



VirginiaTech
Invent the Future

Human-Centric Security

YAO GROUP

@ CS.VT

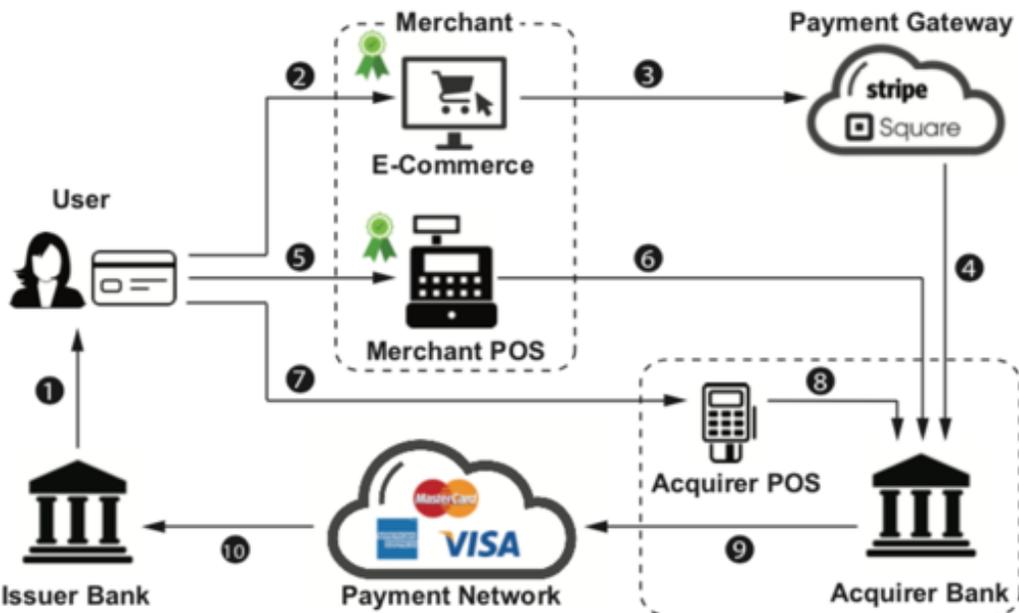


Deployable and Measurable Security in Software and Systems

姚丹凤 (Daphne Yao)

Department of Computer Science
Virginia Tech

Testbeds, Benchmarks, Measurement, Open Source Tools, Deployment



Web Security and Payment

Make secure coding more effective



Fallthrough Map:
 3725c -> 1324a
 1324b -> 23e35
 23e36 -> 82d27
 82d28 -> 49ea3
 49ea4 -> 598aa

Address	Memory Space
...	...
1324a	mov rsi, r14
...	...
1c9bc	jne 3725b
...	...
23e35	call [r12+rbx*8]
...	...
3725b	mov rdx, r13
...	...
49ea3	cmp rbp, rbx
...	...
598aa	ret
a	...
7cb20	add rsp, 0x8
...	...
82d27	add rbx, 0x1

Address space layout randomization under JIT-ROP attacks

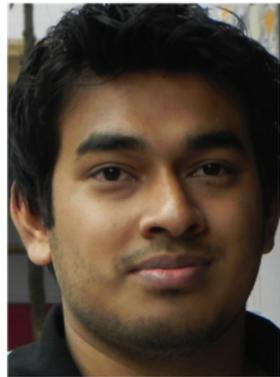


SIGSAC is planning a women's networking dinner event at ACM CCS '19



Women in Cybersecurity (CyberW) Workshop, Dallas, TX

Acknowledgements to Yao Group Members



Sazzadur Rahaman



Ya Xiao



Sharmin Afrose



Xiaodong Yu



Salman Ahmed



Miles Frantz



Yuan Luo
(visiting student)

Acknowledgements to Yao Group's Recent Collaborators



Elisa Bertino
(Purdue U)



Raheem Beyah
(GaTech)



Bart Miller
(UW-Madison)



Xu Liu
(Williams & Mary)



N. Asokan
Aalto U (Finland)



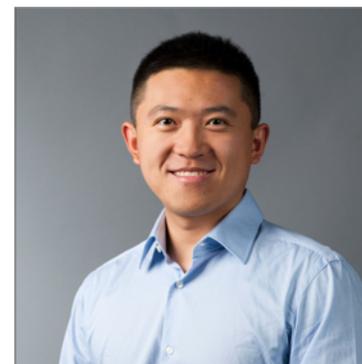
Na Meng (VT)



Trent Jaeger (PSU)



Gang Tan (PSU)



Gang Wang (VT)



Fabian Monrose
(UNC-Chapel Hill)

Software is everywhere

Ford GT has over 10 million lines of code

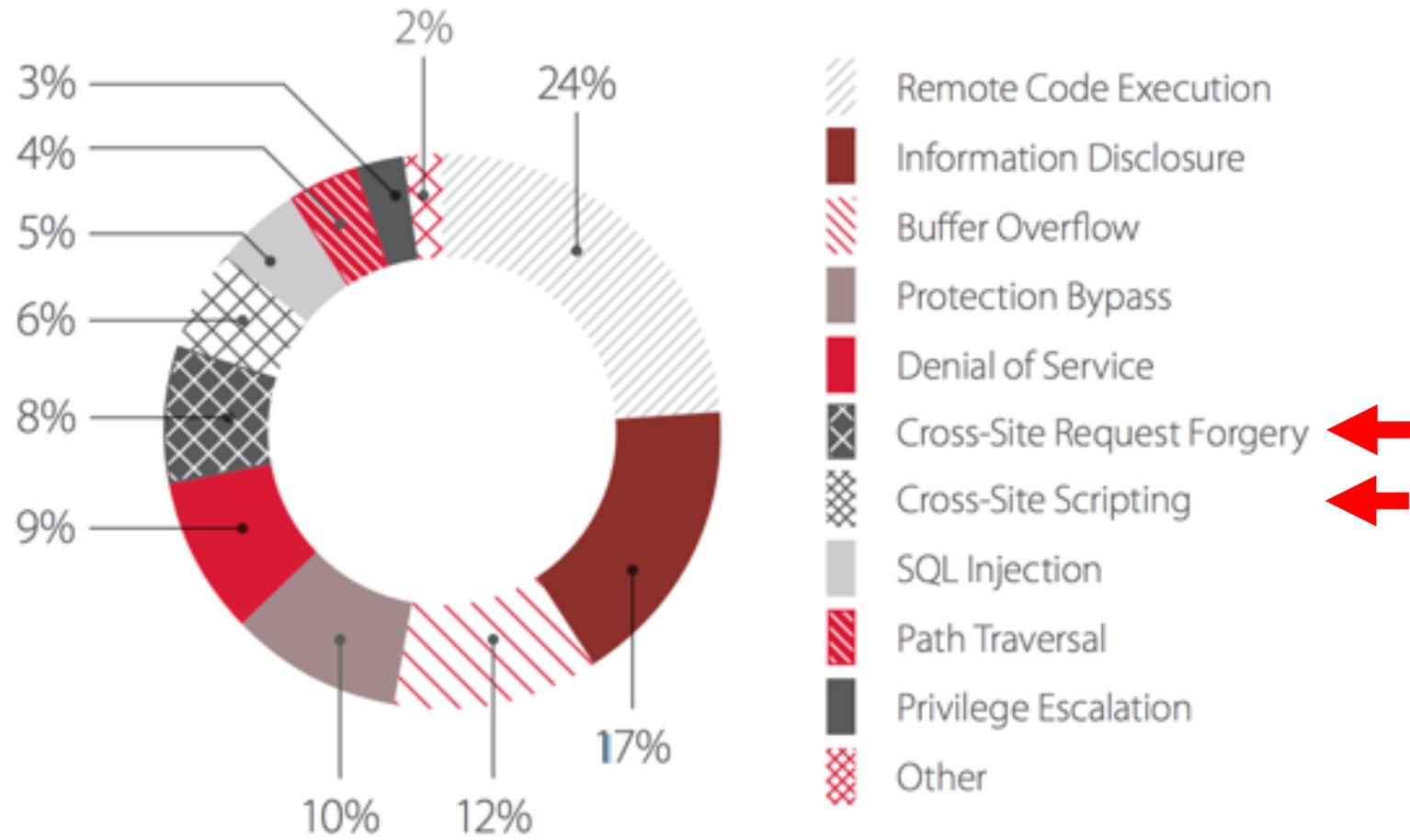
F-22 Raptor has 2 million lines of code

Boeing 787 Dreamliner has 7 million lines of code

Ford pickup truck F-150 has 150 million lines of code



Security of Critical Infrastructure & Cyber-physical systems (CPS)



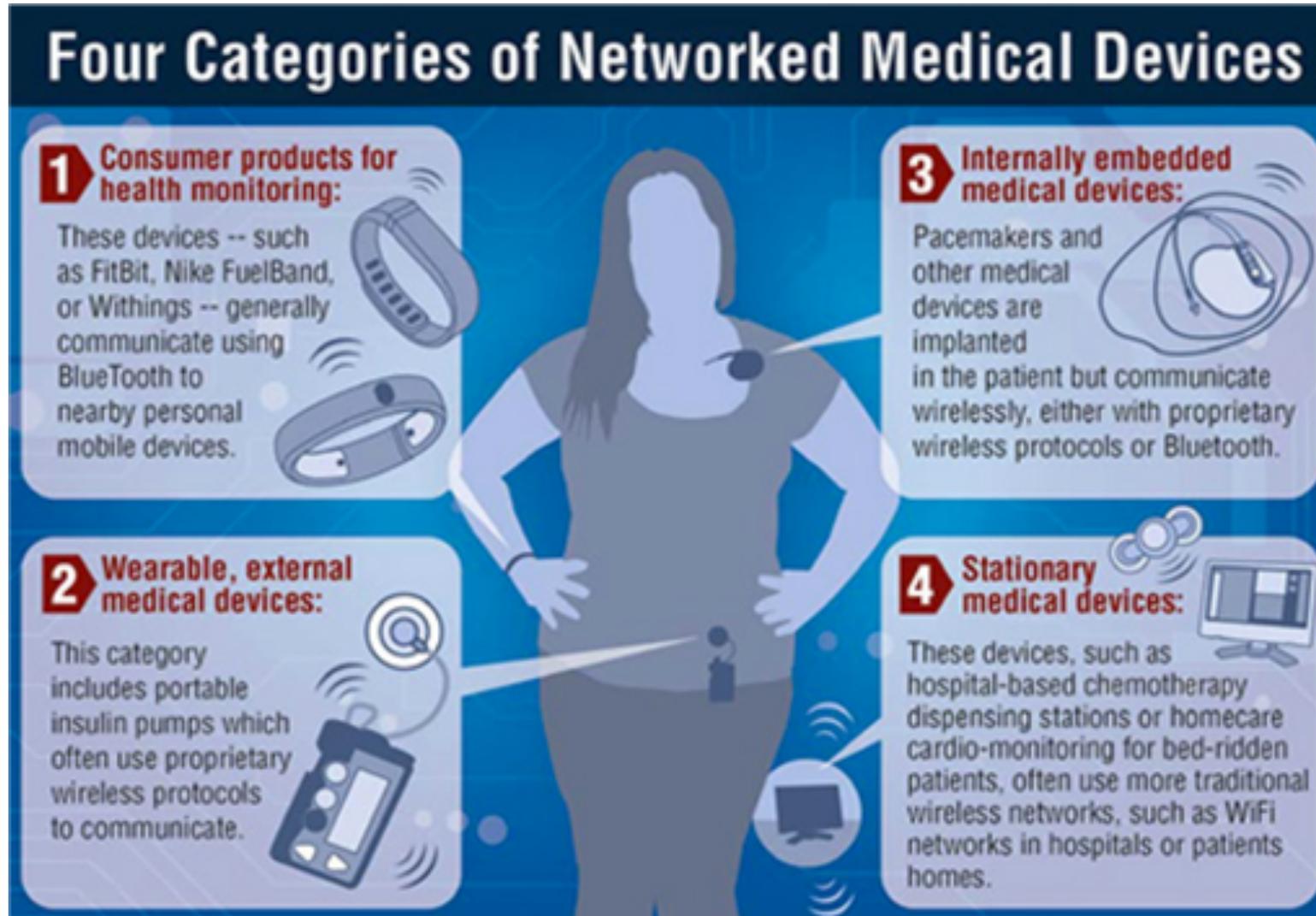
Industrial control systems (ICS)

Types of vulnerabilities in ICS components

<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-Security-2017-eng.pdf>

<https://www.infosecurity-magazine.com/news/critical-infrastructure-more/>

Code gets closer and closer to your body



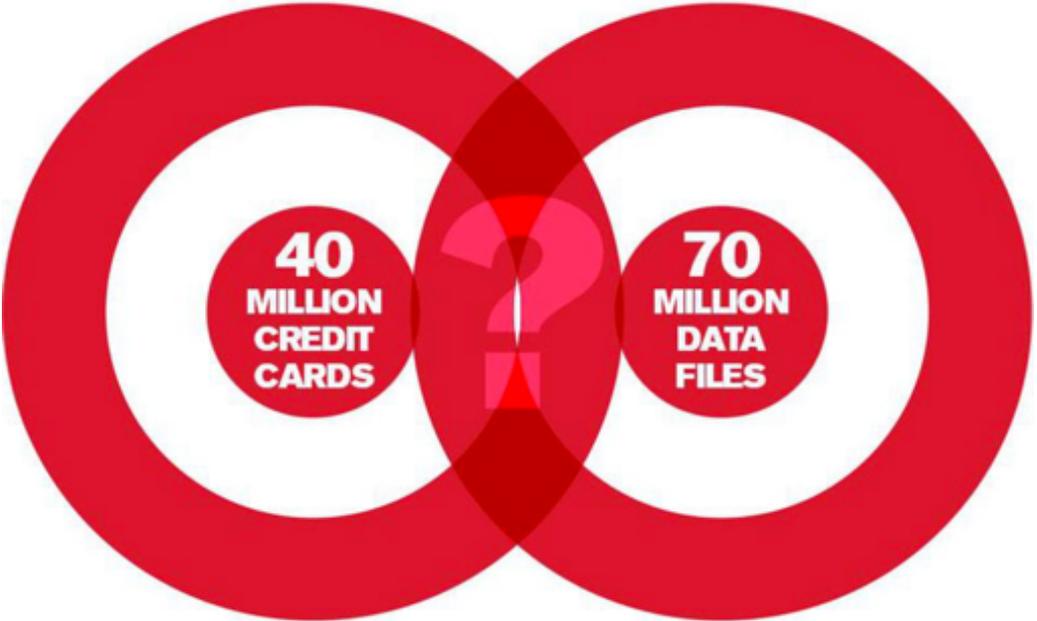
Data Breach at the Retail Giant Target



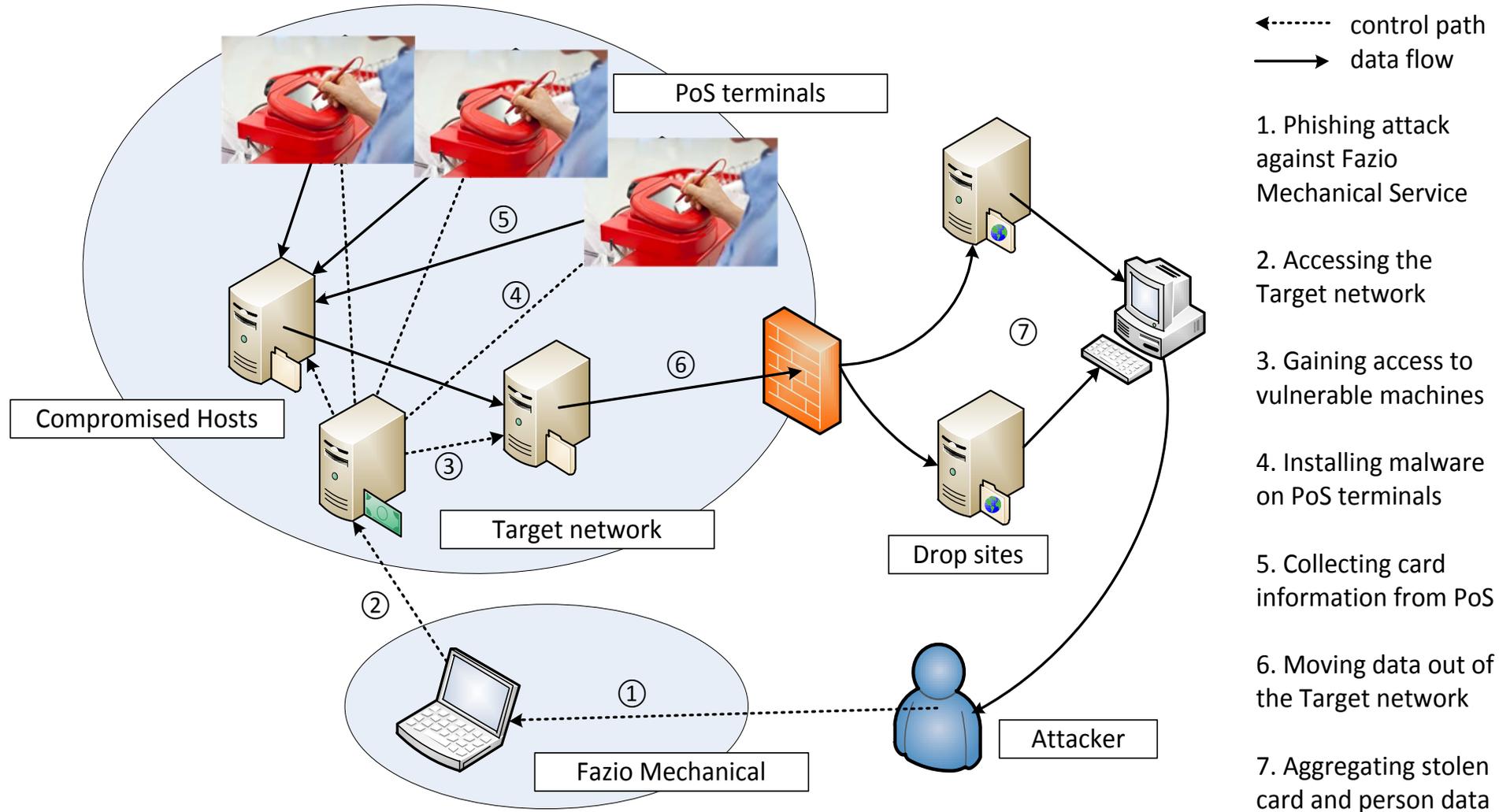
NBC NEWS
BUSINESS NEWS

Target Settles 2013 Hacked Customer Data Breach For \$18.5 Million

by Reuters / May.24.2017 / 10:49 AM ET / Source: Reuters

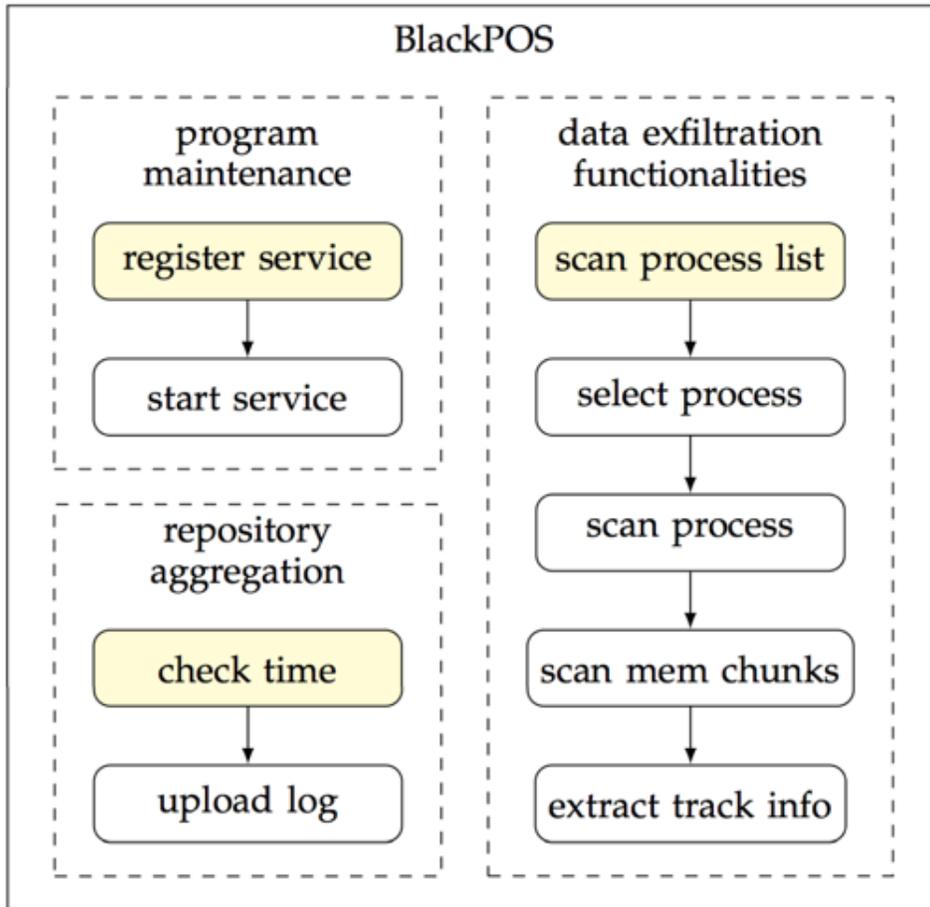


Target Data Breach (Duration from Nov. 27 to Dec. 15, 2013)



BlackPOS (Memory Scraper Malware)

- Runs as a Windows service “POSWDS”
- Scans a list of processes that interact with the card reader
- Uploads credit cards to a compromised server (internal network repository)



How can a HVAC vendor's credential access Target's internal networks?

A Theory About How Hackers Reached Target from Fazio

2. Web server attempted to open it; code got executed

1. Php scripts uploaded as invoices to Target's billing portals





FireEye's Intrusion Detection System (IDS)



Target's security team in Bangalore received FireEye alerts; sent alerts to Target headquarters

FireEye's auto-malware-delete function was turned off

"Target was certified as meeting the standard for the payment card industry (PCI) in Sept. 2013."

-- Gregg Steinhafel (Target then CEO, stepped down in 2014)



Payment Card Industry Security Standard Council Manages All Systems That Touch Payment Cards



Uniquely Yours

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

Section 1 - Company Contact Information	
Date	
Company Legal Name	
Compliance Contact Name	
Compliance Contact Phone Number	(XXX)XXX-XXXX
Compliance Contact E-mail Address	

Section 2 - Company's PCI Compliance Status	
(Name/Title of Officer) certifies the following compliance status (select one):	
<input type="checkbox"/> COMPLIANT	(Company) has achieved full compliance with the PCI DSS as of (date of compliance). Name of Qualified Security Assessor (if applicable): Proceed to Section 4.
<input type="checkbox"/> NON-COMPLIANT	(Company) has not achieved full compliance with the PCI DSS as of (date). Company plans to achieve full compliance on: (date). Company is required to complete Section 3.

Section 3 - Summary of Company's Compliance with PCI DSS Requirements				
Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement.				
PCI Req.	Description of Requirement	Compliance Status (select one)		Remediation Date and Actions (if "Non-Compliant" was selected in the "Compliance Status" column)
		Compliant	Non-Compliant	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Use and regularly update anti-virus software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by cryptographic controls and to-know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	

Protect stored cardholder data

Regularly test security systems and processes



Good News: Multi-factor Authentication -- A Lesson Learned from the Target Breach

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.

Bad News: Current Enforcement of Data Security Standards is Weak

COMPANY	PLACE OF BUSINESS	PRODUCT NAME	EMAIL CONTACT	LOCATIONS SERVED	CERTIFICATION NUMBER
AccessIT Group, Inc **In Remediation**	United States	AccessIT Group ASV	Peterm@...		5086-01-01
Alert Logic, Inc.	United States		...@alertlogic.com	North America, Europe, Japan	4222-01-12
Aperia	United States	Aperia Pro Scan	jnix@aperiasolutions.com	Global	5051-01-07
AppSec Consulting	United States	AppSec Certified	info@appsecconsulting.com	North America	3834-01-12
AT&T Consulting Solutions	United States	AT&T	pci@att.com	Global	5024-

But security guarantees are often vague

PCI merchant levels

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
<p>6M +</p> <p>Process more than 6 million Visa transactions per year, regardless of channel.</p> <p>Be identified as Level 1 by any card association.</p>	<p>1-6M</p> <p>Process 1 to 6 million credit card transactions annually across all channels.</p>	<p>20K-1M</p> <p>Process 20,000 to 1 million e-commerce credit card transactions annually.</p>	<p><20K</p> <p>Process fewer than 20,000 e-commerce transactions annually, or process fewer than 1 million credit card transactions annually across all channels.</p>
SECURITY REQUIREMENTS			
<p>Complete a ROC annually by a Qualified Security Assessor (QSA) *. This means an on-site audit needs to occur every year.</p>	<p>Conduct an annual Self-Assessment Questionnaire (SAQ) *.</p>	<p>Conduct an annual Self-Assessment Questionnaire (SAQ) *.</p>	<p>Conduct an annual Self-Assessment Questionnaire (SAQ) *.</p>
<p>Quarterly scans by an Approved Scanning Vendor (ASV) *.</p>	<p>Quarterly scans by an Approved Scanning Vendor (ASV).</p>	<p>Quarterly scans by an Approved Scanning Vendor (ASV).</p>	<p>Quarterly scans by an Approved Scanning Vendor (ASV).</p>
<p>An AOC that verifies everything meets PCI standards.</p>	<p>An AOC that verifies everything meets PCI standards.</p>	<p>An AOC that verifies everything meets PCI standards.</p>	<p>An AOC that verifies everything meets PCI standards.</p>

Can We Measure the Strength of PCI Enforcement?



Our BuggyCart Testbed embeds 35 vulnerabilities (will open source very soon)

Network security (14 test cases)

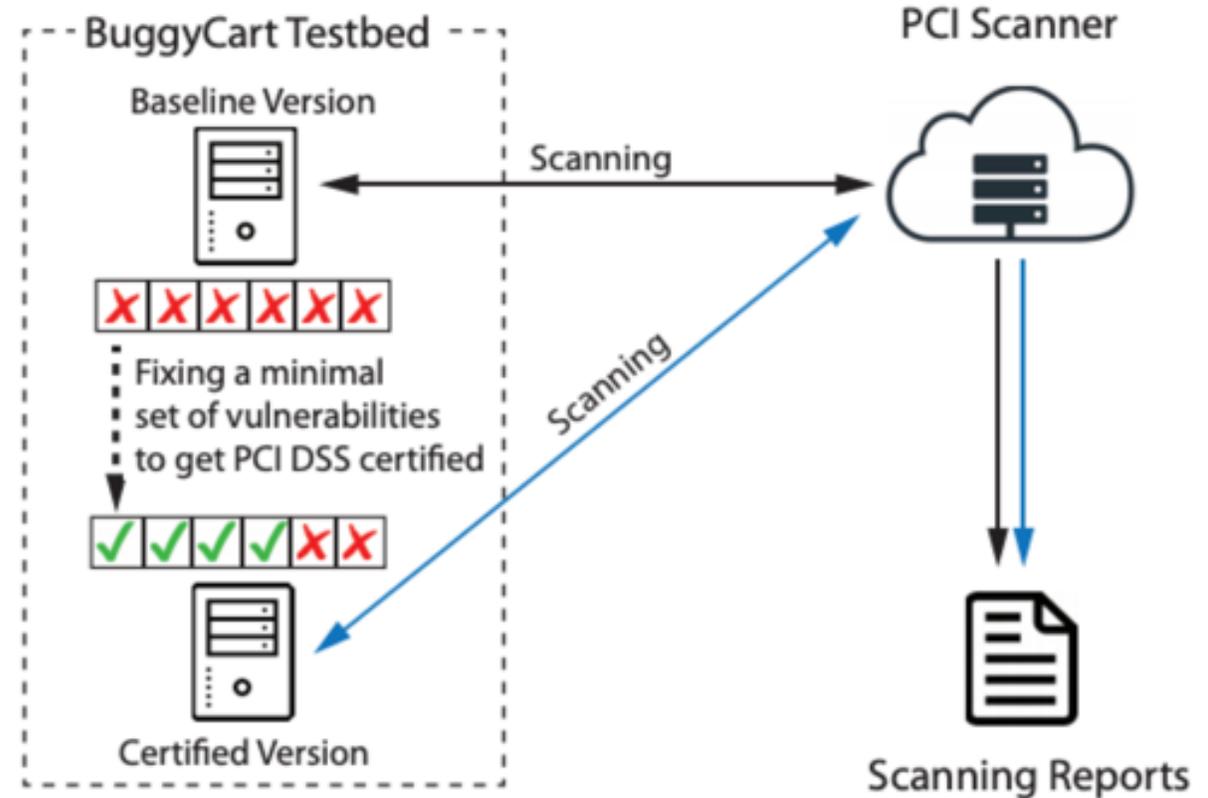
System security (7 test cases)

Web Application security (8 test cases)

Secure storage (6 test cases) – cannot be detected by external scans

Our BuggyCart Testbed and Commercial PCI Scanners Selected

PCI Scanners	Price	Spent Amount
Scanner 1	\$2,995/Year	\$0 (Trial)
Scanner 2	\$2,190/Year	\$0 (Trial)
Scanner 3	\$67/Month	\$335
Scanner 4	\$495/Year	\$495
Scanner 5	\$250/Year	\$250
Scanner 6	\$59/Quarter	\$118
Scanner 7	Unknown	N/A
Scanner 8	\$350/Year	N/A
Total	-	\$1198



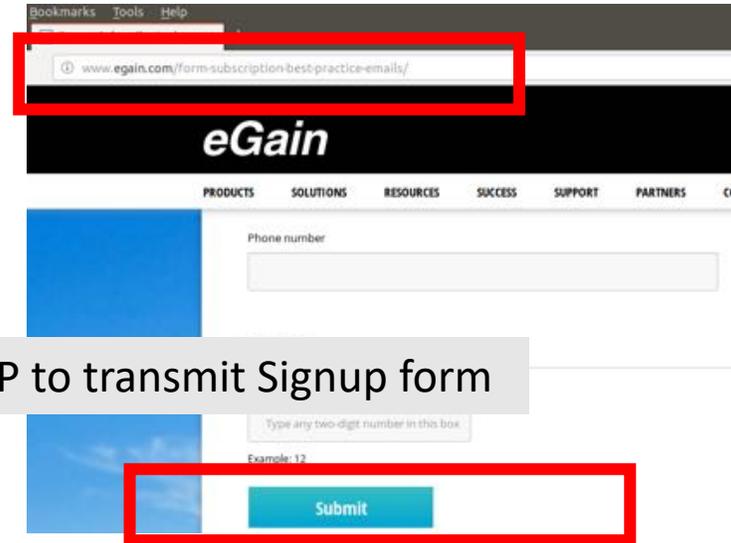
Worrisome PCI scanners security – Summary of Testbed Results

	Scanner 1	Scanner 2	Scanner 3	Scanner 4	Scanner 5
Baseline: #Vul. Detected (29 Total*)	21	16	17	16	7
Certified: #Vul. Remaining	7	15	18	20	25
#Vul. detected, but no need to fix	0	3	7	7	4

*All 29 vulnerabilities violate the PCI's data security specifications and are required by the specifications to be removed.

Assess e-commerce sites with our PCICheckerLite tool

E-commerce Websites		#Vul. Websites	
		At least 1	At least 2
Category (810)	Business (122)	113	81
	Shopping (163)	143	99
	Arts (78)	76	54
	Adults (65)	65	43
	Recreation (84)	75	58
	Computer (57)	56	44
	Games (42)	42	31
	Health (60)	55	41
	Home (102)	93	65
	Kids & Teens (37)	36	21
Ranking (393)	Top (288)	277	203
	Bottom (105)	104	87
Total (1,203)		1,135 (94%)	827 (69%)



Using HTTP to transmit Signup form



Wrong hostname

www.prodapt.com uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
 The certificate is only valid for .
 The certificate expired on February 13, 2018, 5:48:33 AM GMT-5. The current time is March 21, 2019, 9:12 PM.

Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

Self-signed certificate

Summary of Measurement Findings on the Payment Card Industry

5 out of 6 PCI scanners are not compliant with ASV scanning guidelines
– certifying merchants that still have major vulnerabilities

Is the concept of for-profit security certification an oxymoron?

94% payment-card-taking websites (out of 1,203) evaluated, that're supposed to be PCI compliant, are not

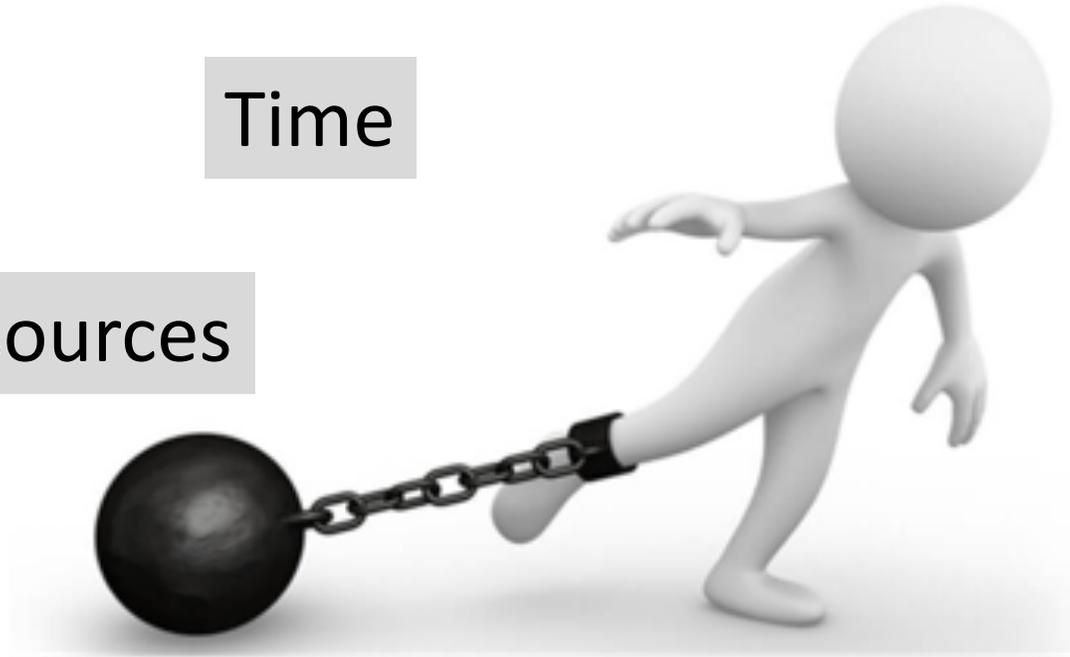
Specifications are comprehensive, enforcement is tough

Who Wouldn't Want to Write Secure Code?

Budget

Time

Resources



Why Care About Deployment and Secure Coding Practices? [ICSE '18]

“Adding `csrf().disable()` solved the issue!!! I have no idea why it was enabled by default”

“adding `-Dtrust_all_cert=true` to VM arguments”

“I want my client to accept any certificate (because I'm only ever pointing to one server)”

```
1 // Create a trust manager that does not validate certificate chains
TrustManager[] trustAllCerts = new TrustManager[] {
    new X509TrustManager() {
        public java.security.cert.X509Certificate[]
            getAcceptedIssuers() {return null;}
        public void checkClientTrusted(...) {}
        public void checkServerTrusted(...) {}
    }
};
// Install the all-trusting trust manager
try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new java.security.
        SecureRandom());
11    HttpsURLConnection.setDefaultSSLSocketFactory(sc
        .getSocketFactory());
12 } catch (Exception e) {}
```

Our work examined 497 Java and security related StackOverflow Posts

How Much Influence Does StackOverflow Have?

Insecure Posts	Total Views	No. of Posts	Min Views	Max Views	Average
Disabling CSRF Protection*	39,863	5	261	28,183	7,258
Trust All Certs	491,567	9	95	391,464	58,594
Obsolete Hash	91,492	3	1,897	86,070	30,497
Total Views	622,922	17	-	-	-

* In Java Spring Security for web applications

StackOverflow posts that make insecure suggestions have a large influence on developers.

Cyberbullying on Stackoverflow

User: skanga
[0]

“Do NOT EVER trust all certificates. That is very dangerous.”

“the "accepted answer" is wrong and INDEED it is DANGEROUS. Others who blindly copy that code should know this.”

User: MarsAtomic
[6,287]

“once you have sufficient reputation you will be able to comment”

“If you don't have enough rep to comment, ... then participate ... until you have enough rep.”

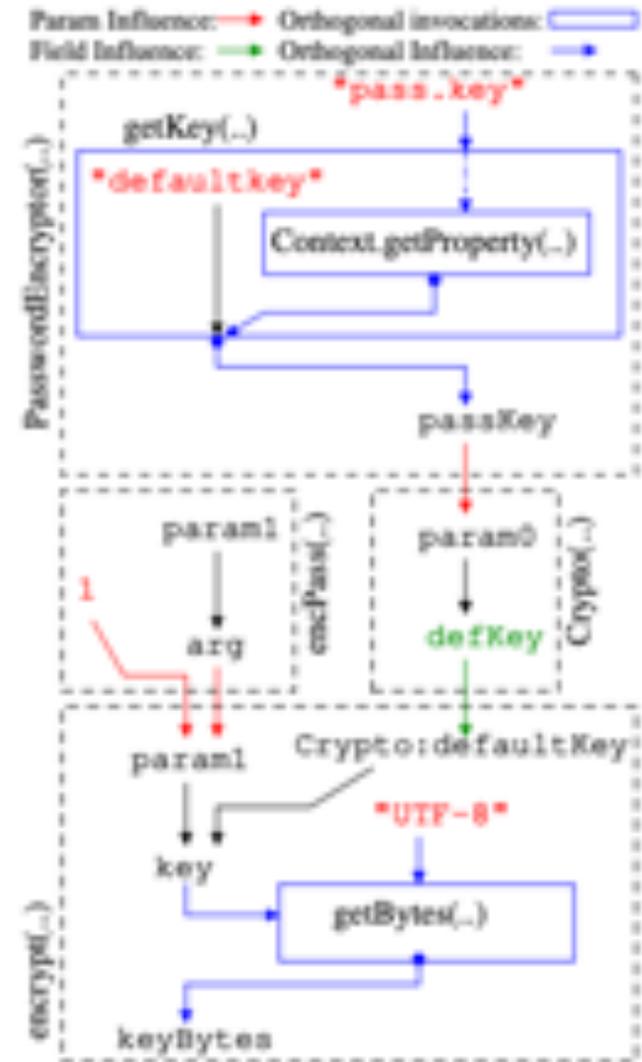
How well are crypto implementations written?

Can one measure it?

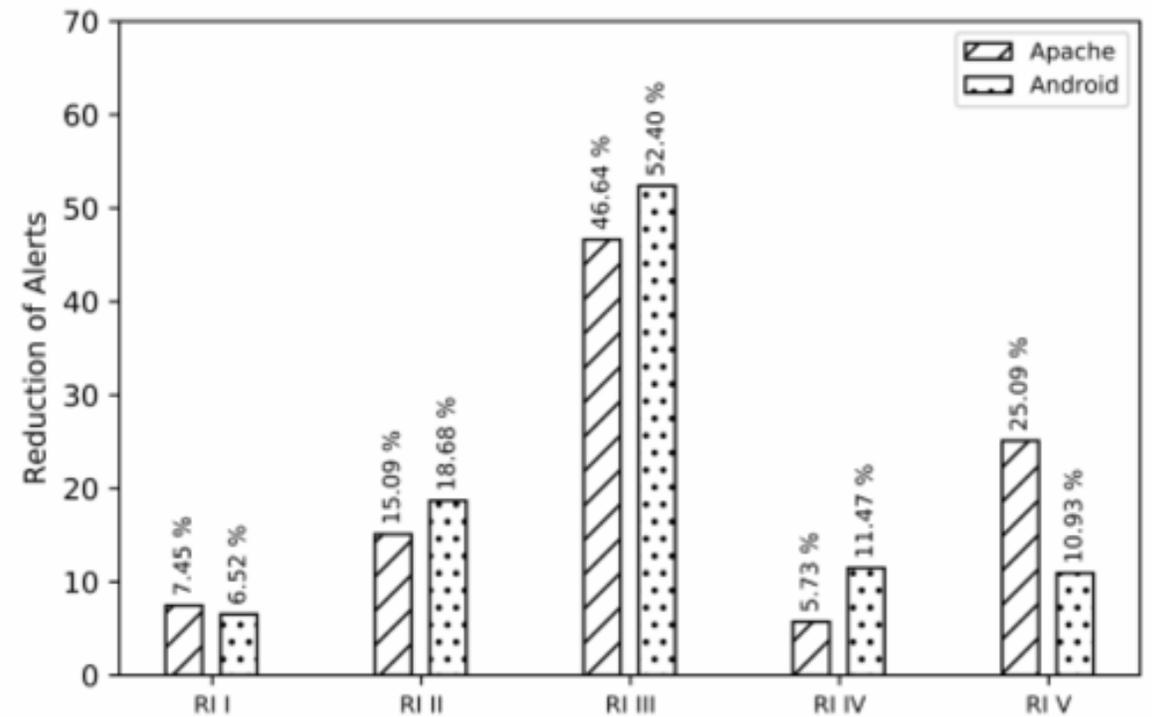
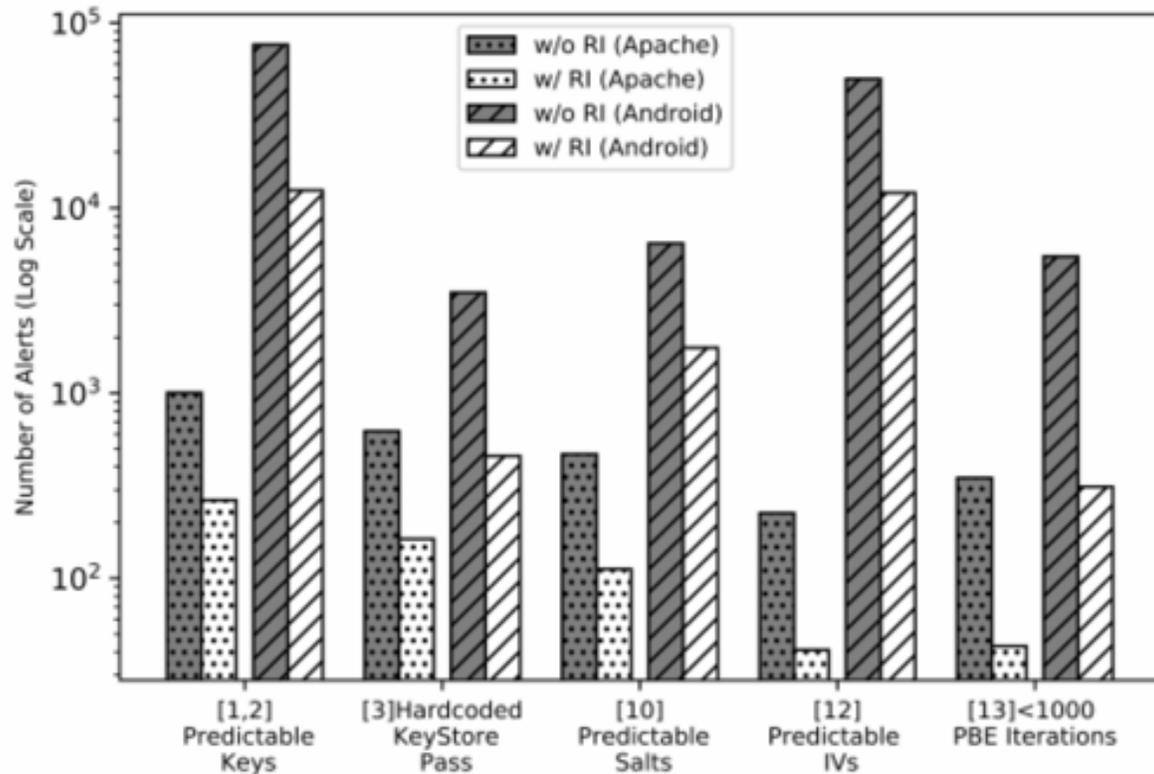
Crypto Code in Java Can Be Complex to Analyze

```
1 class PasswordEncryptor {
2
3   Crypto crypto;
4
5   public PasswordEncryptor() {
6     String passKey = PasswordEncryptor
7       .getKey("pass.key");
8
9     crypto = new Crypto(passKey);
10  }
11
12  byte[] encPass(String [] arg) {
13    return crypto.encrypt(arg[0], arg[1]);
14  }
15
16  static String getKey(String src) {
17    String key = Context.getProperty(src);
18    if (key == null) {
19      key = "defaultkey";
20    }
21    return key;
22  }
```

```
22 class Crypto {
23
24   String ALGO = "AES";
25   String ALGO_SPEC = "AES/CBC/NoPadding";
26   String defaultKey;
27   Cipher cipher;
28
29   public Crypto(String defKey) {
30     cipher = Cipher.getInstance(ALGO_SPEC);
31     defaultKey = defKey; // assigning field
32   }
33
34   byte[] encrypt(String txt, String key) {
35     if (key == null) {
36       key = defaultKey;
37     }
38     byte[] keyBytes = key.getBytes("UTF-8");
39     byte[] txtBytes = txt.getBytes();
40     SecretKeySpec keySpec =
41       new SecretKeySpec(keyBytes, ALGO);
42     cipher.init(Cipher.ENCRYPT_MODE, keySpec);
43     return cipher.doFinal(txtBytes);
44   }
```



Reduction of False Alerts by Our Refinements -- Off-the-shelf Program Slicing Would Fail



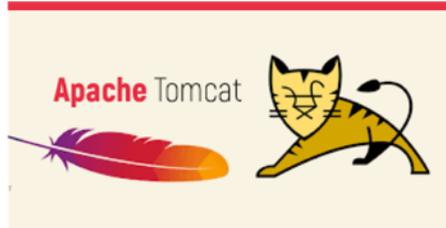
Reduction of false positives with refinement insights in 46 Apache projects (94 root-subprojects) and 6,181 Android apps.

Breakdown of the reduction of false positives due to five of our refinement insights.

Deployment-quality – CryptoGuard handles complex code



Apache Ranger



Maximum, minimum and average LoC: 2,571K (Hadoop), 1.1K (Commons Crypto), and 402K, respectively

CryptoGuard Has the Deployment-grade Accuracy

Rules	Total Alerts	# True Positives	Precision
(1,2) Predictable Keys	264	248	94.14 %
(3) Hardcoded Store Pass	148	148	100 %
(4) Dummy Hostname Verifier	12	12	100 %
(5) Dummy Cert. Validation	30	30	100 %
(6) Used Improper Socket	4	4	100 %
(7) Used HTTP	222	222	100 %
(8) Predictable Seeds	0	0	0%
(9) Untrusted PRNG	142	142	100 %
(10) Static Salts	112	112	100 %
(11) ECB mode for Symm. Crypto	41	41	100 %
(12) Static IV	41	40	97.56 %
(13) <1000 PBE iterations	43	42	97.67 %
(14) Broken Symm. Crypto Algorithm	86	86	100 %
(15) Insecure Asymm. Crypto	12	12	100 %
(16) Broken Hash	138	138	100 %
Total	1,295	1,277	98.61 %

Android App Libraries Have Issues

Package name	Violated rules
com.google.api	3, 4, 5, 7
com.umeng.analytics	7, 9, 12, 16
com.facebook.ads	5, 9, 16
org.apache.commons	5, 9, 16
com.tencent.open	2, 7, 9

96% of detected issues come from libraries

	Rules
2	Predictable pwds for PBE
3	Predictable pwds for keystores
4	Dummy hostname verifier
5	Dummy cert. verifier
7	Use of HTTP
9	Weak PRNG
12	Static IV
16	Broken hash

CryptoAPIBenchmark and Comparison with State-of-the-arts

Advanced Test Cases	True Positive Count	True Negative Count	SpotBugs			CRYPTOGUARD			CRYSL			Coverity		
			TP	FP	FN									
Two-Interprocedural	13	0	0	0	13	12	0	1	10	3	3	3	0	10
Three-Interprocecural	13	0	0	0	13	12	0	1	10	3	3	3	0	10
Field Sensitive	13	0	0	0	13	13	0	0	10	2	3	1	0	12
Combined Case	13	0	0	12	13	12	0	1	0	2	13	3	0	10
Path Sensitive	0	13	0	10	0	0	13	0	0	13	0	0	12	0
False Positive Cases	3	3	0	0	3	3	0	0	0	6	3	0	0	3
Multiple Class methods	13	0	0	0	13	13	0	0	10	3	3	3	0	10
Results		FPR (%)	57.89			44.83			66.67			42.86		
		FNR (%)	100			4.41			41.18			80.88		
		Recall (%)	0			95.59			58.82			19.12		
		Precision (%)	0.00			83.33			55.56			52.00		

Results as of April 8, '19

Benchmarks help motivate researchers to improve their tools; CrySL (from Bodden's group) has shown improved performance

Ongoing Work on Transitioning CryptoGuard to Practice

[Science of Security] Putting together a benchmark for evaluating detection accuracy



[Transition to Practice] Deployment in DHS Software Assurance Marketplace



[Engaging Industry/Government] Training, feedback and improvement

How well are fine-grained address space layout randomization (ASLR) solutions, under JIT-ROP attacks?

Can one measure it?

Measurement of Deep Learning for Software Security



Jump on the bandwagon

【中文】跟风、随波逐流、跟潮流、赶时髦

Harness the Deep Learning Revolution for Security; Ask Measurement Questions

[General purpose embeddings vs. task-specific embeddings]

[Security-relevant datasets]

[Security-relevant tasks, benchmarks]

[Evaluation methodology -- recipes]

[Security-specific interpretation of ML findings]

The Paparazzi



ITER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Java security plagued by crappy docs, complex APIs, bad advice

Boffins bash stale Stack Overflow fixes and lazy developers

By [Thomas Claburn](#) in [San Francisco](#) 29 Sep 2017 at 21:14 51  SHARE ▼

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



Testbeds, Benchmarks, Measurement,
Open Source Tools, Deployment

Deployable and Impactful Security Focus at ACSAC '19



Hard Topic Theme: Deployable and Impactful Security

- Needs to identify key deployment challenges, explain the deficiencies in state-of-the-art solutions, and experimentally demonstrate the effectiveness of the proposed approaches and (potential) impact to the real world.
- May involve prototyping, defining metrics, benchmark evaluation, and experimental comparison with state-of-the-art approaches in testbeds or real-world pilots, possibly with operational data.

CSET '19

12th USENIX Workshop on Cyber Security Experimentation and Test

AUGUST 12, 2019
SANTA CLARA, CA, USA

Co-located with **USENIX Security '19**



Questions and
comments?