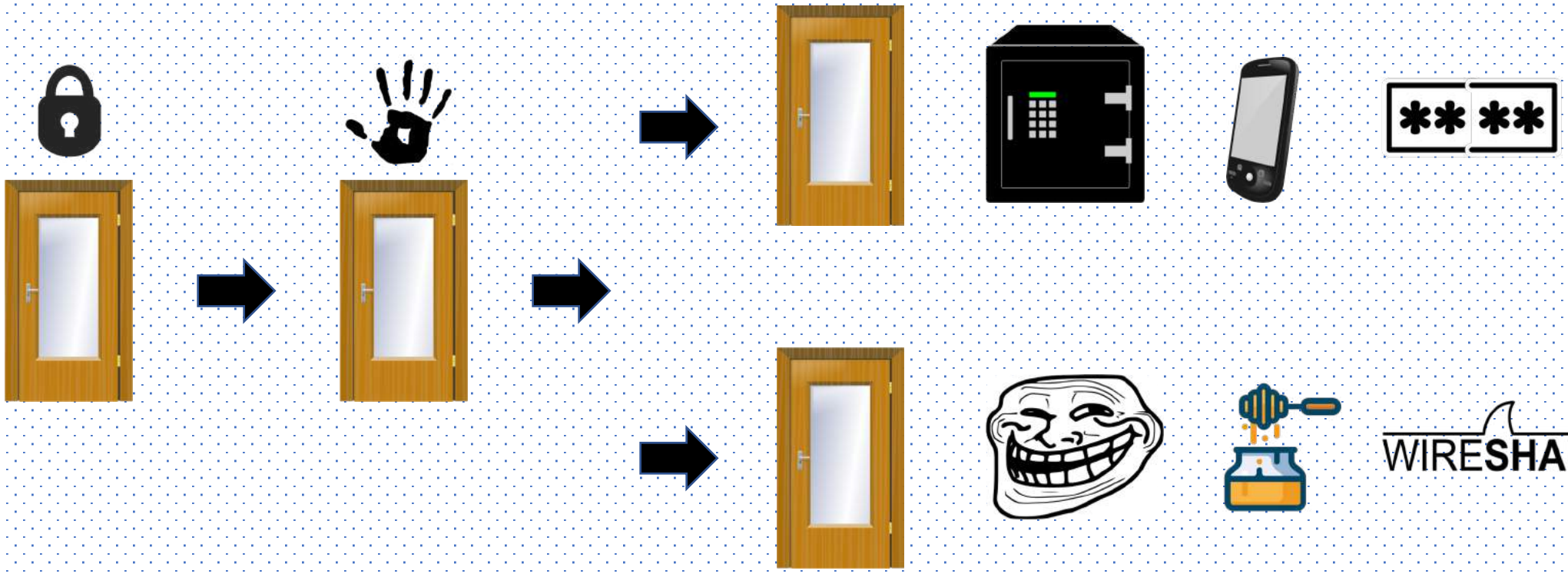
[Rahaman et al. ACM CCS 2019]
CryptoGuard and Benchmark on GitHub



Book in *Information Security, Privacy, and Trust Series*.
Series editors: Elisa Bertino and Ravi Sandhu.
Morgan & Claypool. Oct. 2017. (Book)

Free online access from most universities.

Defense in depth offers redundant protection to reduce risks



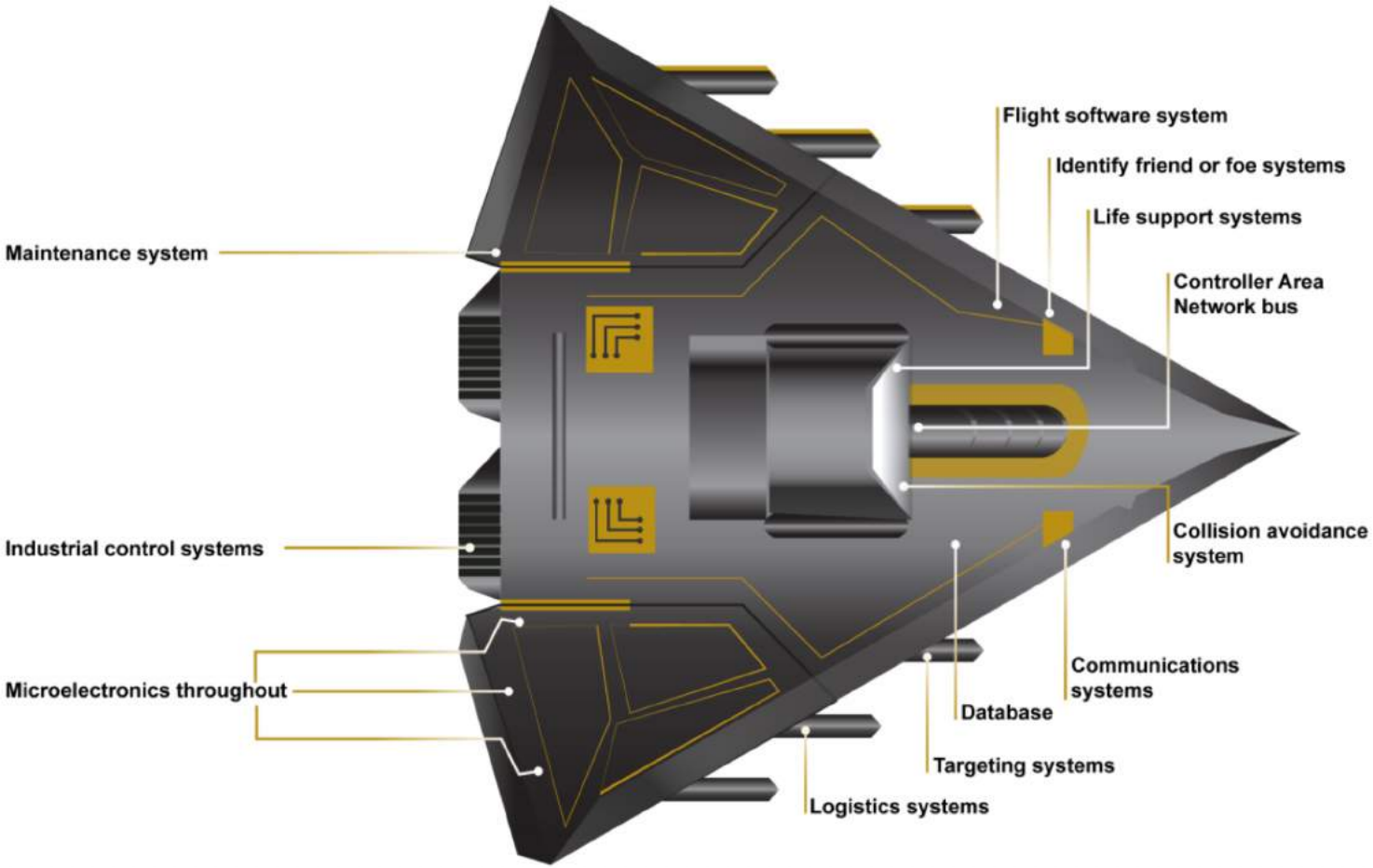
Slide credit: Sam Hentschel

DHS's 2016 defense-in-depth guidelines for ICS: https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

U.S. GAO report on weapon systems' audit (2018)

"DOD is just beginning to grapple with the challenge"

"DOD missed an opportunity to give cybersecurity a more prominent role in key acquisition decisions"



https://www.gao.gov/products/GAO-19-128

VIRGINIA TECH

$1.4 billion (1.1 million payments) had gone to dead people, as of April 2020

GAO U.S. Government Accountability Office

Reports & Testimonies | Bid Protests & Appropriations Law | Key Issues

COVID-19:

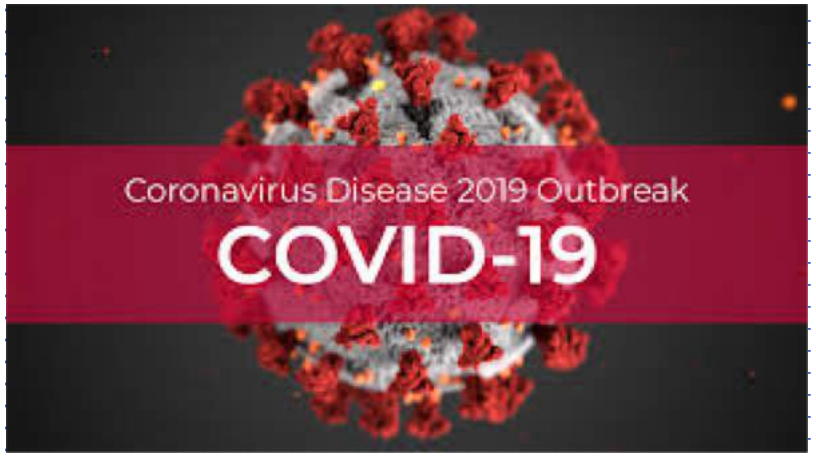
Opportunities to Improve Federal Response and Recovery Efforts

GAO-20-625: Published: Jun 25, 2020. Publicly Released: Jun 25, 2020.

FAST FACTS | HIGHLIGHTS | RECOMMENDATIONS | VIEW REPORT (HTML)

In response to the COVID-19 pandemic, Congress appropriated $2.6 trillion in emergency assistance for people, businesses, the health care system, and state and local governments.

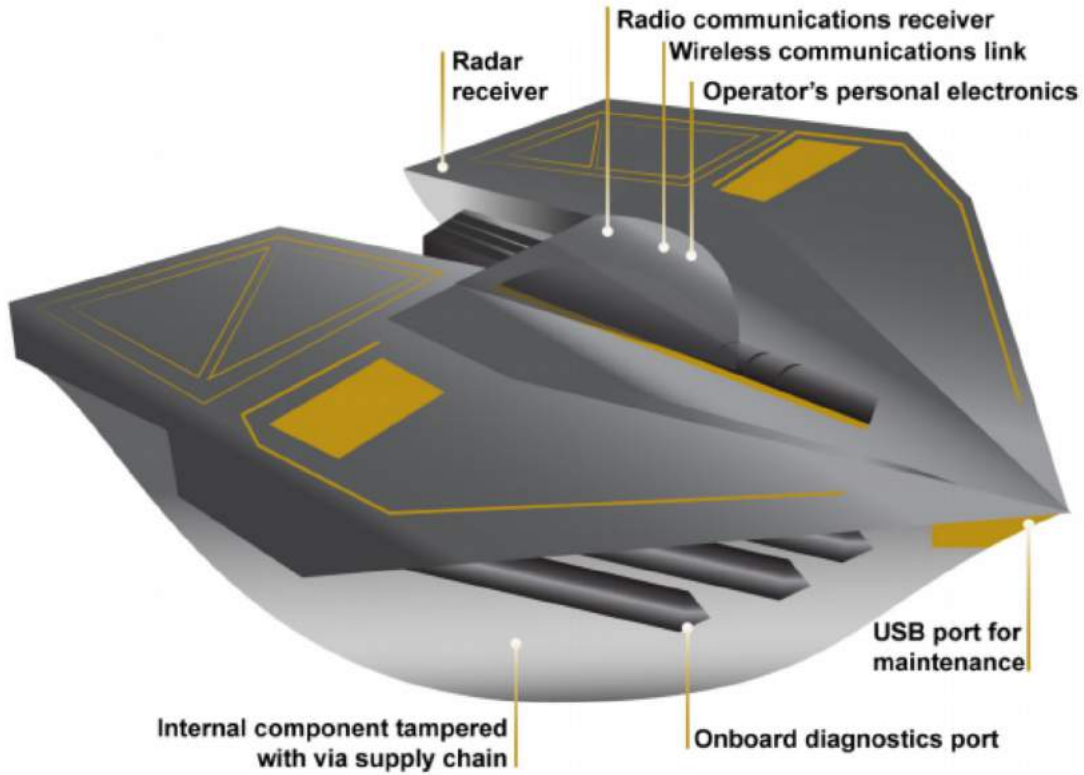
How are federal agencies administering this spending?



https://www.washingtonpost.com/us-policy/2020/06/25/irs-stimulus-checks-dead-people-gao/

Findings in U.S. GAO report on weapon systems' audit (2018)

1. Delays in patch testing and applying
2. Not understand the multitude of information flows, underestimate the attack surface
3. A two-person test team took 1 hour to gain initial access to a weapon system
4. Unauthorized data access, hijacking of an operator's terminal
5. Guessed an admin pwd in 9 seconds
6. Unencrypted pwd files
7. Uncorrected vulnerabilities (e.g., due to contractor errors)
8. Operators thought crashing is normal, not due to attacks



Source: GAO analysis of Department of Defense information. | GAO-19-128

https://www.gao.gov/products/GAO-19-128

More findings from the GAO audit

Needs dual knowledge: weapon system (e.g., aircraft, radar) + security

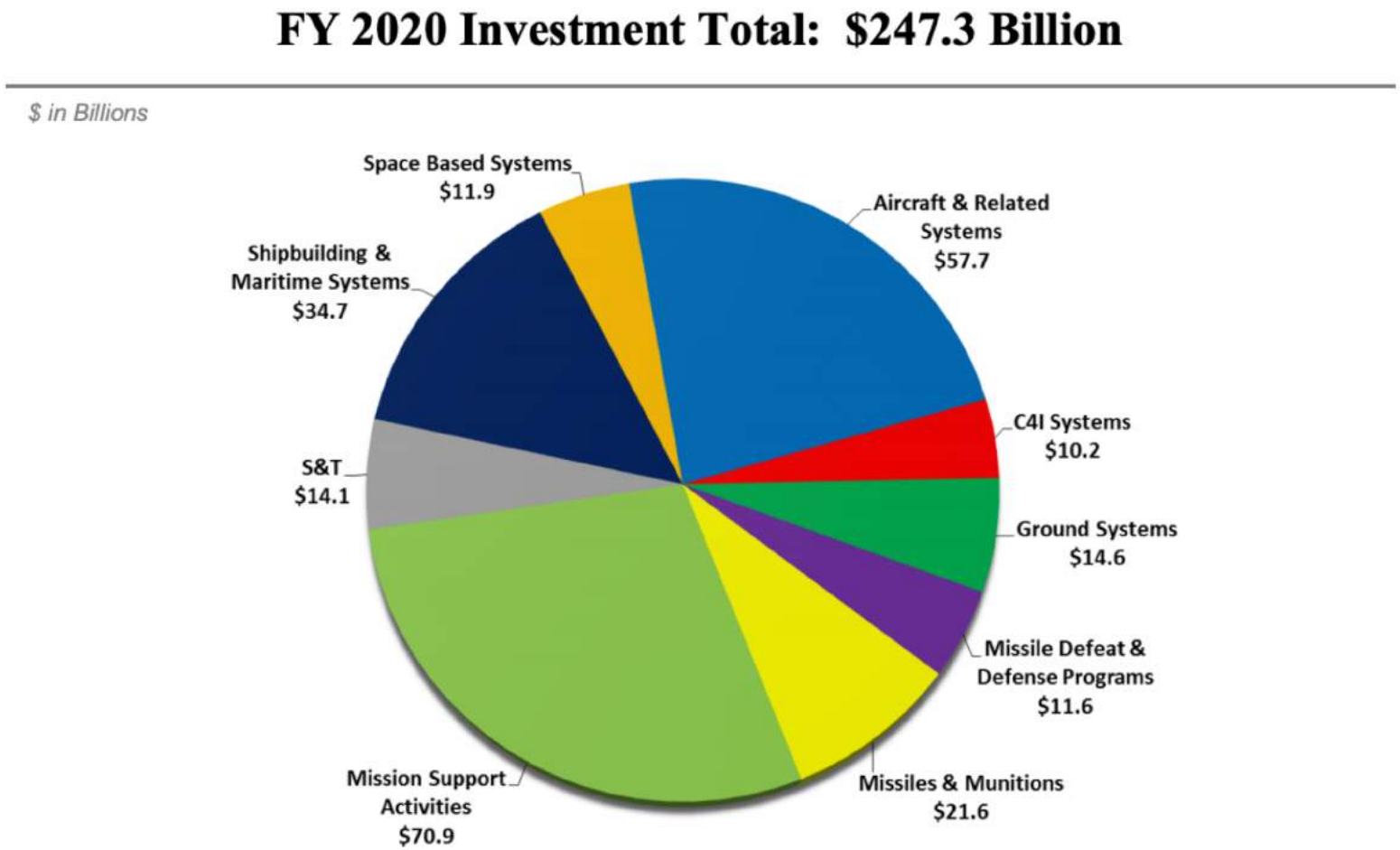
"Officials expressed confidence in the cybersecurity of their systems, but could not point to test results to support their beliefs."

- Poorly implemented security controls (i.e., defenses) are common

Losing cybersecurity talents to private sectors

https://www.gao.gov/products/GAO-19-128

Acquisition (Procurement and Research, Development, Test, and Evaluation) funding



Cybersecurity focus areas:

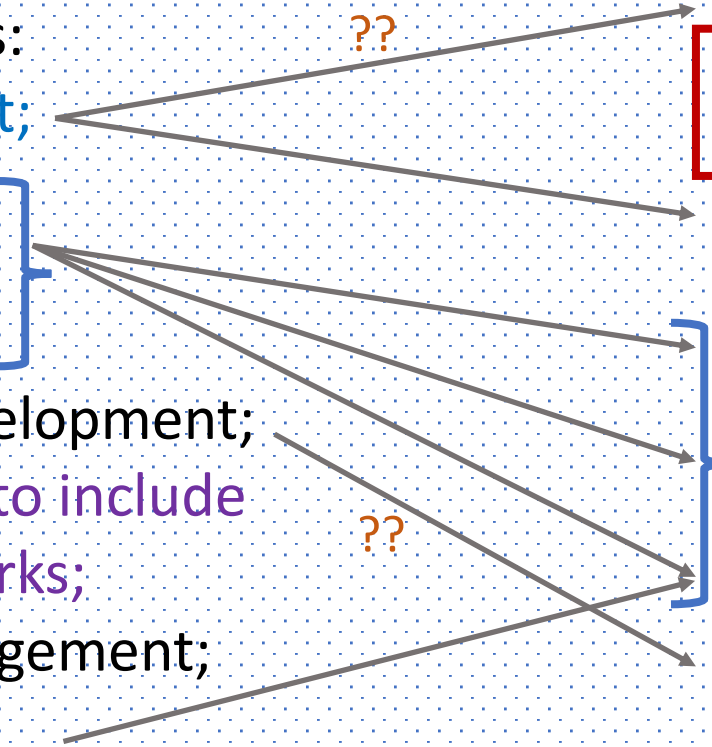
- end point management;
- credential and access management;
- insider threat security;
- secure application development;
- cross-domain security to include mission partner networks;
- supply chain risk management;
- encryption;
- other critical infrastructure

https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2020/fy2020_Weapons.pdf

Mapping between focus areas (in funding) and issues found by GAO

Cybersecurity focus areas:

- end point management;
- credential and access management;
- insider threat security;
- secure application development;
- cross-domain security to include mission partner networks;
- supply chain risk management;
- encryption;
- other critical infrastructure



Issues found in GAO report:

1. Delays in patch testing and applying
2. Not understand the multitude of information flows, underestimate the attack surface
3. A two-person test team took 1 hour to gain initial access to a weapon system
4. Unauthorized data access, hijacking of an operator's terminal
5. Guessed an admin pwd in 9 seconds
6. Unencrypted pwd files
7. Uncorrected vulnerabilities (e.g., due to contractor errors)
8. Operators thought crashing is normal, not due to attacks

Security is a risk management problem

The timing element in some CPS applications

Fiscal year	2012	2013	2014	2015	2016	2017	2018
Overall MC rate	77.90%	77.80%	73.70%	73.10%	72.10%	71.30%	69.97%

US Air Force mission-capable rate (of 5413 aircrafts)

F-22's top speed:
1,500 mph (2414 kph)

Secure by virtue of short mission time? Would it work?

https://www.airforcetimes.com/news/your-air-force/2019/07/26/aircraft-mission-capable-rates-hit-new-low-in-air-force-despite-efforts-to-improve/

Deadly Patriot Missile Defense System Failure

25 February 1991: US Patriot system failed to intercept an incoming Iraqi Scud missile at an army base in Saudi Arabia

However, Patriot battery had been up around **100 hours**

0.34 second
(chopping error)

*

1,676 meters per second
(Scud's speed)

http://www-users.math.umn.edu/~arnold/disasters/patriot.html
https://www.cnbc.com/2017/12/04/patriot-defense-system-likely-failed-in-saudi-ballistic-missile-attack.html

VIRGINIA TECH

Secure by virtue of short mission time does not work

Short fly/mission time  No need to secure the device

Secure by being obsolete?

Legacy software support

COVID and COBOL

04-10-20 | CORONAVIRUS

COBOL, a 60-year-old computer language, is in the COVID-19 spotlight

As state governments seek to fix overwhelmed unemployment benefit systems, they need programmers skilled in a language that was passé by the early 1980s.

COBOL Program Developer

ISSI 4.7 ★

New York, NY • Remote work available

$50 - $60 an hour

Requirements

COBOL Programming: 5 years

Easily apply

- Experienced hands-on mainframe developer that will contribute to all aspects of application development.
- Activities will also include defining functional and...

1 day ago · Save job

https://www.fastcompany.com/90488862/what-is-cobol

Slow progression of military CPS systems

(2001) When F-22 Raptor moved into production (after a decade development), its Intel i960MX processor **went out of production 4 years ago**

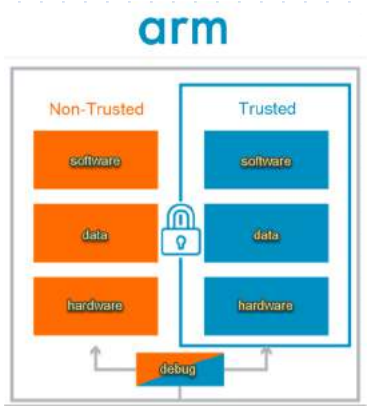
(2016) Pave Hawk to use a new control-display unit with a PowerPC processor, as CMA-882 CDU was no longer procurable

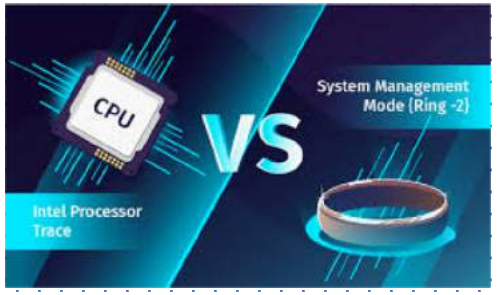
Power Macintosh

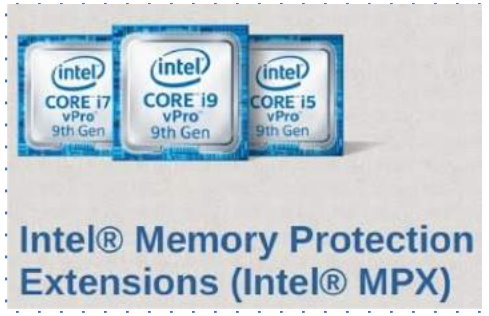
June 19, 1995: Apple releases the Power Macintosh 9500, a high-end Mac that boasts a second-generation PowerPC chip that's much faster than its predecessor.

https://www.militaryaerospace.com/computers/article/16710716/f22-avionics-designers-rely-on-obsolescent-electronics-but-plan-for-future-upgrades
https://www.militaryaerospace.com/computers/article/16710502/cmc-uses-cots-to-develop-family-of-optical-avionics-displays

Fancy hardware security features cannot be used on legacy systems, e.g., ARM TrustZone, Intel SGX, Intel MPX, Intel PT…







Researchers: to help secure legacy systems? Or to publish on cool new technologies?

N. Asokan's talks on TEE: https://asokan.org/asokan/research/talks.php

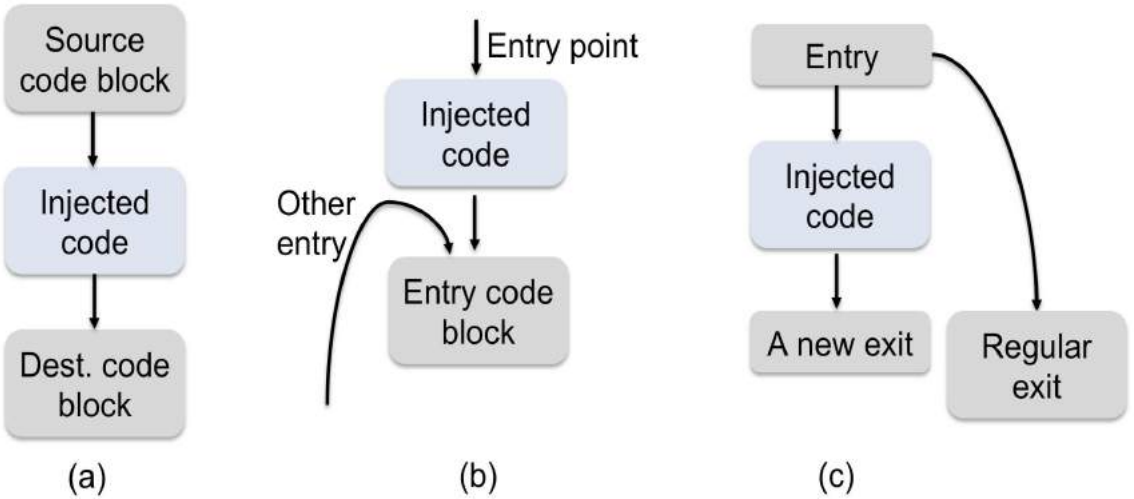
An SoK paper on TEE: https://arxiv.org/pdf/1910.04957.pdf

VIRGINIA TECH

Researchers:
To help secure legacy systems?
Or to publish about cool new technologies?

Legacy systems are less researched, less understood, less supported for security

E.g., for platform dependent code analysis, instrumentation (static or dynamic)



Security code placements for instrumenting binaries (following DynInst)

```
1.  struct Coordinate {
2.      double lat, lon, alt;
3.  };
4.  struct WaypointManager {
5.      unsigned int size; //for total number of coordinates
6.      struct Coordinate *coordinates; //a list that holds coordinates
7.  };
8.  struct Drone {
9.      void fly(struct WaypointManager *wp);
10. };
11. void drone_manage(){
12.     struct WaypointManager wp; // create an instance of WaypointManager
13.     struct Drone dr; // create an instance of Drone
14.     wp.size = receive_size(); //get the number of coordinates
15.     if (wp.size > 0) {
16.         wp.coordinates = (struct Coordinate *)malloc(wp.size*sizeof(Coordinate));
17.         for (int i = 1; i <= wp.size; i++)
18.             wp.coordinates.add(receive_coordinates_from_network());
19.         dr.fly(wp);
20.     }
21. }
```

E.g., vulnerable waypoint management code lacking proper boundary checking

Angr: a multi-architecture binary analysis toolkit (no PowerPC support)

More findings from the GAO audit

Needs dual knowledge: weapon system (e.g., aircraft, radar) + security

"Officials expressed confidence in the cybersecurity of their systems, but could not point to test results to support their beliefs."

Poorly implemented security controls (i.e., defenses) are common

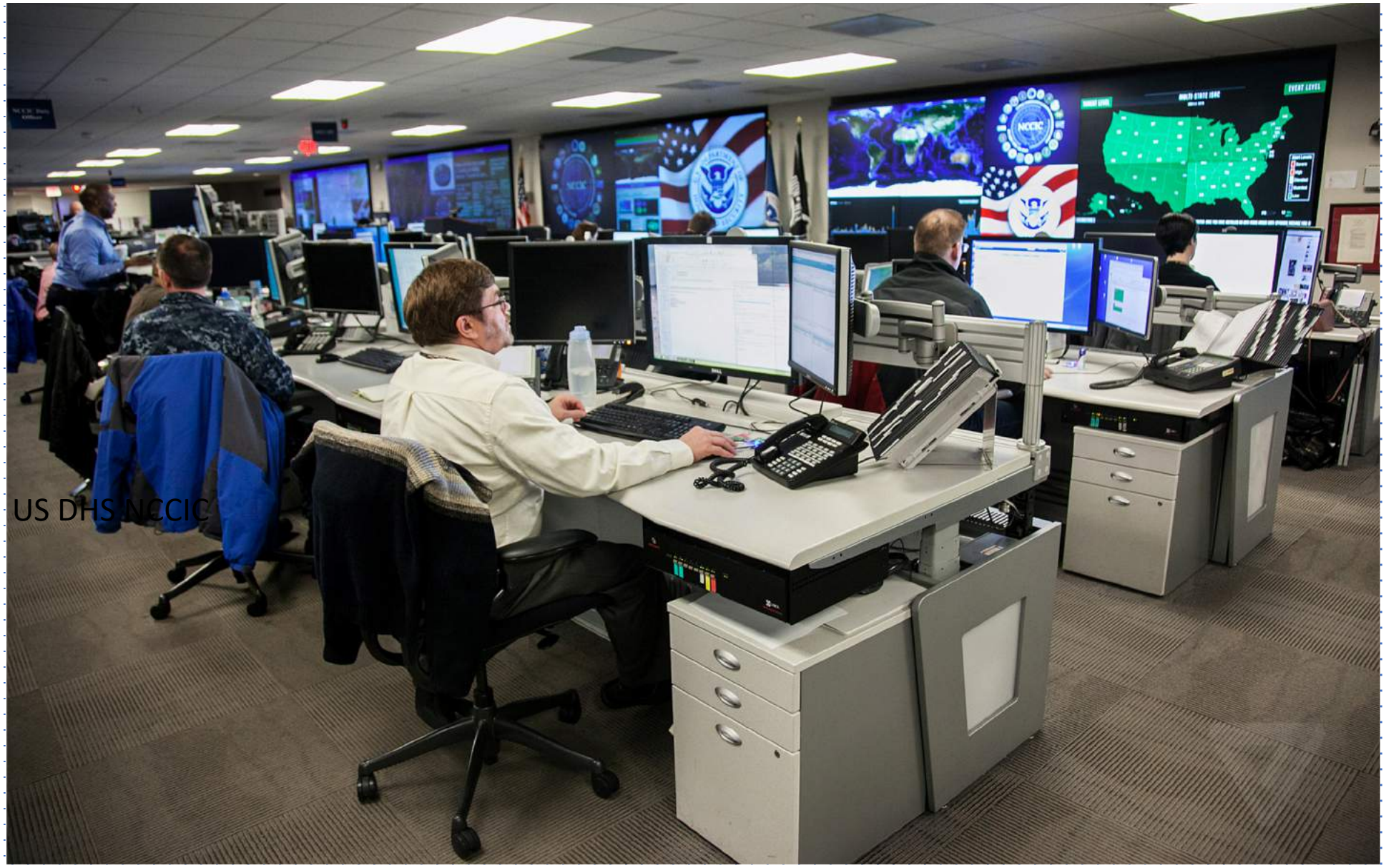
Losing cybersecurity talents to private sectors

https://www.gao.gov/products/GAO-19-128

Security of ICS and defense in depth

Image from: https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

National Cybersecurity and Communications Integration Center (DHS)

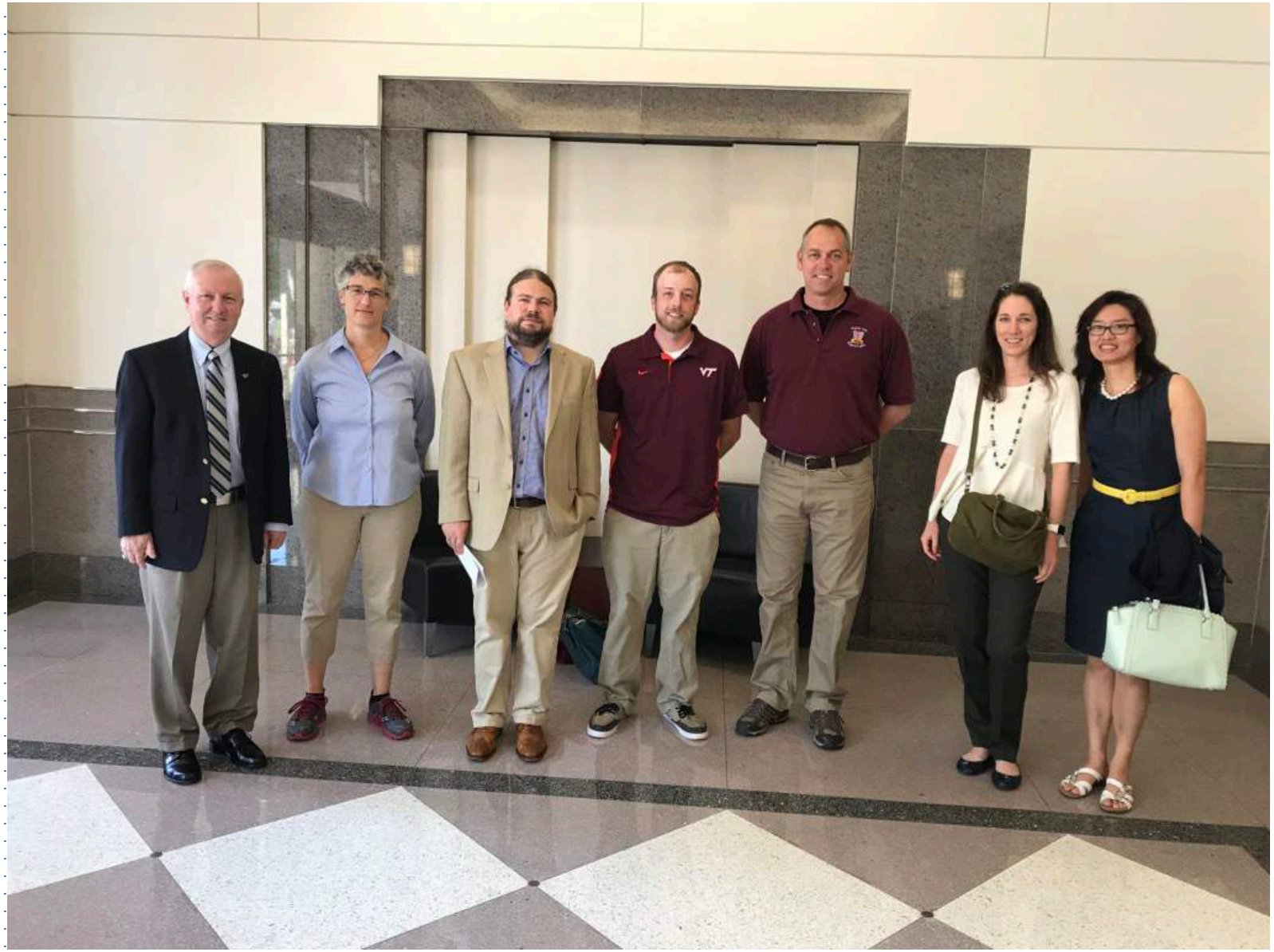


US DHS NCCIC

https://www.theverge.com/2016/5/6/11601248/nccic-tour-photos-cyber-attack-hq-dhs

VIRGINIA TECH

DHS NCCIC welcomes visitors



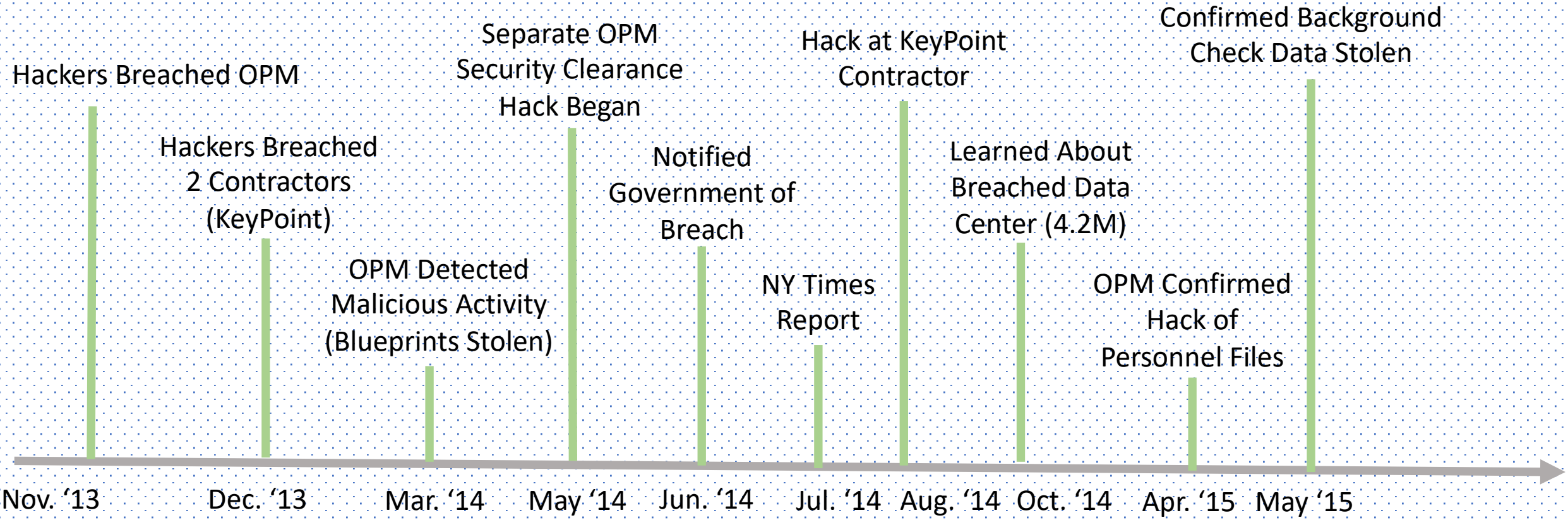
New name:

CISA
CYBER+INFRASTRUCTURE

Old name:

2015 U.S. Office of Personnel Management (OPM) data breach

More than 21.5 million sensitive background check files (including fingerprints of secret agents) were stolen



https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html

https://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/

Discovery of OPM Data Breach (Detected in 2015)

opmsecurity.org
registered in April ‘14

1. SSL signal pinging detected in May ‘15

2. PlugX malware attached to mcutil.dll (on ~10 OPM machines)

F-86, a 127-page questionnaire for security clearance

Data center gateway infected w/ PlugX

Used KeyPoint credential while owner on vacation

KeyPoint Government Solutions (contractor)

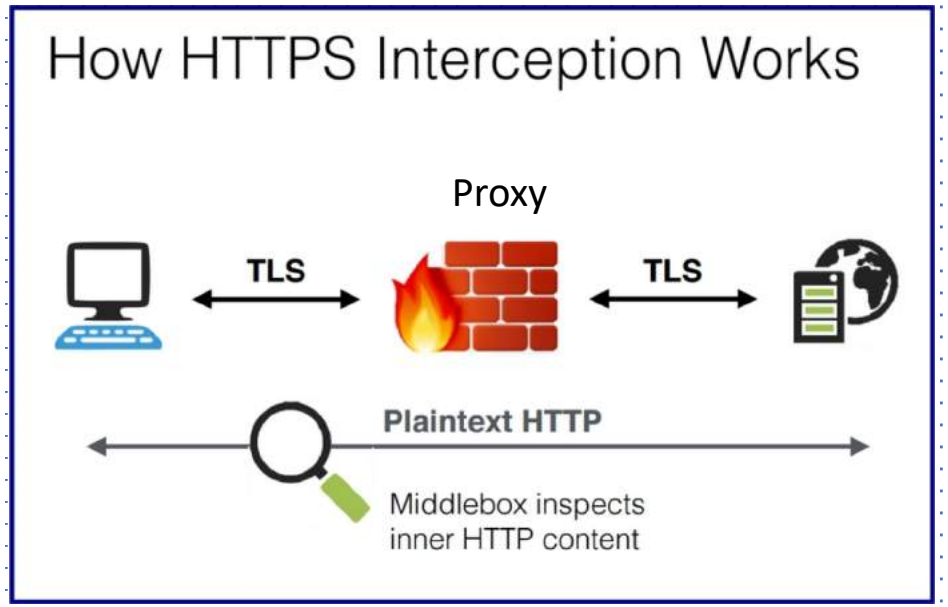
3. Interviews to identify which credentials were breached

OPM forensics team

https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

OPM contractor KeyPoint's security flaws in 2015

- No an outbound proxy (for data loss inspection)
- No process for regularly auditing on workstations, servers and databases
- No formal procedures for reviewing logs
- No formal process for auditing physical access privileges

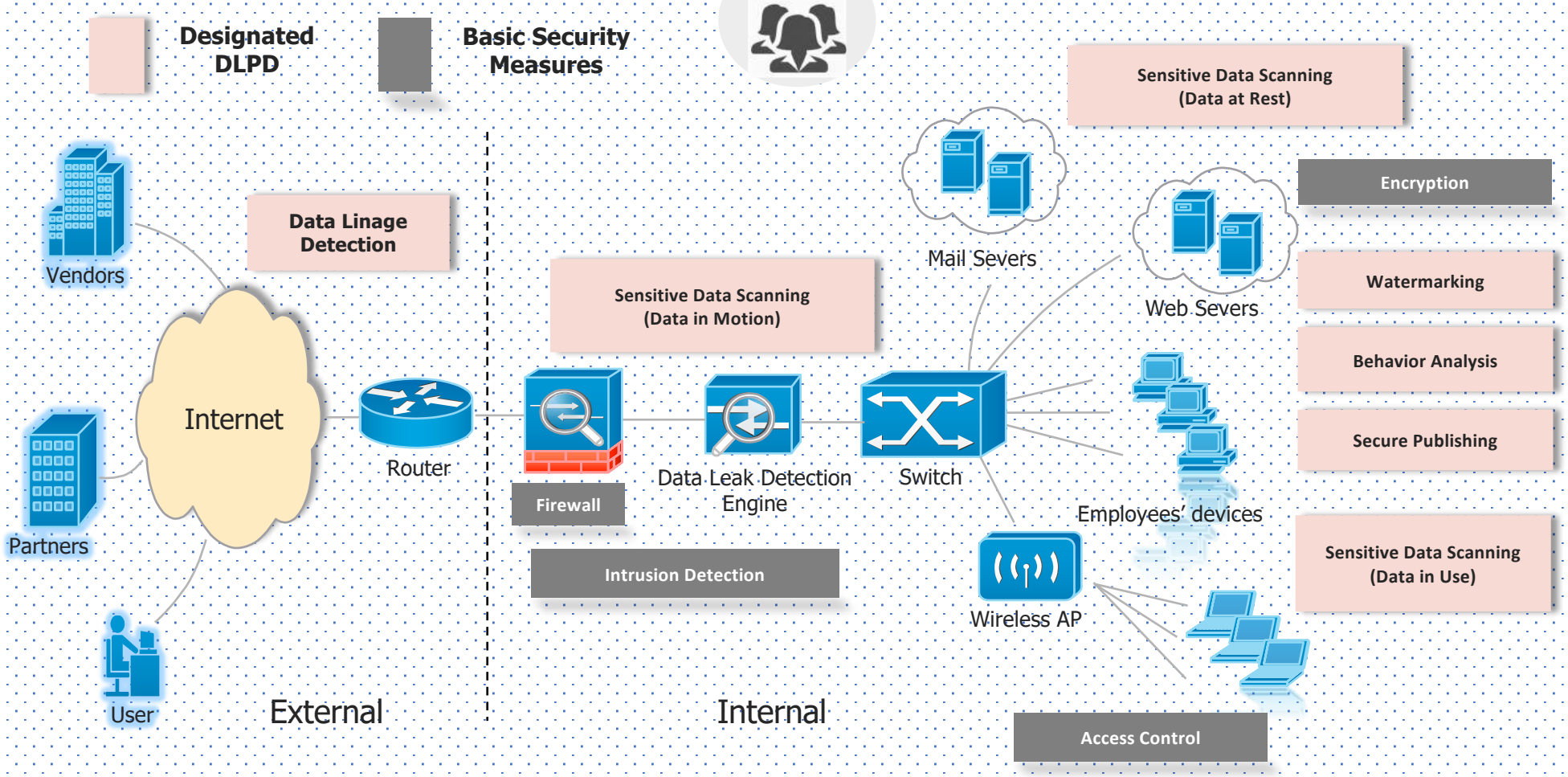


https://www.thesslstore.com/blog/ssl-inspection/
https://fcw.com/articles/2016/02/18/opm-oig-keypoint.aspx

Defense in depth for IT data loss prevention & detection

Developers **Security analysts** **Decision makers** **Operators**

Stakeholders

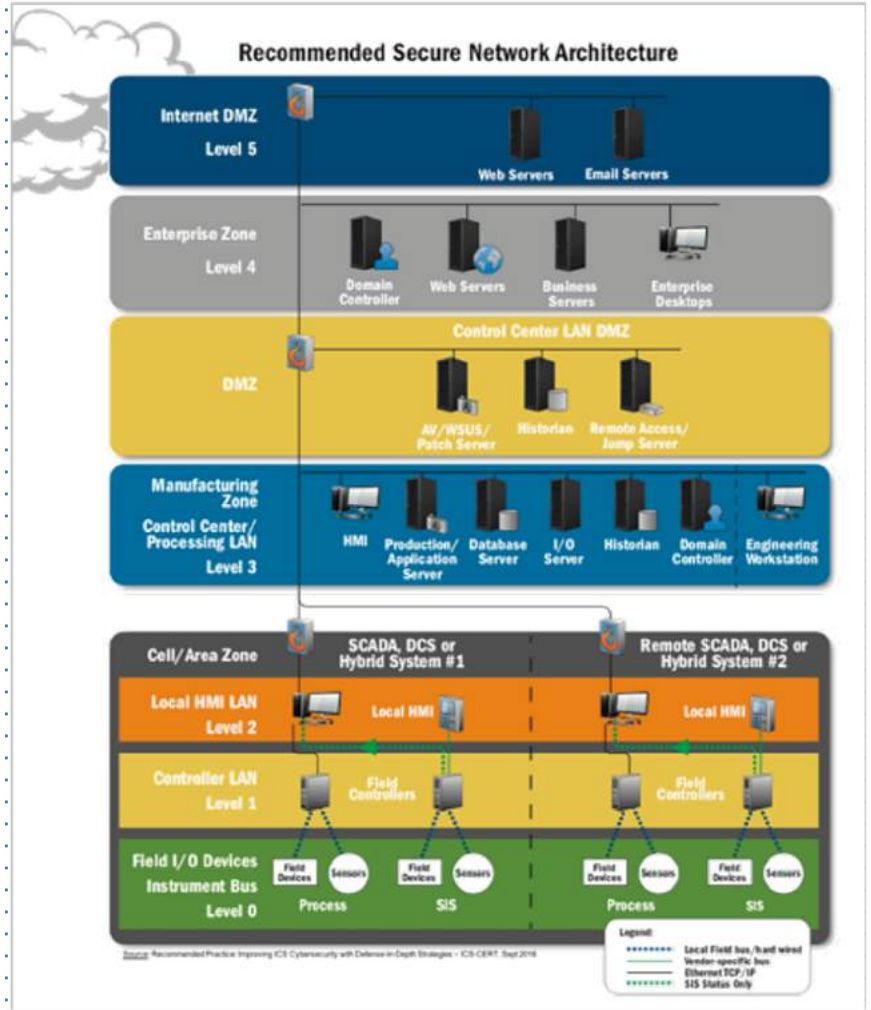


[IEEE TIFS '15, IEEE TIFS '16, ACM CODASPY '15, Wiley WIREs '17]
http://yaogroup.cs.vt.edu/publication.html

VIRGINIA TECH

A basic defense-in-depth question for an ICS CISO:

How big is my attack surface?



Important elements of a defense in depth strategy for SCADA systems are:

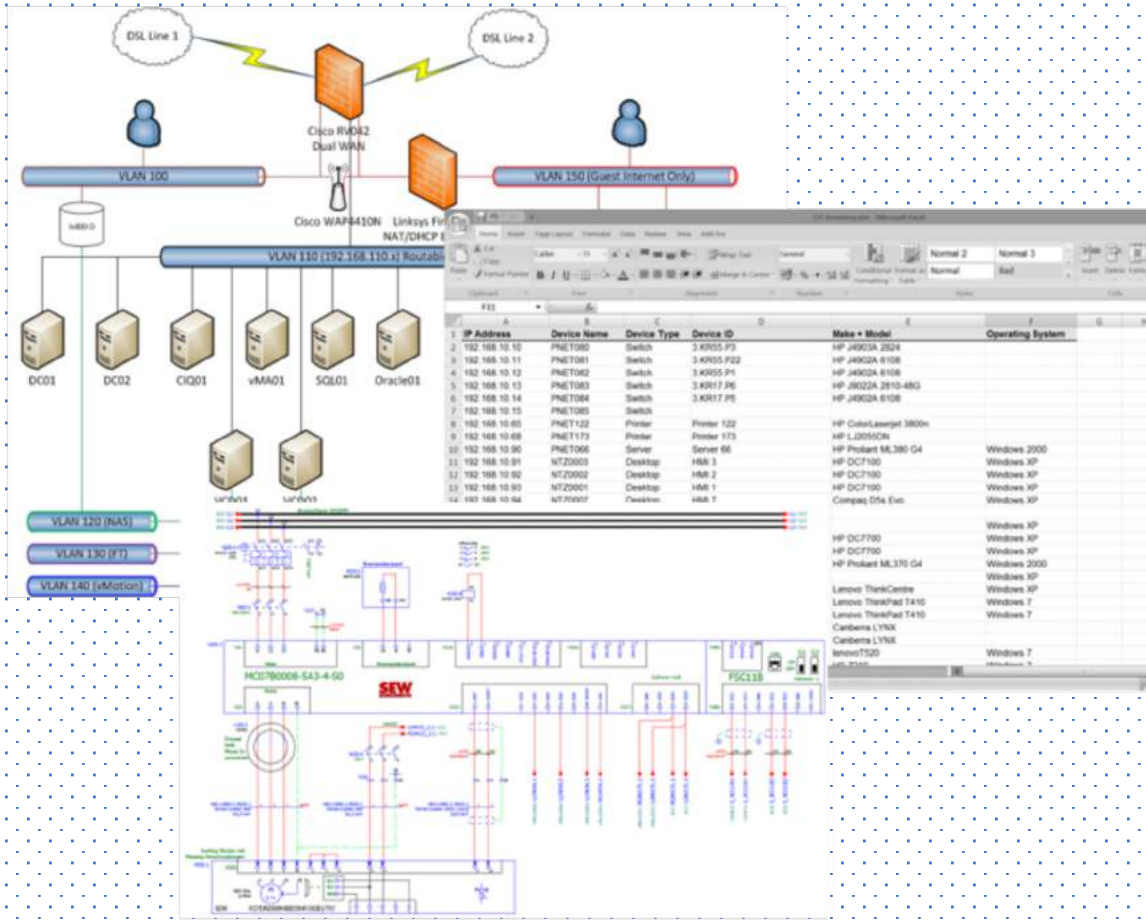
- Create awareness and understanding
- Network segmentation
- Remove unnecessary features
- Strong IO security (e.g., firewalls)
- Regular risk and security assessments
- Application white listing

https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems/at_download/fullReport

ICS asset discovery and management tools and their quality?

How well are discovery tools (scanning for used hardware/software) for complex and distributed systems?

Need objective and systematic measurement



OT-Base (a product)

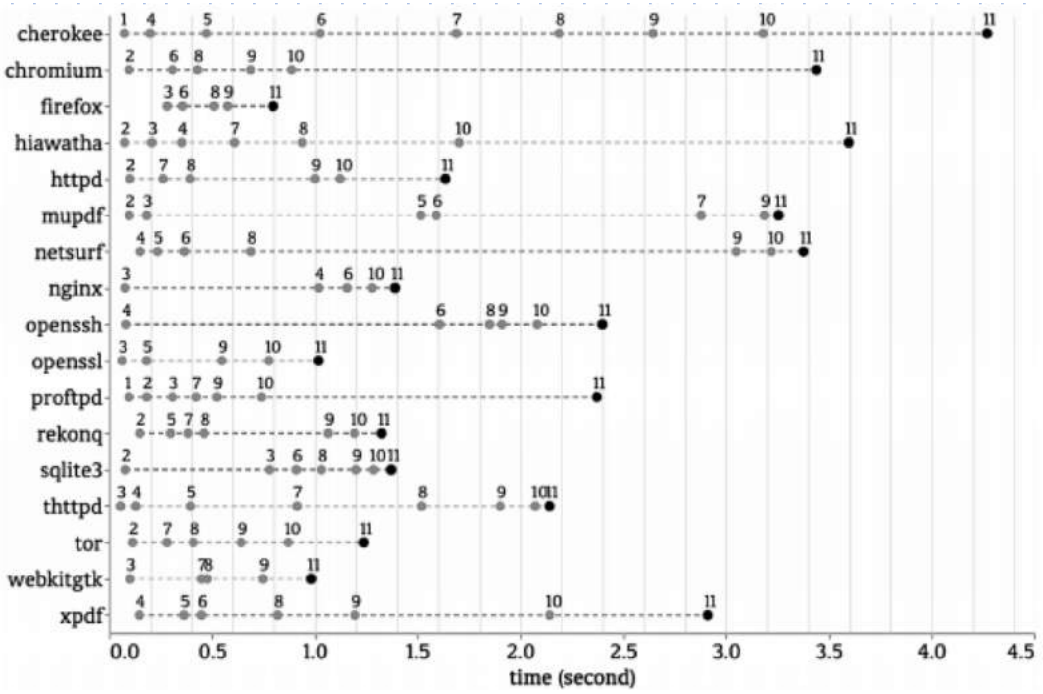
https://www.langner.com/ot-base/

https://www.csiac.org/journal-article/practical-industrial-control-system-ics-cybersecurity-it-and-ot-have-converged-discover-and-defend-your-assets/

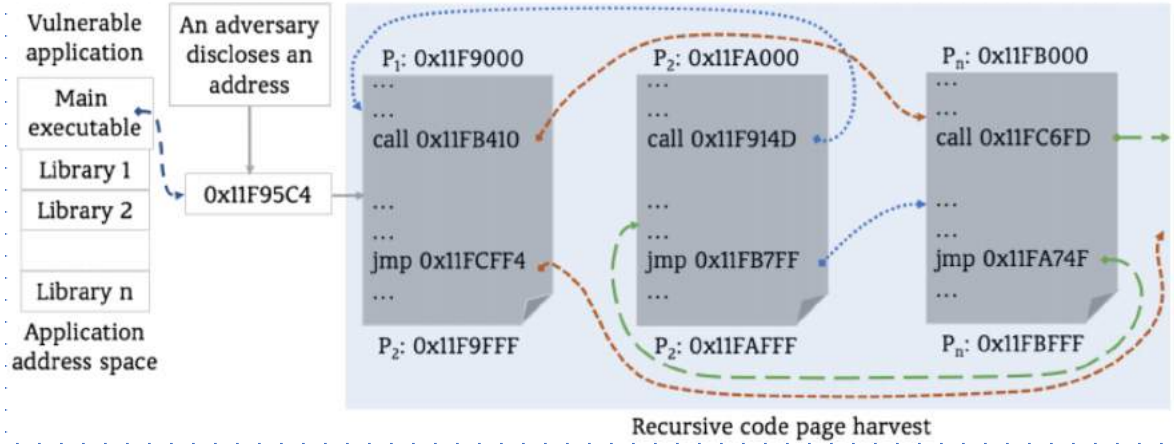
VIRGINIA TECH

We (cybersecurity researchers) shouldn't blindly accept some security products. Why?

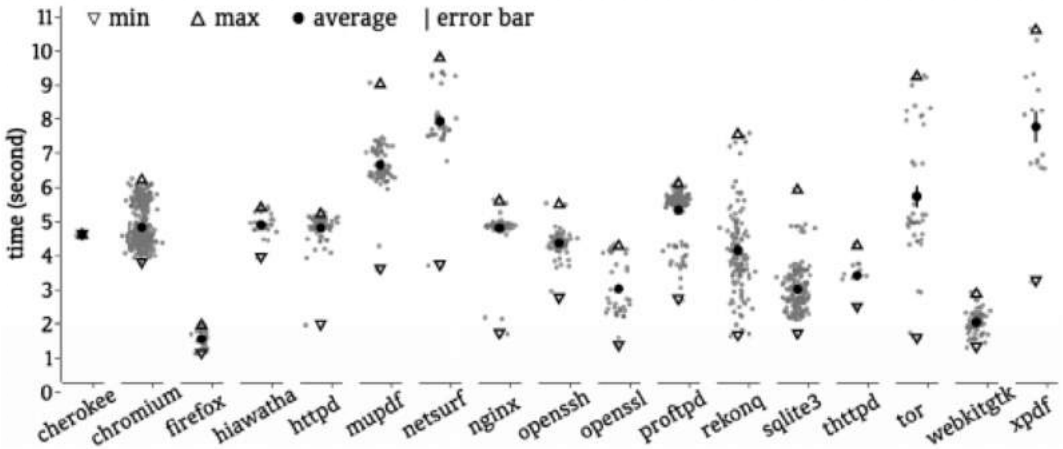
Our ASLR measurement work under JIT-ROP model (ACM CCS'20)



Result on re-randomization timing: minimum time to obtain the Turing-complete gadget set with a timeline



Just-in-time ROP attack circumvents fine-grained ASLR and even discovers randomly located code pages



Result: impact of starting pointer locations on gadget harvesting

Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP http://yaogroup.cs.vt.edu/

VIRGINIA TECH

A major fine-grained ASLR deployment deficiency: No current randomization tool can randomize the libc library

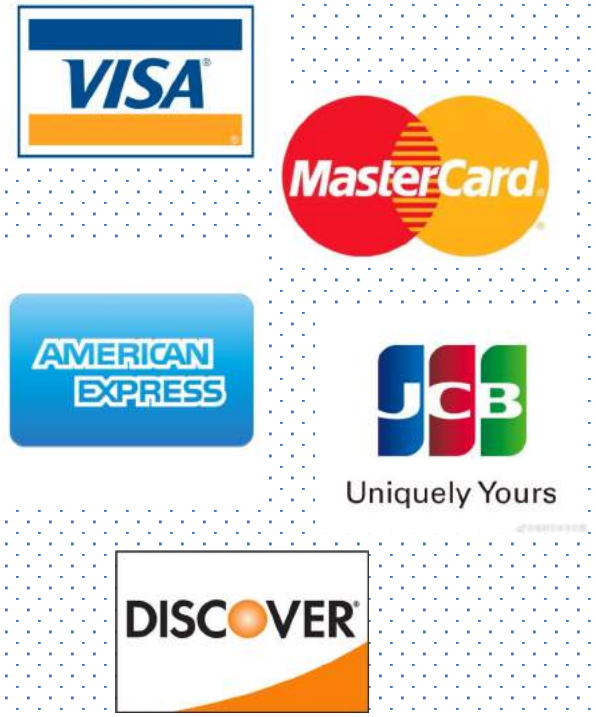
Reduction (%) of Turing-complete (TC) gadgets in 7 TC operations (MIN-FP | EX-FP)

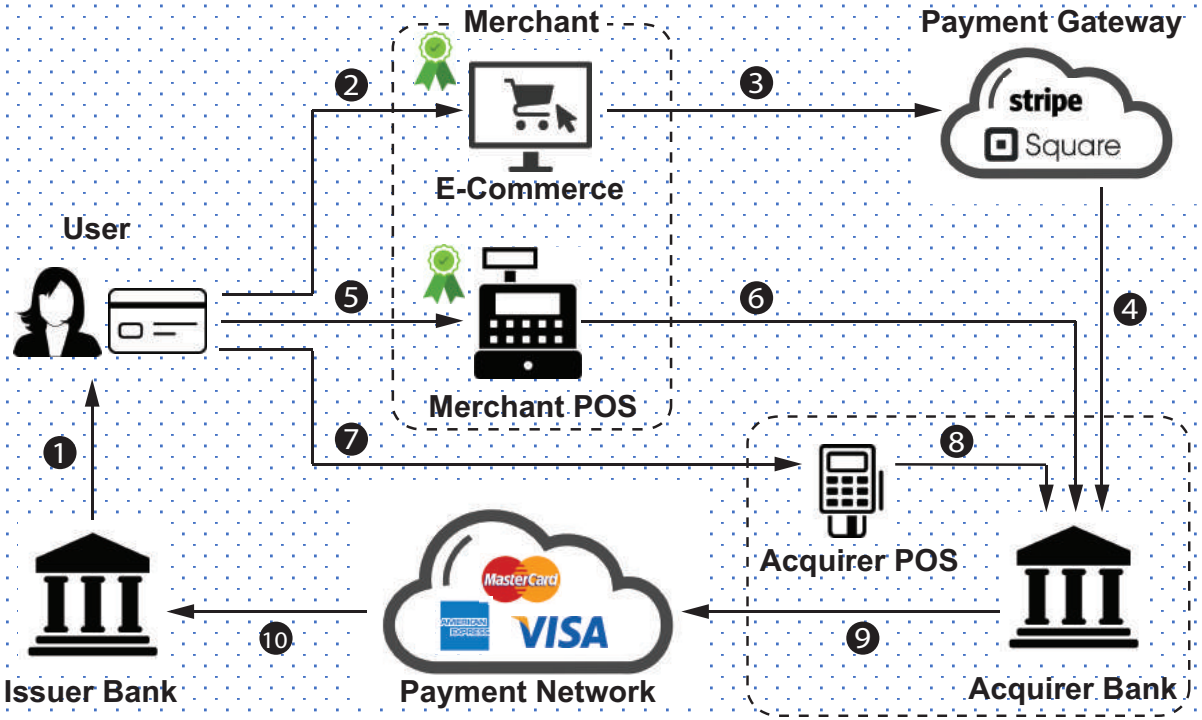
Randomization schemes	Granularity	⇓ (%) MIN-FP	⇓ (%) EX-FP	Memory	Assignment	Arithmetic	Logical	Control Flow	Function Call	System Call	TC Preserved?
Applications											
Inst. level rando.	Inst.	**79.7**	**82.5**	**97.4** | 82.7	58.8 | 81.7	**95.9** | 64.9	85.8 | 85.4	49.4 | 80.1	67.4 | 83.9	83.3 | 0	✗*
Func. level rando.	FB	27.63	36.55	0.8 | 29.2	10.6 | 43.5	19.3 | 15.1	35.1 | 35.9	21.1 | 29.1	18.2 | 46.9	0 | 0	✓
Func.+Reg. level rando.	FB & Reg.	17.62	42.37	-8.3 | 35.0	-5.1 | 35.2	26.1 | 44.9	21.3 | 38.1	34.0 | 60.2	11.8 | 64.9	80.0 | 0	✓
Block level rand.	BB	19.58	44.64	5.5 | 40.9	6.1 | 47	26.1 | 33.7	20.4 | 37.4	41.2 | 63.1	23.3 | 56.3	0.0 | 0	✓
Libraries											
Inst. level rando.	Inst.	**81.3**	**92.2**	**93.7** | 96.1	60.7 | 93	**91.8** | 84.9	84.5 | 90.4	59.8 | 93.5	51.8 | 92.9	66.7 | 0	✗*
Func. level rando.	FB	46.5	43.8	24.2 | 71.1	15.9 | 31	41.2 | 65.4	56.9 | 25	34.5 | 78.7	23 | 75.8	3.5 | 14.5	✓
Func.+Reg. level rando.	FB & Reg.	44.2	43.9	35.5 | 44.8	35.3 | 43.4	63.2 | 61.8	44.8 | 49.0	36.4 | 52.1	43.1 | 35.3	66.7 | 0	✓
Block level rand.	BB	20.98	37.0	7.3 | 36.3	8.1 | 32.1	13.9 | 55.9	24.8 | 31.6	22.2 | 52.1	18.1 | 44.6	50.0 | 0	✓

* For instruction-level randomization scheme [50], TC is not preserved for minimum footprint gadgets, but TC is preserved for extended footprint gadgets.

Another measurement work on payment card industry (PCI)

PCI data security standard (DSS) is a widely deployed standard for securing electronic payments

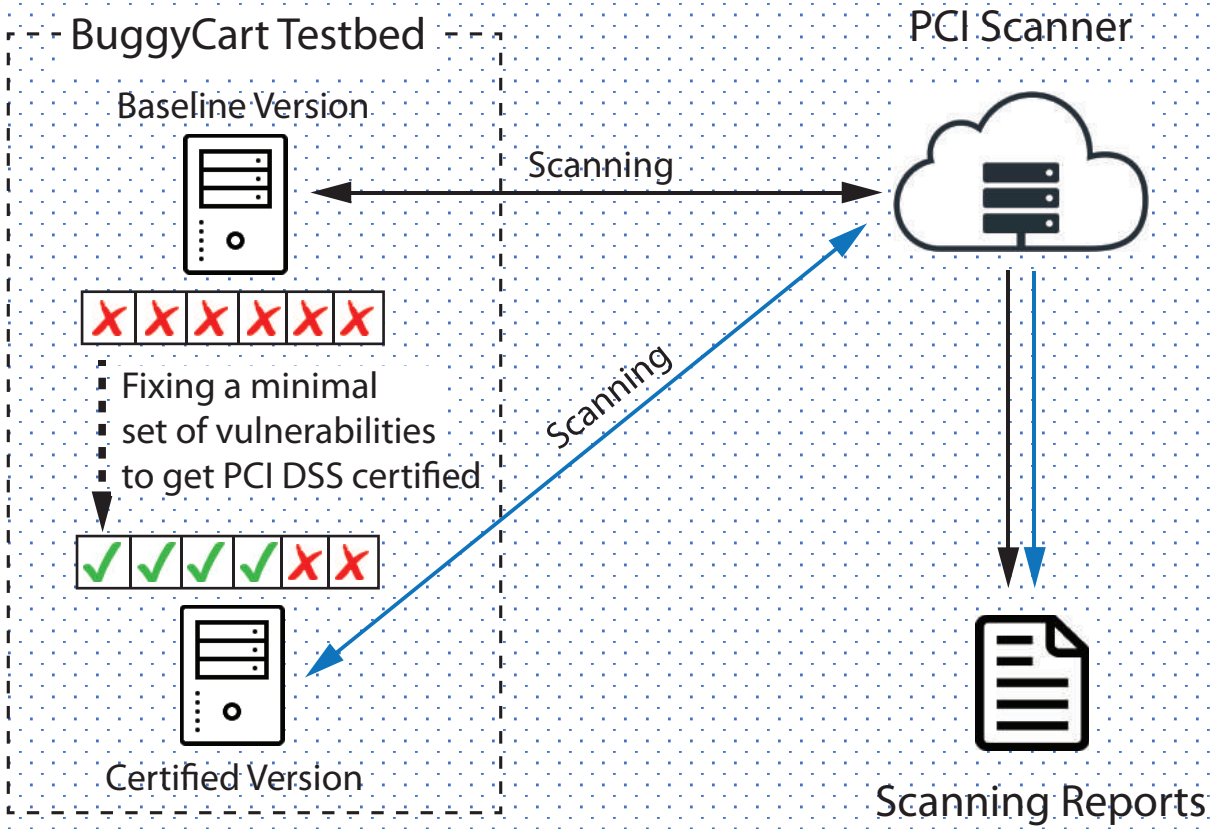




[ACM CCS 2019]

Our setup for evaluating the security of commercial PCI scanners

PCI Scanners	Price	Spent Amount
Scanner1	$2,995/Year	$0 (Trial)
Scanner2	$2,190/Year	$0 (Trial)
Scanner3	$67/Month	$335
Scanner4	$495/Year	$495
Scanner5	$250/Year	$250
Scanner6	$59/Quarter	$118
Scanner7	Unknown	N/A
Scanner8	$350/Year	N/A
Total	-	$1198



Scanning starts with all vulnerabilities enabled

[ACM CCS 2019]

Key takeaways from our PCI measurement study

5 out of 6 PCI scanners

certify

vulnerable

merchant sites

94% websites (out of 1,203)

Not PCI

compliant

[ACM CCS 2019]

Our measurement revealed commercial PCI scanners' deficiencies on application security

Rq.	Test Cases	Vul. Location	In ASV Scope?	CVSS Score	Must Fix?	Scanner2		Scanner5		Scanner4 / Scanner1		Scanner6 (not aprvd.)		Scanner3 (not aprvd.)		Website Scanners			
						Baseline	Certified	Baseline	Certified	Baseline	Certified	Baseline	Certified	Baseline	Certified	Scanner2W	Scanner5W	W3af	ZAP
6.5	21. Sql inject in admin login	Webapp	Y	9.8	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	22. Sql inject in customer login	Webapp	Y	9.8	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	23. Disable password retry limit	Webapp	Y	5.3	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	24. Allow passwords with len <8	Webapp	Y	5.3	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	25. Javascript source integrity check	Webapp	Y	9.8	Y	●	✓	✗	✗	✗	✗	✗	✗	✗	✗	-	-	-	-
	26. Don't hide program crashes	Webapp	Y	6.5	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	27. Implant XSS	Webapp	Y	6.1	Y	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	28. Implant CSRF	Webapp	Y	8.8	Y	◐	✓	✗	✗	✗	✗	✗	✗	✗	✗	-	-	-	-

"○", "◐", "●" means severity levels low, medium and high, respectively.

"✓" : requires fixing

"✗" : undetected

[ACM CCS 2019]

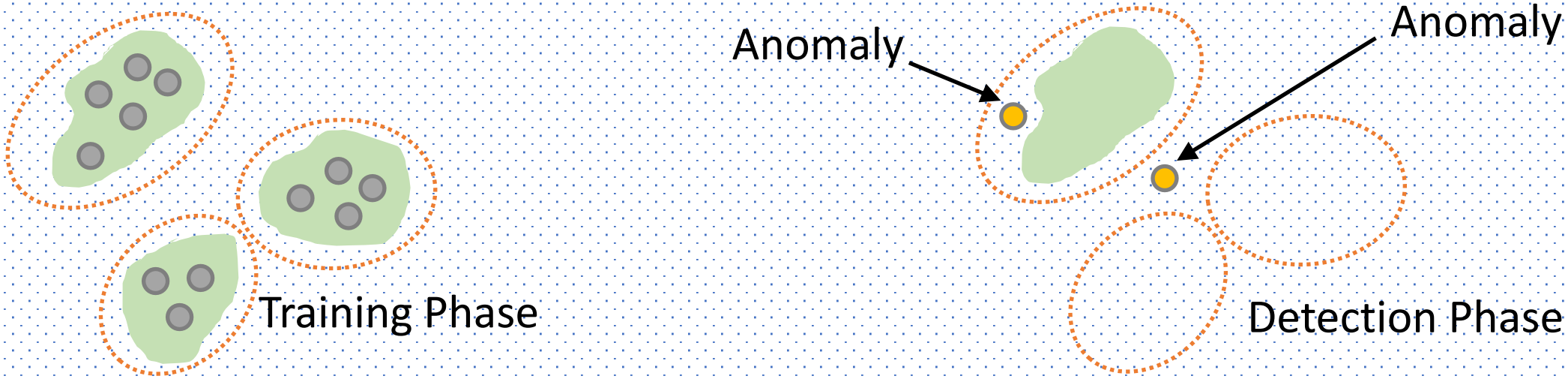
VIRGINIA TECH

PCI measurement shows big gaps between security knowledge & practice

VIRGINIA TECH

Securing OT as if securing IT?

Training anomaly detection models for IT



Anomaly detection in infinite-long system/function call traces

[Shu et al. CCS '15, ACM TOPS '17]

To reason program behaviors in CPS vs. a cyber system

Should a control command be issued?

Depends on the physical environment

```
while(…){
  eventRead();
  if(Push_Event())
    push-syringe();
  else if(Pull_Event())
    pull-syringe();
  …
}
```

Attacks on Control Branch

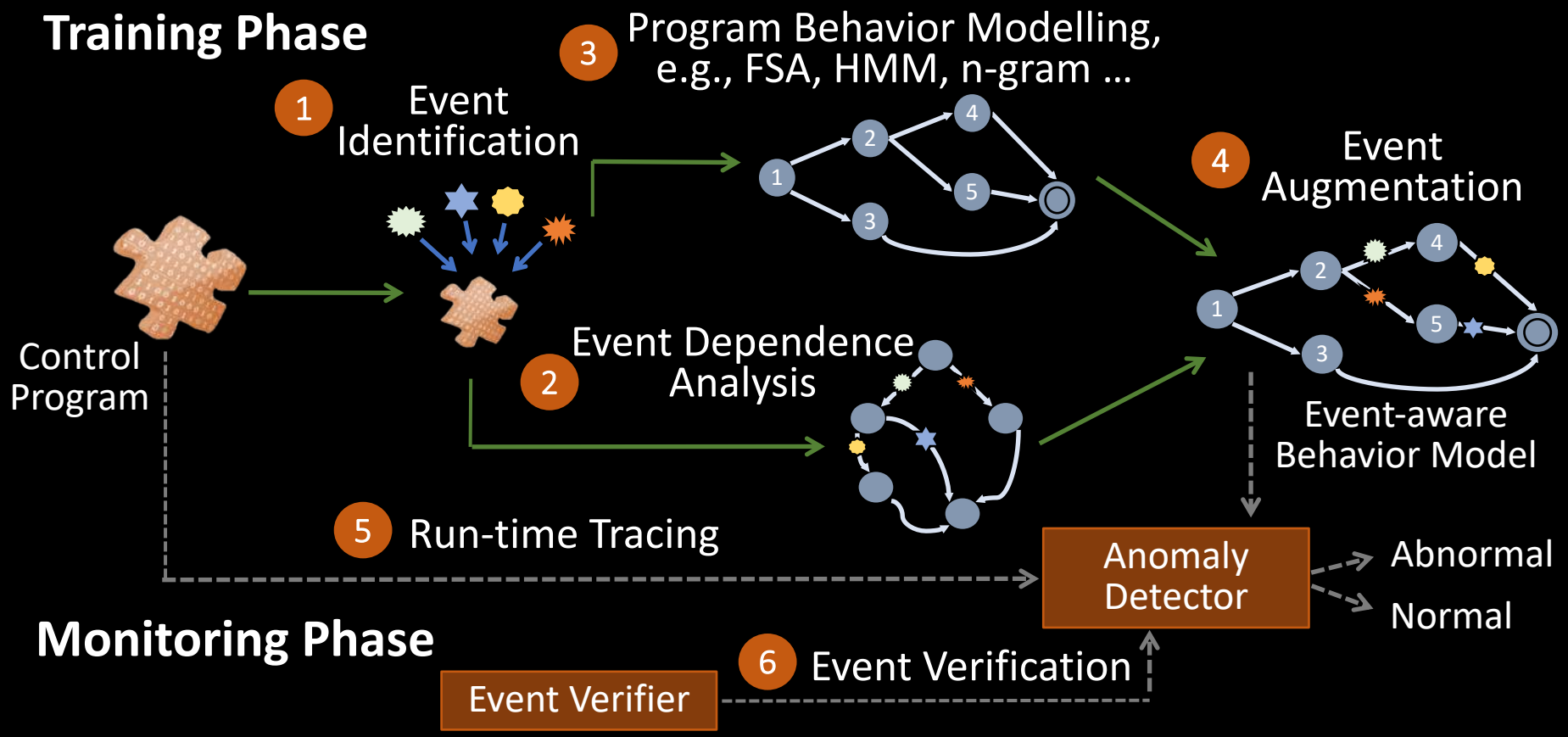
```
9  push-syringe(){
10   steps=…   ; //sensor data dependent
11   for(i=0; i<steps; i++)
12   {
13     write(i2c,…);
14     …
15   }
16 }
```

Attacks on Control Intensity

[ACSAC 2017, IEEE TDSC 2019]

http://yaogroup.cs.vt.edu/publication.html

Program Anomaly Detection in CPS



VIRGINIA TECH

But, how to do anomaly detection on legacy systems?

"The TDC2000 (a distributed control system, introduced in 1975) is still a very sizable portion. We have an extremely large installed base on the order of **$16 to $18 billion of TDC3000 equipment in the field** that was installed in the 80s and 90s."

-- Jason Urso, vice president of technology for Honeywell Process Solutions (2010)

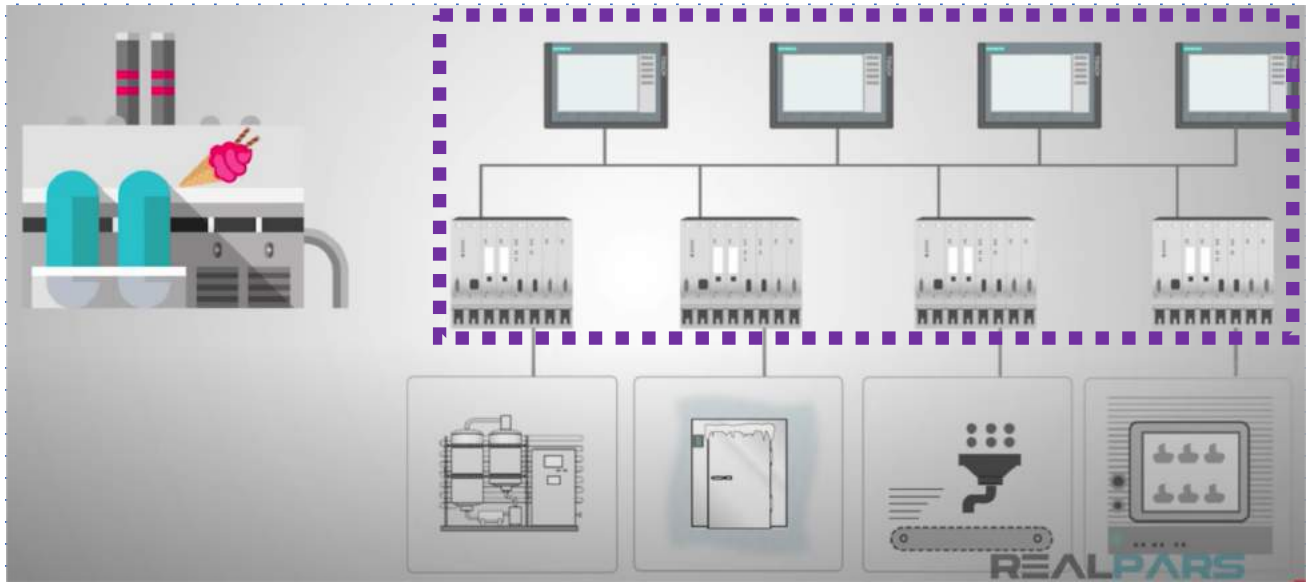
https://www.plantengineering.com/articles/control-system-lifespan-how-long-is-long-enough-2/

Honeywell's solution (ELCN) for technology obsolescence

Virtualization solutions to preserve and extend investments in decades-old DCS technology; ELCN emulates the TDC system as software (2018)

Chevron Oronite seeks to manage the lifecycle of its existing automation assets while employing new digital technologies.

Virtualization enables better connectivity, usability, cloud integration, security (e.g., anomaly detection)



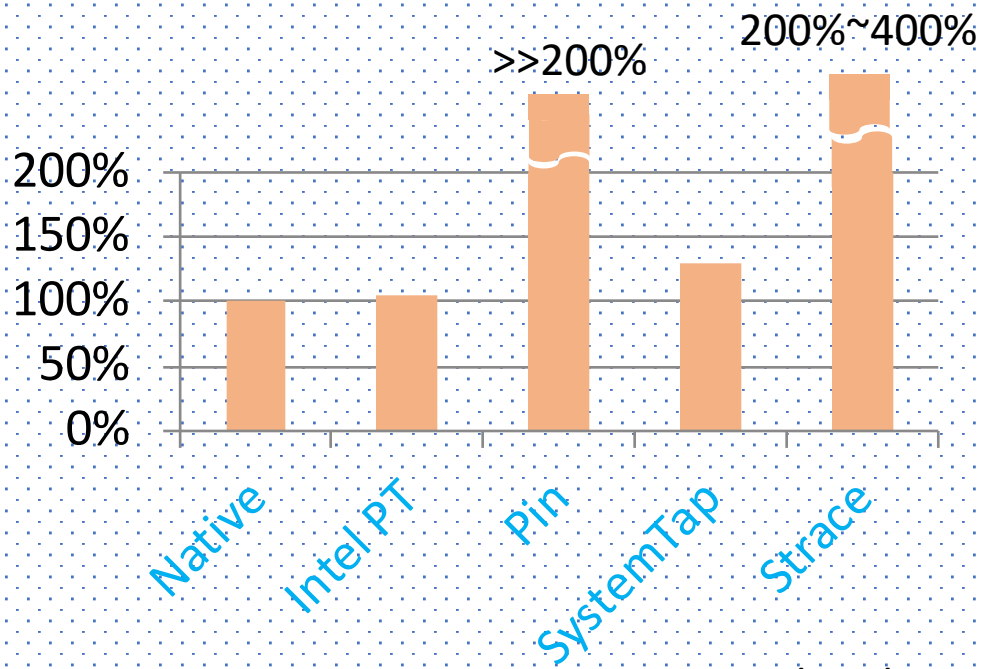
https://www.honeywellprocess.com/library/marketing/case-studies/HPS-Chevron-Oronite-Case-Study.pdf
https://www.youtube.com/watch?v=iF99iKlDpxA

My review article on deep learning anomaly detection for CPS

Deployment challenges:

- Need to state the threat model/security guarantees/limitations
- Evaluation on more real-world datasets (like SUTD's SWaT)
- Need more thorough performance evaluation, benchmarks
- To automate threshold/parameter selection
- Incremental/continuous training

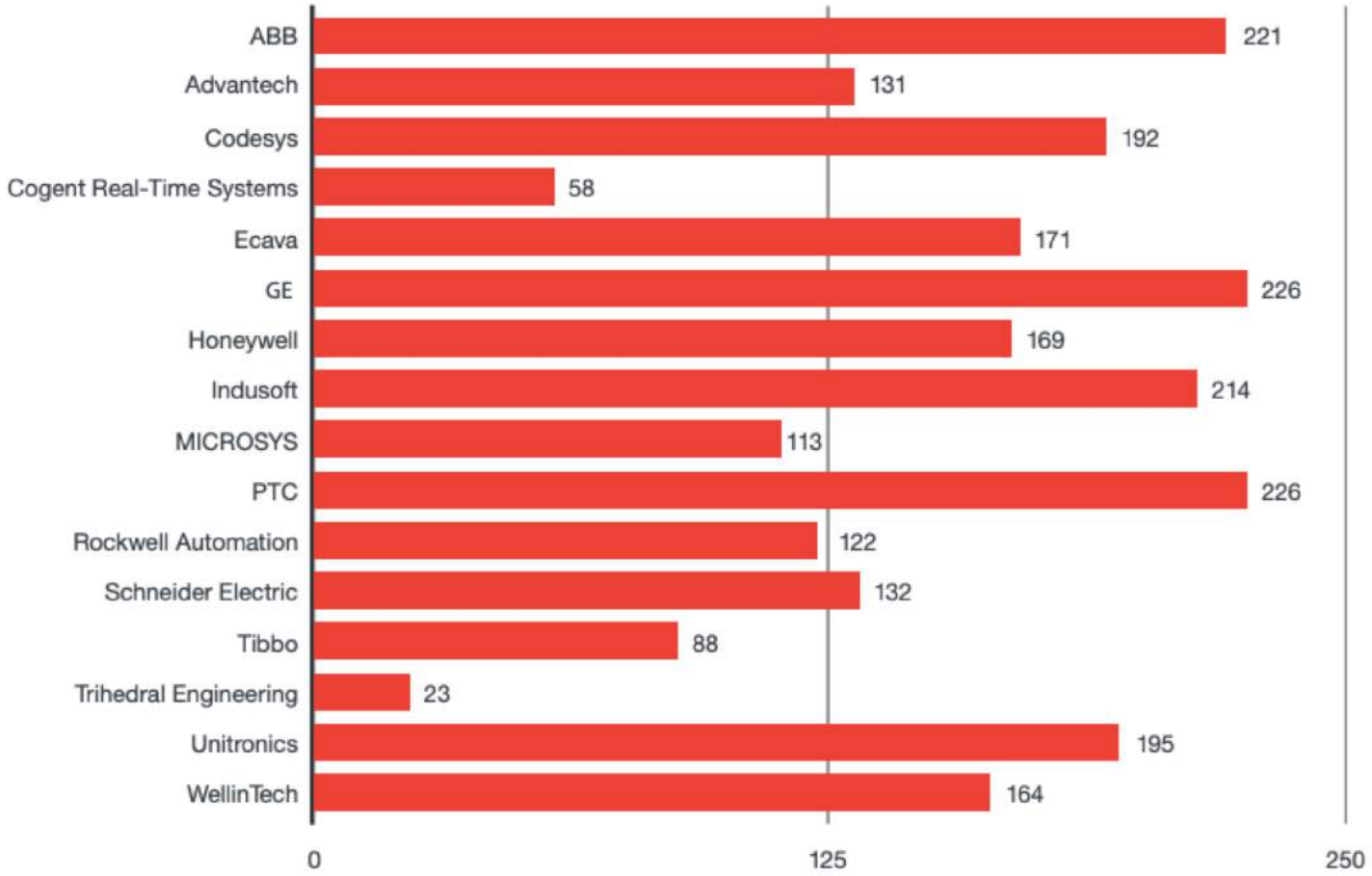
Secure Water Treatment Testbed (SUTD)



Runtime system tracing overhead

Available at: https://arxiv.org/pdf/2003.13213.pdf

How to expedite patching?



Mean time to patch vulnerabilities from the time they were disclosed by vendor

https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf (2017)

Equifax data breach --147 million consumers affected

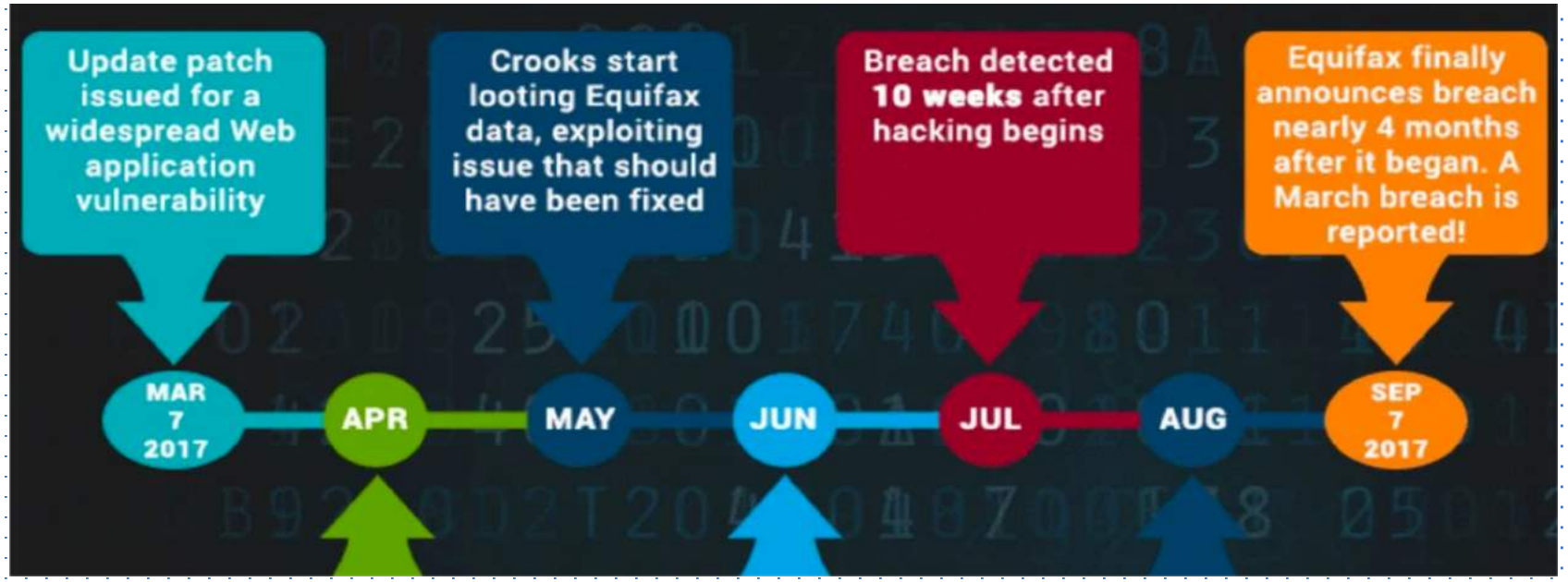
Apache Struts Vulnerability (CVE-2017-5638)

2017-03-06: vulnerability announced on along with a patch

2017-03-07: an exploit released

2017-07-30: Equifax patched

146 days: Time to patch at Equifax



https://www.gracefulsecurity.com/equifax-breach-timeline/

https://blog.blackducksoftware.com/equifax-apache-struts-cve-2017-5638-vulnerability

Vulnerability allows remote attackers to execute commands

For error-handling during file upload

```
1. if (multiWrapper.hasErrors()) {
2.    for (LocalizedMessage error : multiWrapper.getErrors()) {
3.       if (validation != null) {
4.          validation.addActionError(LocalizedTextUtil.findText(error.getClazz(),
error.getTextKey(), ActionContext.getContext().getLocale(),
error.getDefaultMessage(), error.getArgs()));
        }
     }
}
```

Vulnerability: Struts' error message render engine shows untrusted properties back to the user

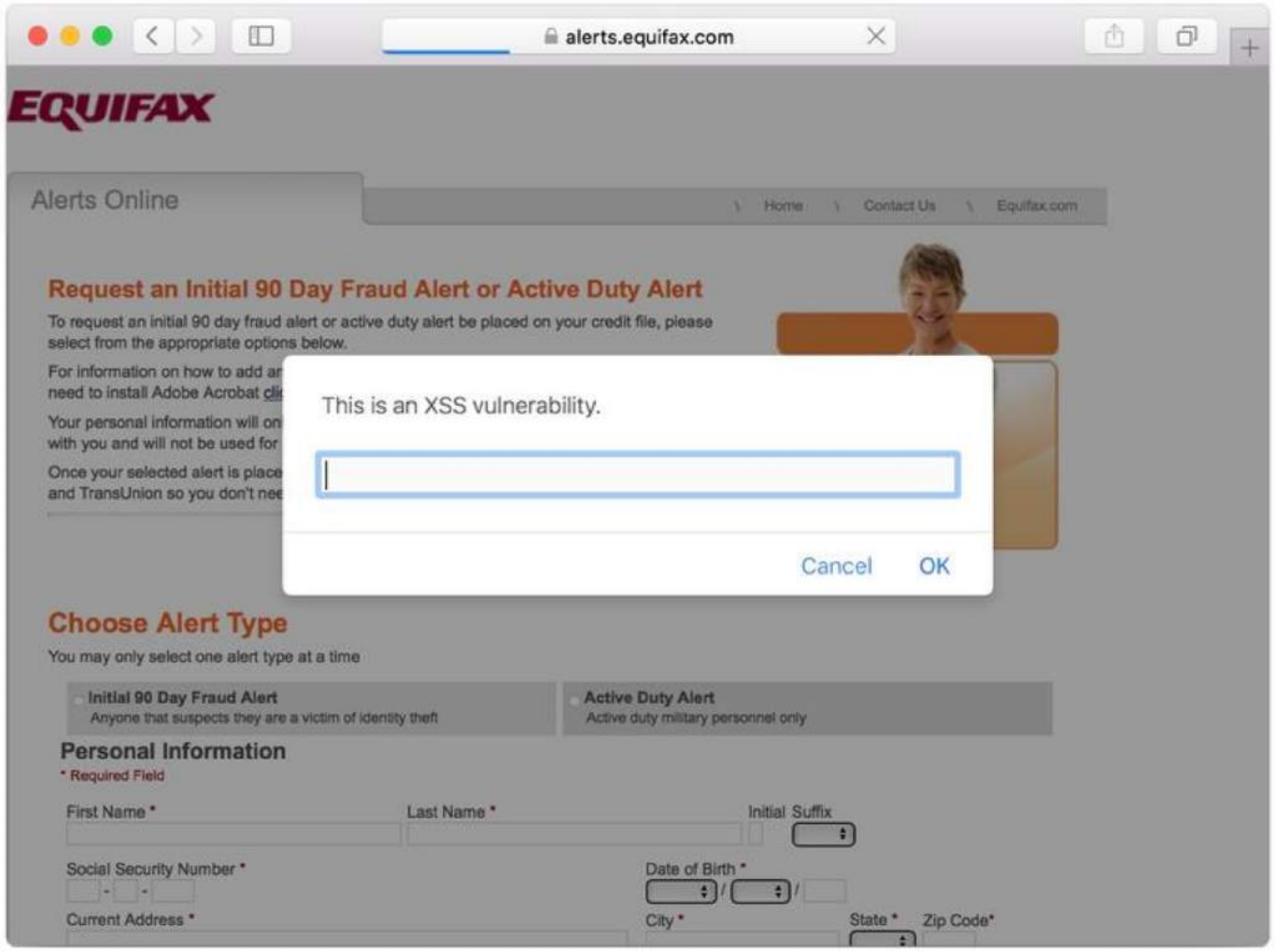
Apache Struts: an open-source framework for Java web applications

```
root@sh:~/struts2-S2-045# python exploit.py http://127.0.0.1:8080/2.3.15.1-showcase/showcase.action "ls -l"
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: ls -l

total 12
lrwxrwxrwx 1 root    root      12 Nov 15 09:37 conf -> /etc/tomcat8
drwxr-xr-x 2 tomcat8 tomcat8 4096 Nov 15 09:37 lib
lrwxrwxrwx 1 root    root      17 Nov 15 09:37 logs -> ../../log/tomcat8
drwxr-xr-x 2 root    root    4096 Mar  7 00:55 policy
drwxrwxr-x 3 tomcat8 tomcat8 4096 Mar  7 01:34 webapps
```

https://github.com/rapid7/metasploit-framework/issues/8064

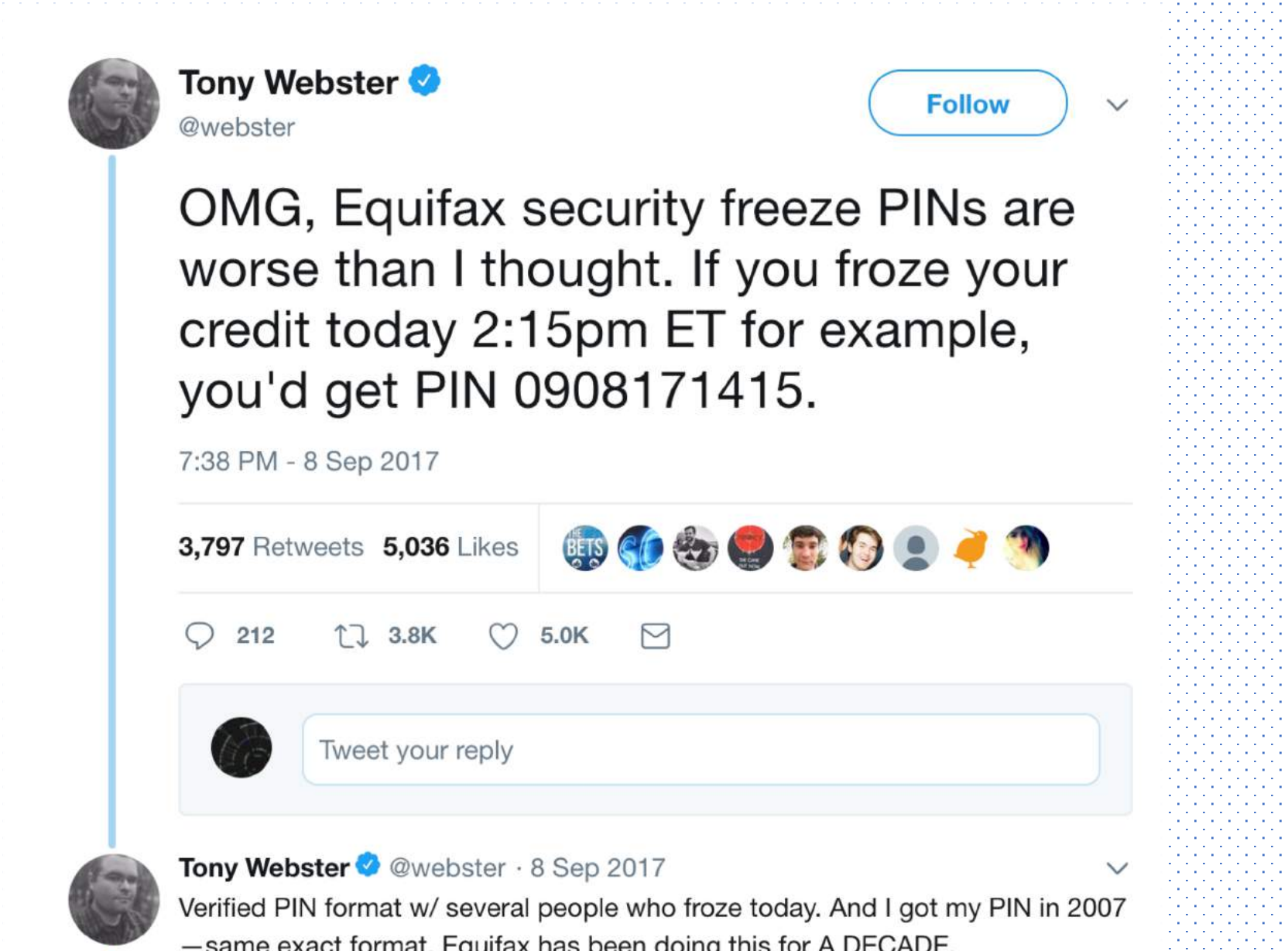
Cross-site Scripting (XSS) Negligence at Equifax



In addition, apparently no Intrusion Detection Systems

https://www.netsparker.com/blog/web-security/how-equifax-data-breach-hack-happened/

Equifax's old freeze PIN is the timestamp -- predictable



Tony Webster
@webster

Follow

OMG, Equifax security freeze PINs are worse than I thought. If you froze your credit today 2:15pm ET for example, you'd get PIN 0908171415.

7:38 PM - 8 Sep 2017

3,797 Retweets **5,036** Likes

212 3.8K 5.0K

Tweet your reply

Tony Webster @webster · 8 Sep 2017

Verified PIN format w/ several people who froze today. And I got my PIN in 2007 —same exact format. Equifax has been doing this for A DECADE.

“admin/admin” login for Equifax Argentina employee portal

Id	Apellido	Nombre	Usuario	documento	Email	Estado	Perfil		
1859471	A	Marcela	m		ma ar	INACTIVO	USUARIO	Eliminar	Editar
1859475	A	Yeimy	ya		ye	INACTIVO	USUARIO	Eliminar	Editar
1271524	A	Maria Belen	ba		ma om.ar	INACTIVO	USUARIO	Eliminar	Editar
274804	A	Martin	m		ma	INACTIVO	USUARIO	Eliminar	Editar
527	A	Marita	m		me	INACTIVO	ADMINISTRADOR	Eliminar	Editar
1358701	A	Eugenia	ea		Eu .ar	INACTIVO	USUARIO	Eliminar	Editar
1859467	A	Alejandra	aa		ale .ar	INACTIVO	USUARIO	Eliminar	Editar
1572254	A	Mariela	m		ma	ACTIVO	USUARIO	Eliminar	Editar
2025633	A	Carlos	ca		ca	INACTIVO	USUARIO	Eliminar	Editar
2025667	A	Carlos	ca		ca ar	INACTIVO	USUARIO	Eliminar	Editar
2025660	A	Jose Pablo	jp		Jo	INACTIVO	USUARIO	Eliminar	Editar
709	B n	Marcelo	m		mi	ACTIVO	USUARIO	Eliminar	Editar
1572338	B	Gaston	gb		ga n.ar	INACTIVO	USUARIO	Eliminar	Editar
1789253	B	Priscila	pb	x	pis .ar	INACTIVO	USUARIO	Eliminar	Editar
1536812	B	Martin	m		ma	INACTIVO	USUARIO	Eliminar	Editar
711	B e	Oscar	ob		ob	ACTIVO	USUARIO	Eliminar	Editar
334837	C	Alejandra	ac		ale om.ar	INACTIVO	USUARIO	Eliminar	Editar
123392	C	Guillermo	gc		gu n.ar	INACTIVO	USUARIO	Eliminar	Editar
1433356	D	Laura	ld		lau	INACTIVO	USUARIO	Eliminar	Editar
1702095	D	Eliana	ec		eli r	INACTIVO	USUARIO	Eliminar	Editar

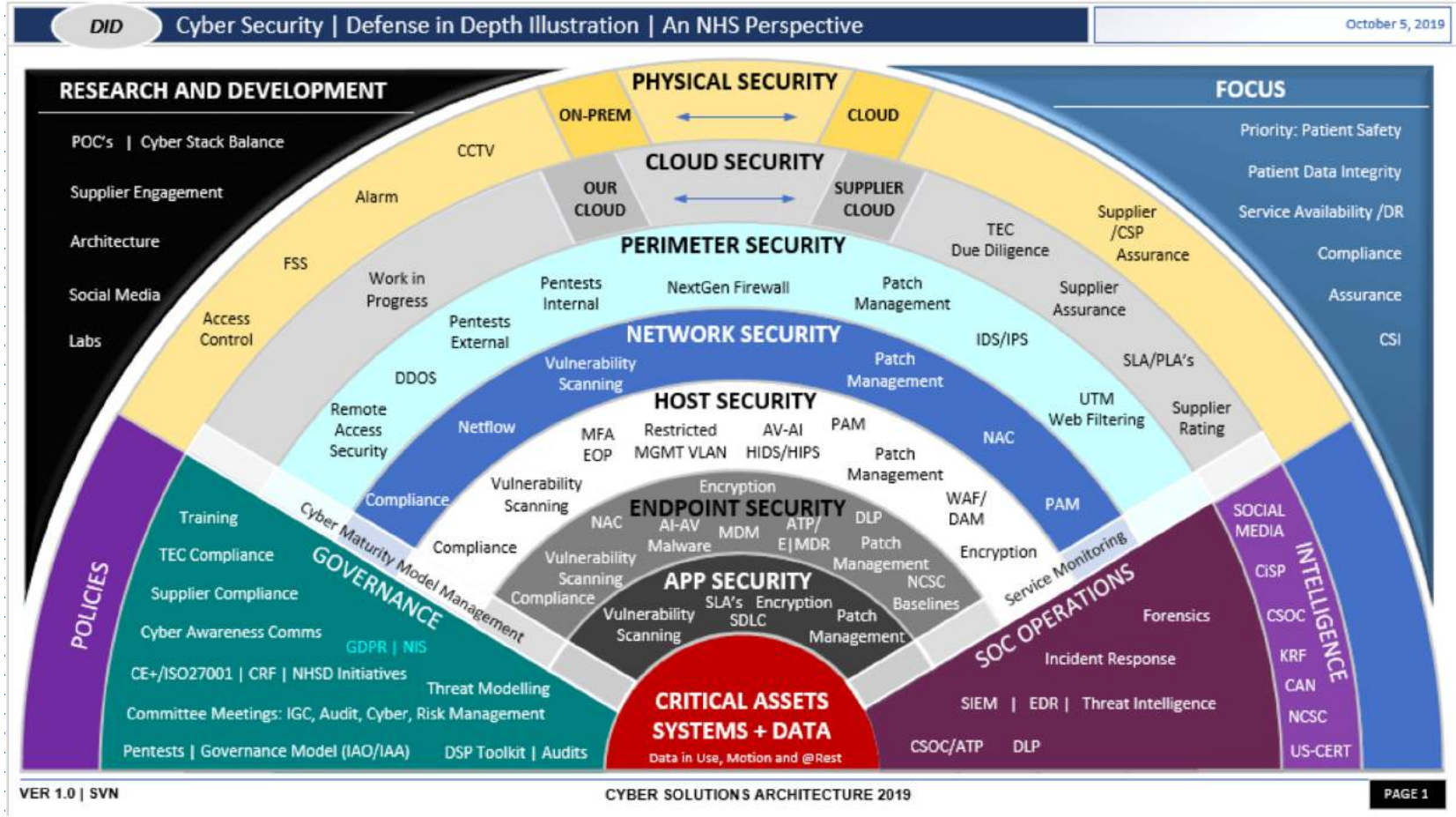
VIRGINIA TECH

Did Equifax practice defense in depth?

☐ NO ☐ YES

VIRGINIA TECH

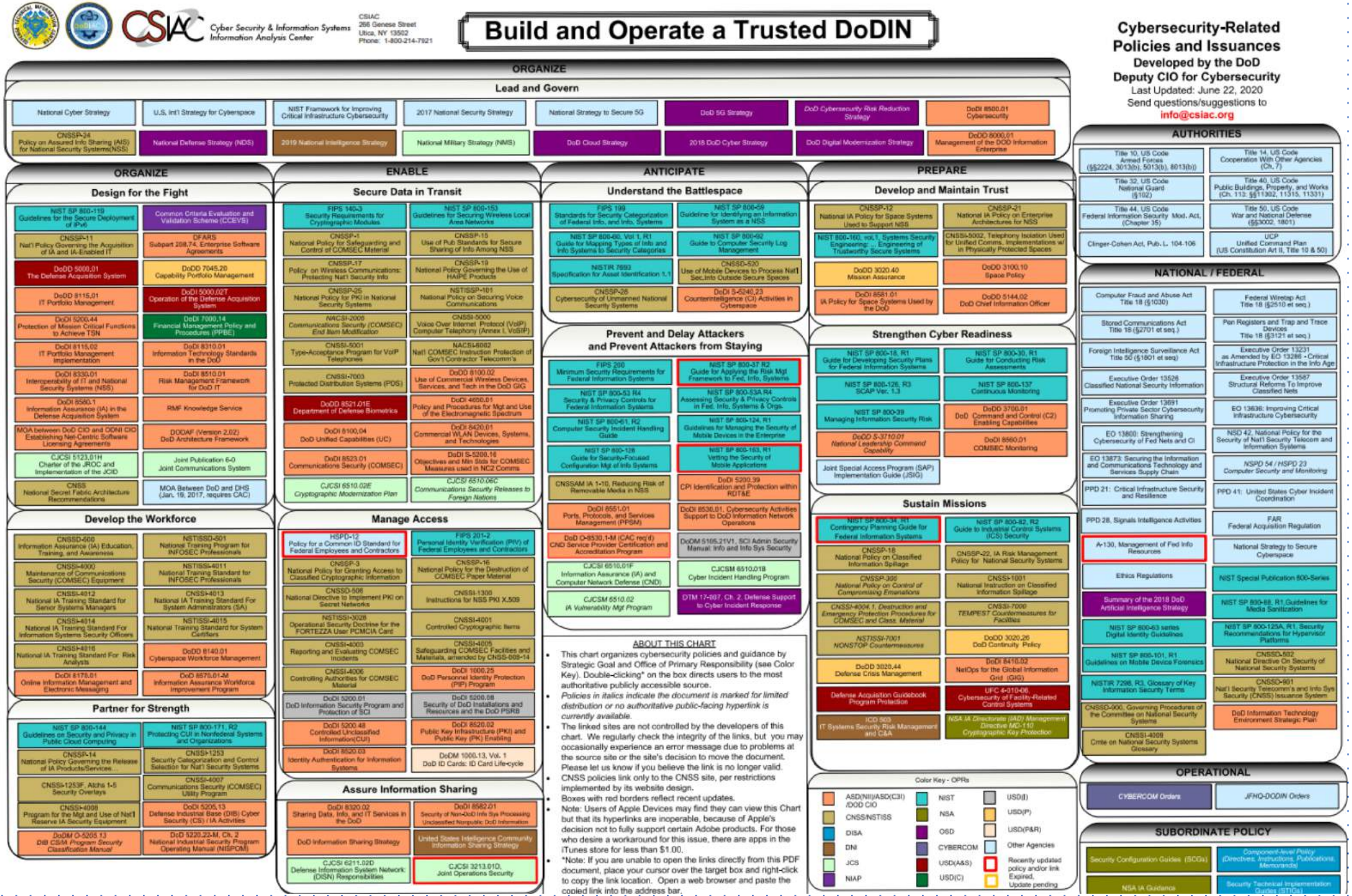
Can one **quantify** how well defense-in-depth is done? More measurement, metrics, benchmarks are needed



https://www.peerlyst.com/posts/nhs-healthcare-defense-in-depth-shaun-van-niekerk

VIRGINIA TECH

US Government regulations on cybersecurity



https://www.csiac.org/wp-content/uploads/2020/06/ia-policychart-22-June-20-DoDIN.pdf

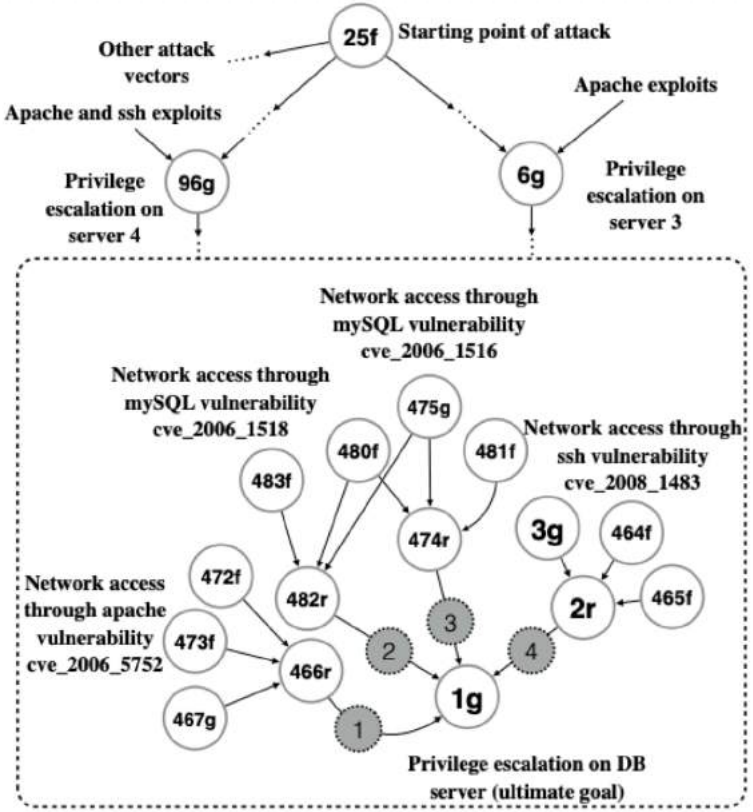
VIRGINIA TECH

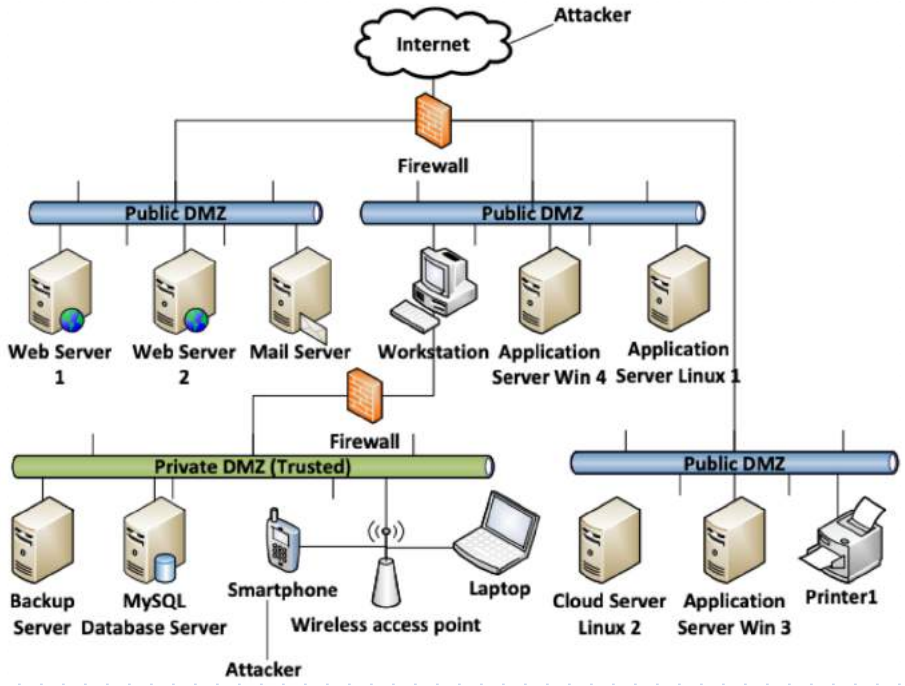
What can researchers do?

Evidence-based quantitative risk assessment

Need evidence-based quantitative risk assessment for CPS

My old (2016) attack graph quantifying risks got so many rejections☹





Vulnerability fact node u_i	$E[X_{u_i}]$
CVE_2006_1516	5.0
CVE_2006_1518	6.5
CVE_2008_1483	6.9
CVE_2006_5752	4.3
CVE_2011_1929	5.0
CVE_2011_1968	7.1
CVE_2004_0331	5.0
CVE_2009_4565	7.5
CVE_2005_2090	4.3
CVE_2010_1899	4.3

[IEEE TDSC 2016] http://yaogroup.cs.vt.edu/publication.html

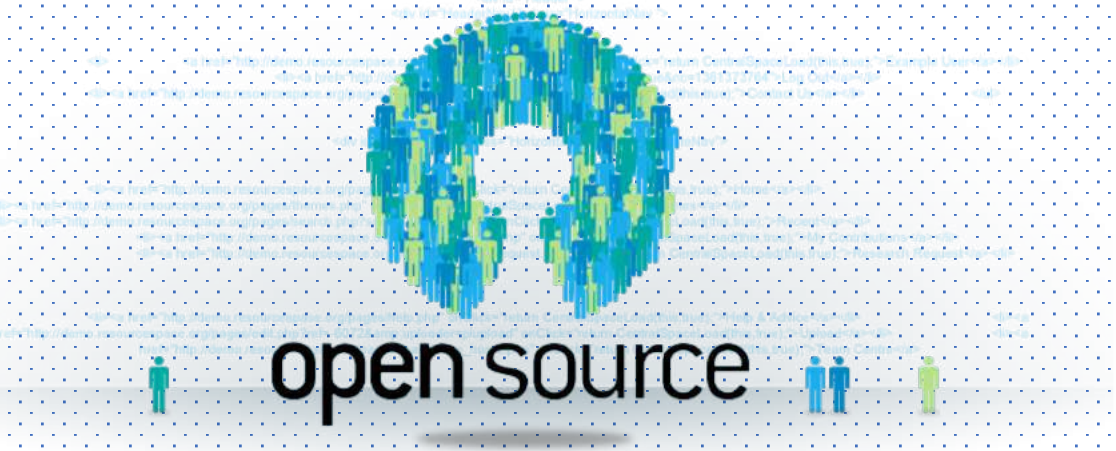
VIRGINIA TECH

This year's IEEE CNS best paper award

SCIBORG: Secure Configurations for the IOT Based on Optimization and Reasoning on Graphs

Hamed Soroush (PARC, USA); Massimiliano Albanese (George Mason University, USA); Milad Asgari Mehrabadi (University of California, Irvine, USA); Ibifubara Iganibo (George Mason University, USA); Marc Mosko (Palo Alto Research Center, USA); Jason Gao and David Fritz (Sandia National Laboratories, USA); Shantanu Rane and Eric Bier (Palo Alto Research Center, USA)

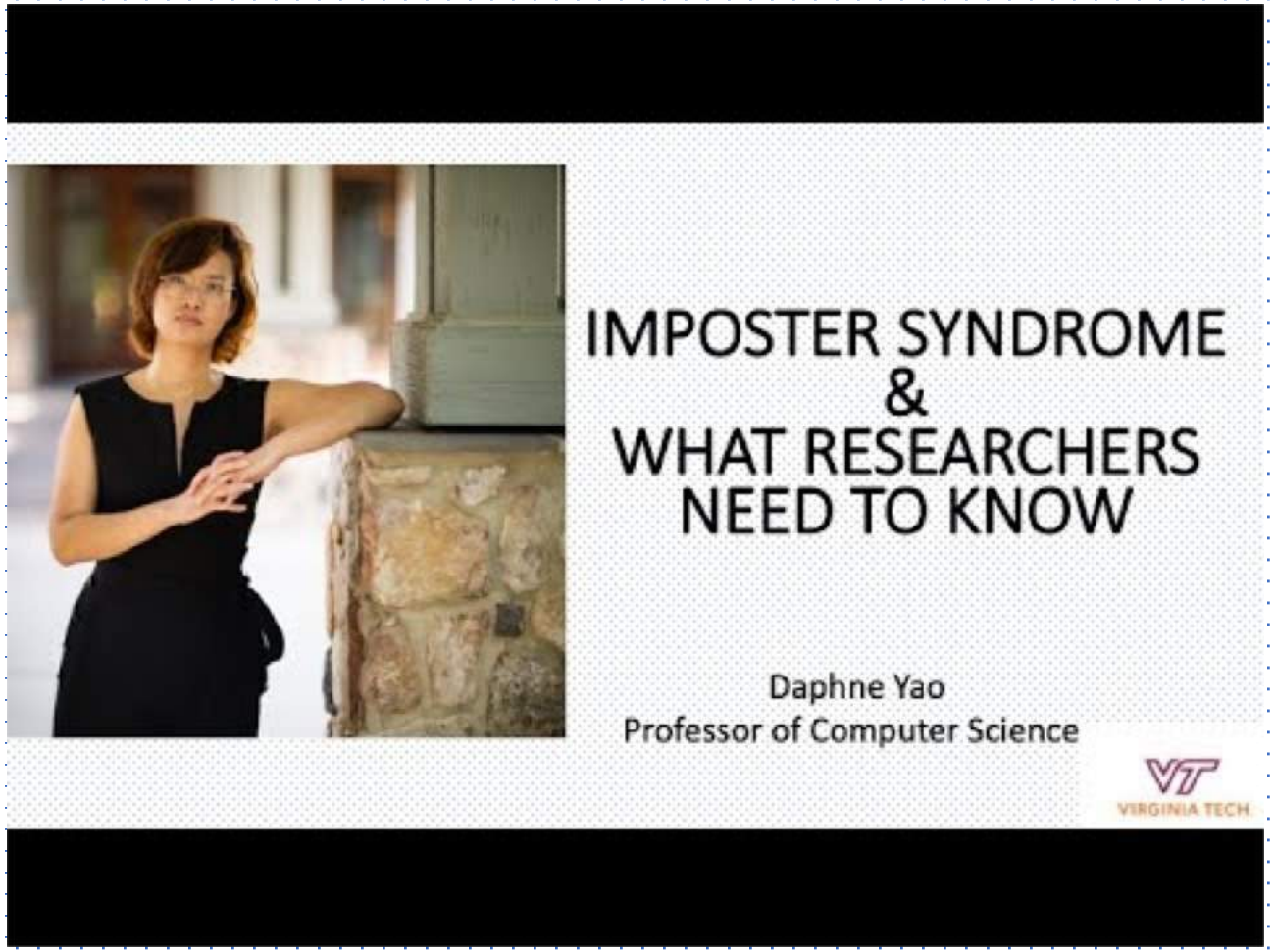
Researchers Have a Unique Position -- Bringing in Transparency and Science



Testbeds, Benchmarks, Measurement, Open Source Tools, Deployment

Need community's support for research on deployable security

Check out my YouTube talk on impostor syndrome and research



https://youtu.be/JqFKv9Rg0k8 or
just search for my name on YouTube

Slides available on my website
http://people.cs.vt.edu/danfeng/