“*Belt and suspenders*” or “*just red tape*”?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification

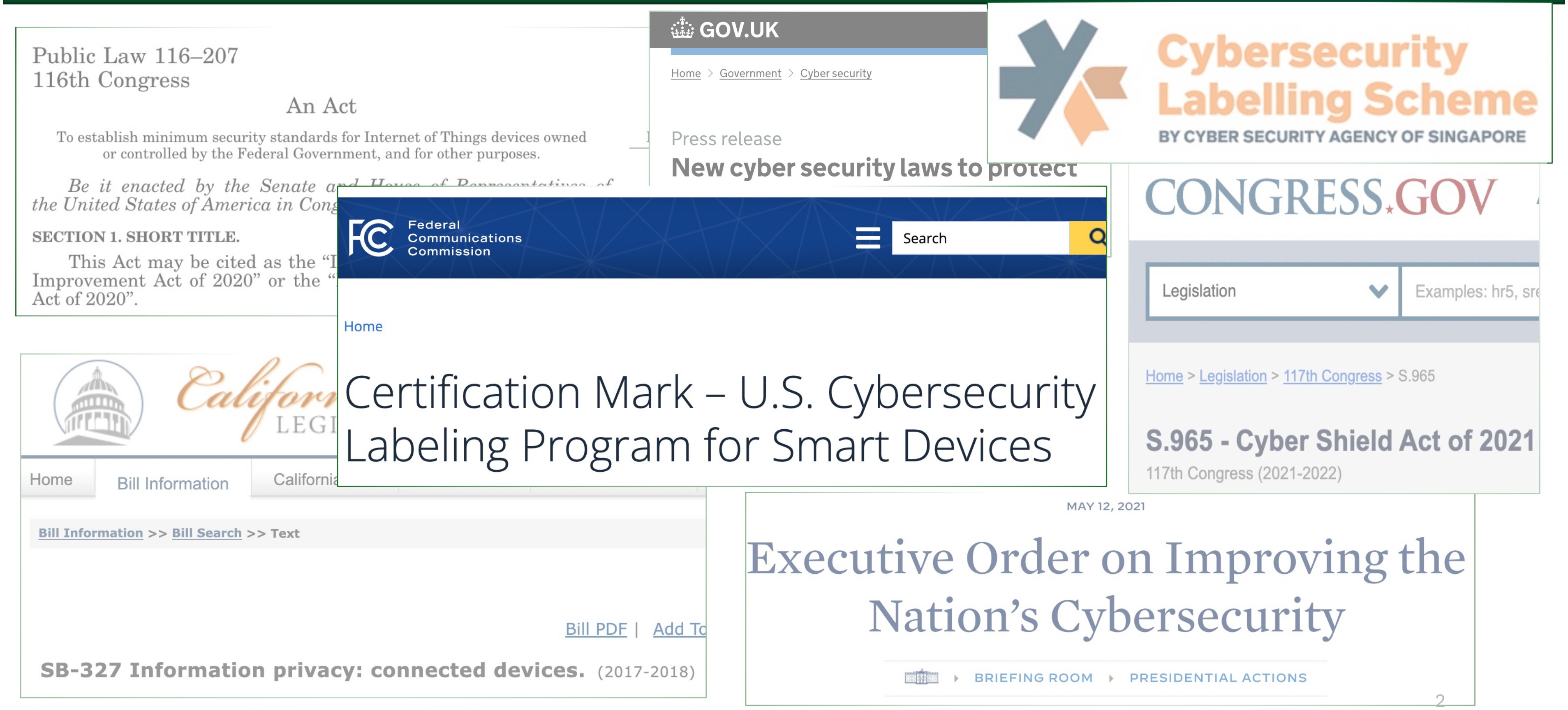
Prianka Mandal, Amit Seal Ami, Victor Olaiya, Sayyed Hadi Razmjo, and Adwait Nadkarni

William & Mary

Secure Platforms Lab

WILLIAM & MARY
CHARTERED 1693

Public Sector Focusing on IoT Security



Public Law 116–207
116th Congress

An Act

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Cong

SECTION 1. SHORT TITLE.

This Act may be cited as the "I Improvement Act of 2020" or the " Act of 2020".

GOV.UK

Home > Government > Cyber security

Press release

New cyber security laws to protect

Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

CONGRESS.GOV

Legislation

Examples: hr5, sre

Home > Legislation > 117th Congress > S.965

S.965 - Cyber Shield Act of 2021

117th Congress (2021-2022)

Federal Communications Commission

Search

Home

Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices

California LEGI

Home | Bill Information | California

Bill Information >> Bill Search >> Text

Bill PDF | Add To

SB-327 Information privacy: connected devices. (2017-2018)

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM > PRESIDENTIAL ACTIONS

Commercially Licensed Evaluation Facility (CLEF) or “Labs”

ioXt
internet of secure things

AUJAS CYBERSECURITY

NSE NSEIT

ValueMentor

RAPID7

RED ALERT LABS
IoT Security

TBG SECURITY

GUIDEPOINT SECURITY

IoT Security Standards

IoT Security Foundation

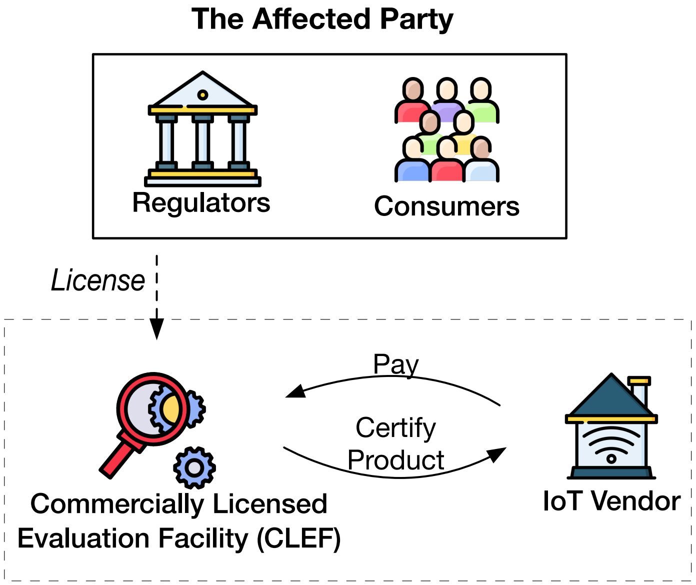
IoTA IoT Alliance Australia

NIST

GSMA™

ioXt
internet of secure things

The Traditional Security Certification Model



Does this traditional security certification model work

i. in the *context of IoT products*, and

ii. as well as *consumers expect it to*?

Research Questions and Approach

RQ1: Are certified IoT products vulnerable?

1. Mobile-IoT App Analysis

RQ2: Are vulnerable but certified IoT products non-compliant?

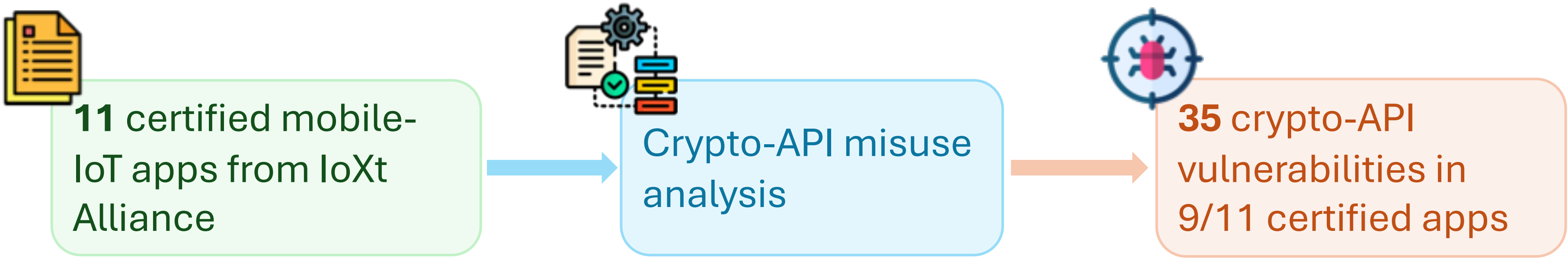
2. Security Compliance Analysis

RQ3: How do consumers perceive compliance enforcement?

3. User Study

17 Findings!

Mobile-IoT App Analysis



11 certified mobile-IoT apps from IoXt Alliance

Crypto-API misuse analysis

35 crypto-API vulnerabilities in 9/11 certified apps

- Primary UIs for controlling, configuring and automating IoT devices
- 25/30 CLEFs provide certification/assessments for mobile-IoT apps

- Uncover gaps in compliance enforcement
- Do not seek coverage of all vulnerabilities

Manual

Find vulnerabilities and understand the implications

Key Findings - Mobile-IoT App Analysis

```
this.ALGO = "AES/" +
            ((char) ("AES/GCM/NoPadding".charAt(4) - 2))
            + "AES/GCM/NoPadding".charAt(5) +
            ((char) ("AES/GCM/NoPadding".charAt(6) - 11))
            + "/NoPadding";

Cipher cipher = Cipher.getInstance(this.ALGO );
```

```
// The string operations result in: "AES /" + "E" + "C" + "B" +
"/NoPadding"
// = "AES/ECB/NoPadding"
```

Finding 1: Some mobile-IoT apps evade compliance checks by disguising vulnerable code as compliant.

```
Cipher cipher = Cipher.getInstance("AES");
```

AES/ECB/NoPadding

Finding 2: Some certified mobile-IoT apps use vulnerable encryption when transmitting sensitive audio/video data to/from IoT devices

SAST tools could not find this!

Finding 5: CogniCrypt, MobSF, and CryptoGuard, do not detect several of the 35 critical vulnerabilities discovered using manual reverse engineering, and none detect the evasive use.

Security Compliance Analysis

IoT Security Foundation standard

OWASP Mobile Application Security Verification standard

IoT Alliance Australia security guidelines

NIST's Core IoT Cybersecurity Capabilities Baseline

ioXt standard

- What criteria apply to the vulnerabilities?

- How they apply?

Systematically transform the relevant parts of the standard into specific criteria

Compare criteria with the vulnerabilities

Key Findings - Security Compliance Analysis

3 key reasons

Overly broad criteria

"Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. "

Finding 9: Broad criteria can seem comprehensive but may help developers claim vulnerable code as compliant.

Ambiguous test cases

"… does not request excessive sensitive permissions."

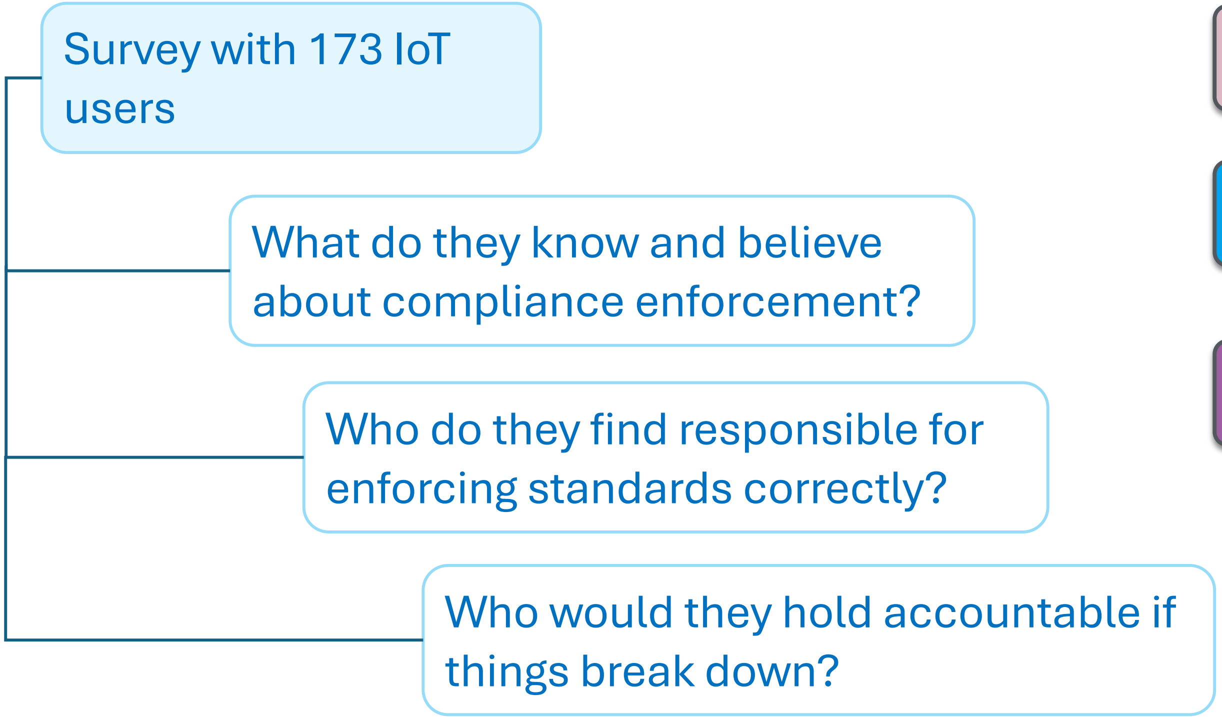
Finding 10: Ambiguous test cases allow significant discretion to the tester, preventing an unequivocal determination of compliance.

Loopholes in the criteria

"Encrypt all network traffic, using verified TLS where possible"

Finding 11: ioXt's discretionary criteria let developers choose what communication or data to protect, risking vulnerable apps claiming compliance.

User Study



Survey with 173 IoT users

What do they know and believe about compliance enforcement?

Who do they find responsible for enforcing standards correctly?

Who would they hold accountable if things break down?

IRB approved

39 questions

Thematic Analysis

Key Findings - User Study

Lack of Exposure to Compliance Standards

"...aware about from my colleague and then I further looked into it." (P99)

Finding 12: Users are generally not informed of IoT compliance standards, and often unaware of the certified (status of the) mobile-IoT apps they use.

Trust in Certification over Brand Reputation

"I wouldn't know where to start looking for this information or how to interpret it. I would instead trust reviews or I guess expert opinions". (P41)

Finding 14: Users overwhelmingly put their trust in certification, assuming that (1) certified apps are more secure, (2) their developers spend more effort on security, and (3) they can be trusted to handle security/privacy sensitive information.

Key Findings - User Study

All Stakeholders (except users) are Responsible, but Developers Are Mostly to Blame

“The developer - for the safety and security of the user.
The certification lab - their certification should not have dangerous cracks in the infrastructure.
The standards body - by not vetting the certification lab as well as they should.
*The user - just a pawn and a victim.” (*P32)

Most users trust security compliance to work as security assurance, i.e., a *“**belt and suspenders scenario**”* (P144), *however,*

Some were skeptical, believing that **certifications are** “***just red tape***” (P11)

Takeaways

1. As the traditional model does not seem to work, it needs to be **reformed through effective checks and balances**, such as developing tools for auditing CLEFs' effectiveness.

2. **Effective and robust vulnerability discovery tools** are needed as current tools have proven insufficient for compliance enforcement.

3. Mechanisms to **deter, prevent and detect evasive developers** needs to be built into the certification model.

4. **Users should be informed about the IoT product security certification** and their rights if things break down.

pmandal@wm.edu https://priankamandal.com/