Do vulnerabilities matter? Practical Implications of Vulnerability Analysis in the IoT Ecosystem

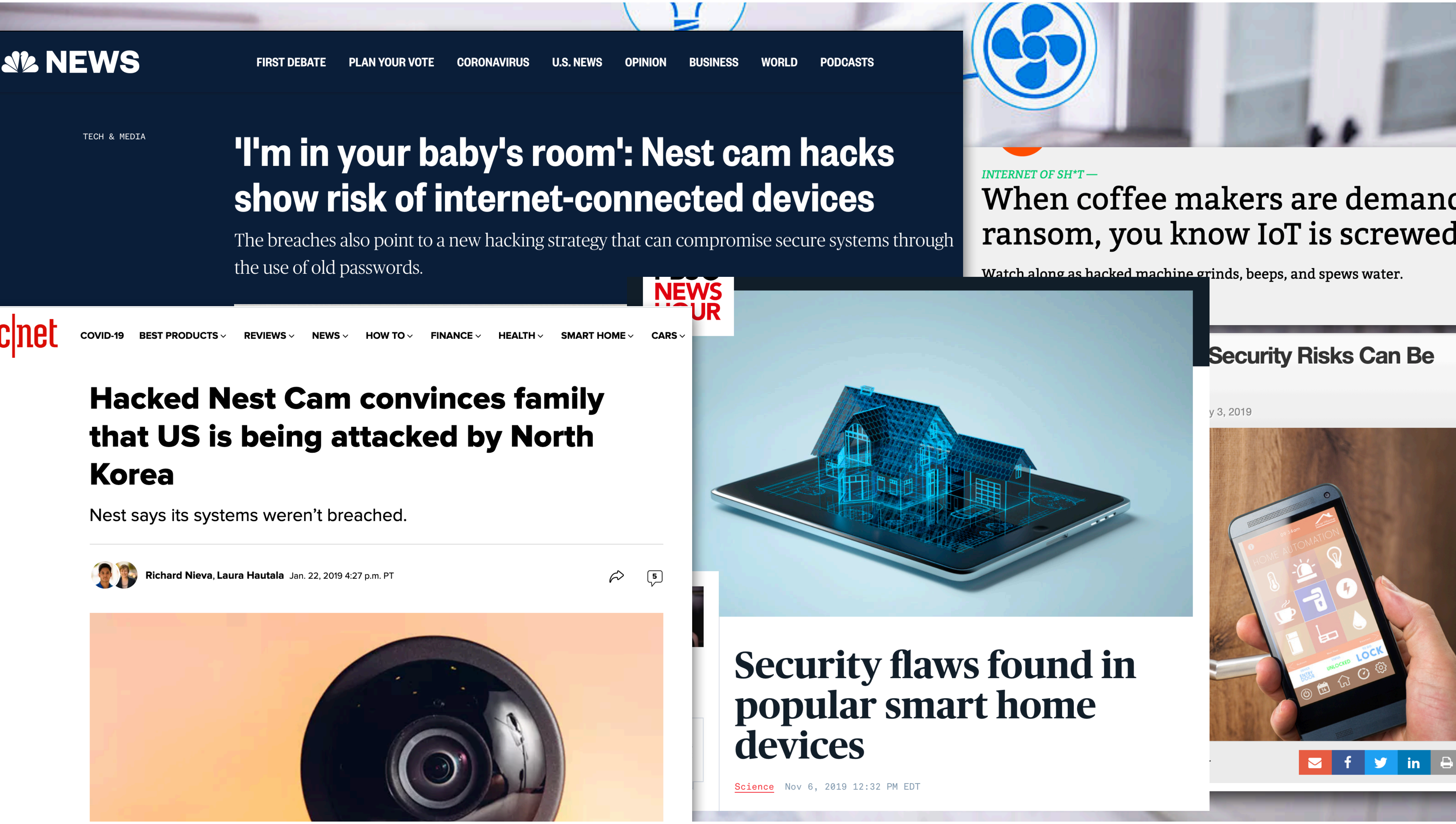
CSCI 445/545, Spring 2026

- Prof. Adwait Nadkarni

Secure Platforms Lab

William & Mary

CHARTERED 1693



TECH & MEDIA

'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices

The breaches also point to a new hacking strategy that can compromise secure systems through the use of old passwords.

INTERNET OF SH*T —

When coffee makers are demand ransom, you know IoT is screwed

Watch along as hacked machine grinds, beeps, and spews water.

Hacked Nest Cam convinces family that US is being attacked by North Korea

Nest says its systems weren't breached.

Richard Nieva, Laura Hautala Jan. 22, 2019 4:27 p.m. PT

Security flaws found in popular smart home devices

Science Nov 6, 2019 12:32 PM EDT

Security Risks Can Be

y 3, 2019

Home automation

trigger

1 When Alice leaves, turn the Camera ON (*for **security***)

action

trigger

2 When Alice returns, turn the Camera Off (*for **privacy***)

action

Home Automation *routines*/ *IoT apps*/*programs*

Security Implications of Home Automation

Bob wants to steal from Alice *without being monitored*

Bob tries to directly attack the security camera, *and fails*

However, **Bob** can *indirectly* attack the camera

Security Implications of Home Automation

Bob performs a *lateral privilege escalation*[1]

1 Compromise a *vulnerable* component

2 Leverage it to *remotely disable the camera*

[1] Kafle, Kaushal, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, and Denys Poshyvanyk. ***A Study of Data Store-based Home Automation.*** In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY)*, ***Best Paper Award.***

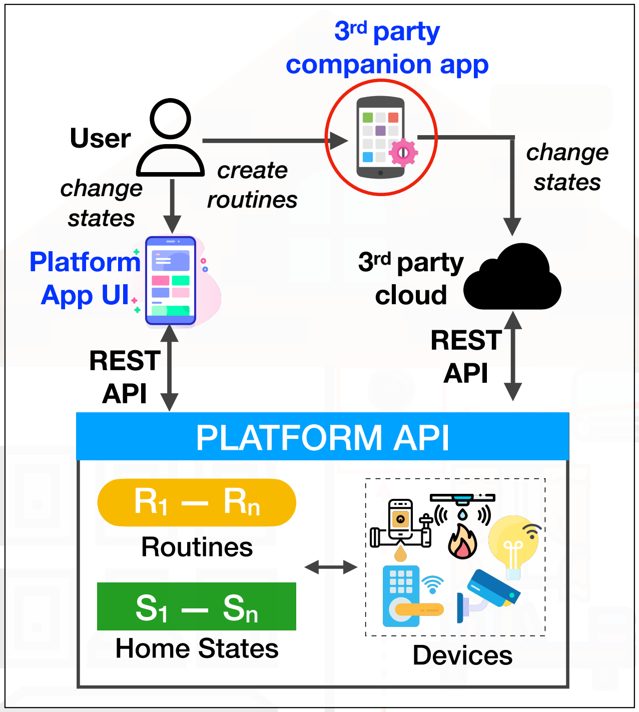
Security Implications of Home Automation *and* mobile-IoT apps

Bob performs a *lateral privilege escalation*[1]

1 Compromise a *vulnerable* component

TP Link Kasa app + MiTM Attack

Auth Token



2 Leverage it to *remotely disable the camera*

SET *away —> home*

Platform API (e.g., SmartThings)

camera= Off

home

Routines

If home *then* camera Off

If away *then* camera ON

...

home

- mode = *home*
- camera = *ON*
- temp = *75f*
- ...

Home State

Lesson 1: Every part of the IoT system can be vulnerable to attack

Lesson 2: There is the possibility of tangible harm to users

[1] Ka... ...e Automation. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY), Best Paper Award.

Vulnerabilities Matter *in principle*

Because they can be used to cause harm

Then why do vulnerabilities persist?

*Can we make **meaningful change** upon finding and reporting a vulnerability?*

*Are there environmental factors that inhibit impact? Where are the **loose ends**?*

*Do vulnerabilities matter **in practice**? To other stakeholders?*

Context: IoT Product Security Certification

ioXt
internet of secure things

NIST
IoT Security Guidelines

IoT
Security Foundation

IoTA
IoT Alliance Australia

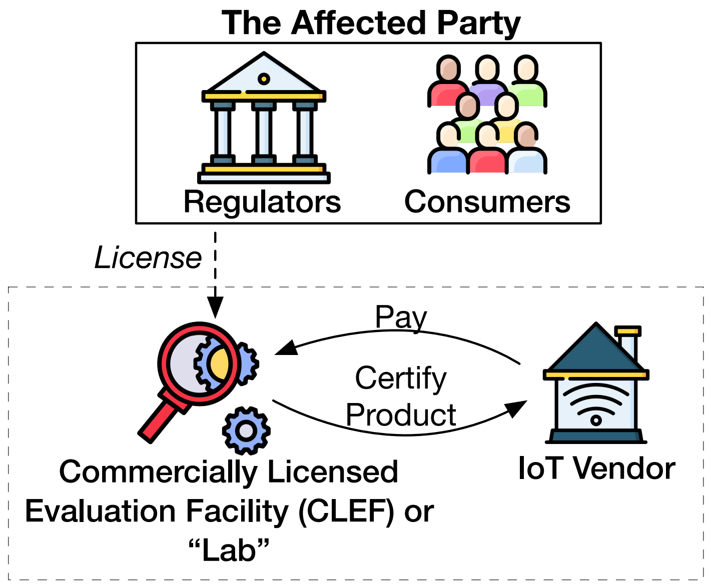
U.S. CYBER TRUST MARK

Product Security and
Telecommunications
Infrastructure Act
2022

Standards and regulations **enable change**: You can ***hold vendors accountable*** to the standard, and ***make vendors fix vulnerabilities***!

Problem solved?

Context: IoT Product Security Certification



The Affected Party

Regulators

Consumers

License

Pay

Certify Product

Commercially Licensed Evaluation Facility (CLEF) or “Lab”

IoT Vendor

The ***traditional*** model for compliance enforcement

ioXt internet of secure things

NIST IoT Security Guidelines

IoT Security Foundation

IoTA IoT Alliance Australia

U.S. CYBER TRUST MARK

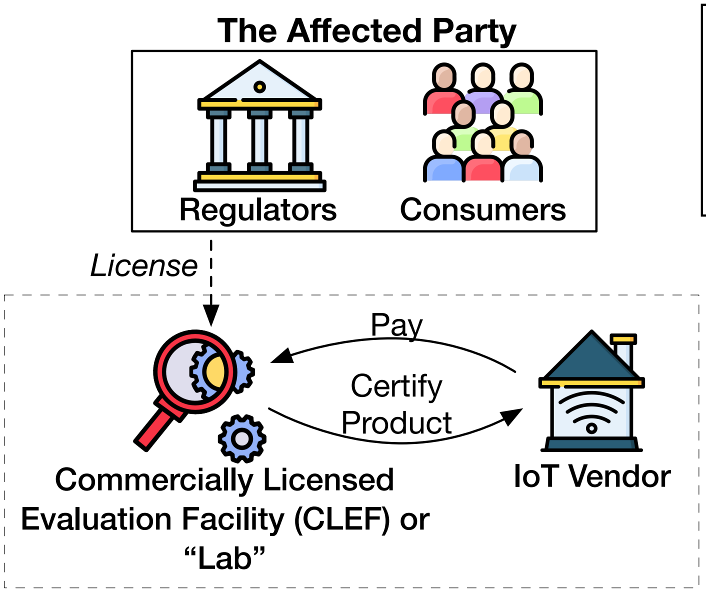
Product Security and Telecommunications Infrastructure Act 2022

What **incentive** do vendors have to ***select a lab that would be thorough in finding vulnerabilities***, as opposed to one that will provide quick certification?

What **incentive** do labs have to ***rigorously find vulnerabilities***?

Standards and regulations ***can enable change***: You can hold vendors accountable, make them make fix vulnerabilities, ***but only if the enforcement model works***

Investigating IoT Product Security Certification



The ***traditional*** model for compliance enforcement

Research Question — Does the traditional model for compliance certification *work for IoT, and as well as consumers expect it to?*

Are certified IoT products *vulnerable*?

Analyzed all (11) certified mobile-IoT apps from ioXt internet of secure things

Do vulnerabilities make them *non-compliant*?

Compliance analysis with 5 standards: ioXt, MASVS, IOTAA, IoTSF, NIST Baseline

How do consumers perceive IoT security certification?

Survey with **173 IoT users**

Mandal, Prianka, Amit Seal Ami, Victor Olaiya, Sayyed Hadi Razmjo, and Adwait Nadkarni. "***'Belt and suspenders' or 'just red tape'*?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification.**" In *Proceedings of the 2024 USENIX Security Symposium (USENIX),* Aug 2024.

Findings: Security Analysis of Certified Apps

Analyzed 11 certified mobile-IoT apps from ioXt internet of secure things

35 crypto-API vulns in 9/11 ***certified*** apps

Finding 2: Certified apps use vulnerable encryption for ***transmitting sensitive audio/video data*** to IoT devices (e.g., cameras) `E.g., Cipher.getInstance(“AES/ECB/NoPadding“);`

Finding 3: Certified apps override `TrustManagers` and `HostnameVerifiers` in vulnerable ways, ***exposing authentication tokens to MiTM attacks***.

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

Example: Vulnerable Code in an IoT SDK/platform; used by ***580k developers*** (app ***installed by >5 million users***)

Finding 1: Developers may try to ***evade compliance checks by disguising vulnerable code as secure***.

Findings: Compliance Analysis of Vulnerable but Certified Apps

Question: Would a vulnerability in a certified app make it non-compliant?

Short Answer (from analysis of 5 standards): **No!**

Vulnerable App
3 reasons
compliant

Reason 1: Overly Broad Criteria

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

```
E.g., Cipher.getInstance("AES")
```

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

Reason 2: Ambiguous Test Cases

the tester may accept the app if it "… does not request **excessive** sensitive permissions."

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

Reason 3: Loopholes

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

Finding 11: **Developers may have discretion** in determining when secure implementation is possible, making security certification pointless.

Findings: User Expectations and Perceptions

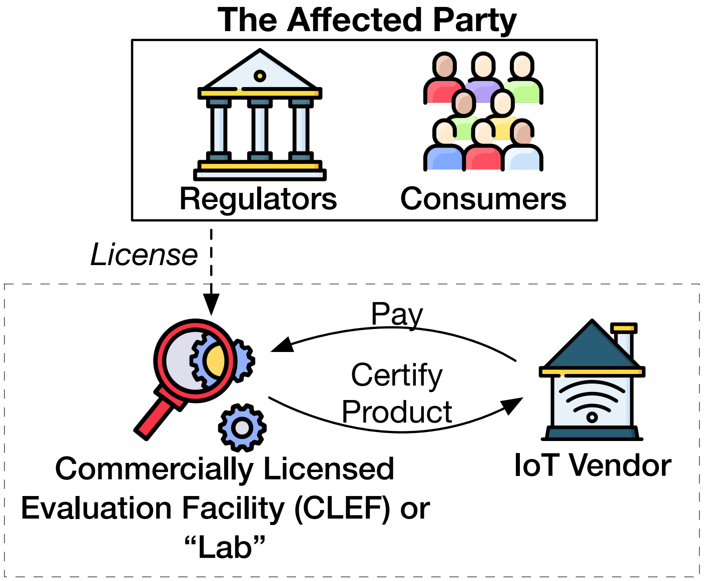
Survey with 173 IoT users: knowledge, expectations, and beliefs regarding liability in case of compliance failures

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

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)

Recall: IoT Product Security Certification as a means of enabling change



The ***traditional*** model for compliance enforcement

Regulations and certification *can enable change*: You could hold vendors accountable and make them make fix vulnerabilities, ***but only if the enforcement model works***

A "*belt and suspenders scenario*"

However, in practice, it is ***"just red tape"***

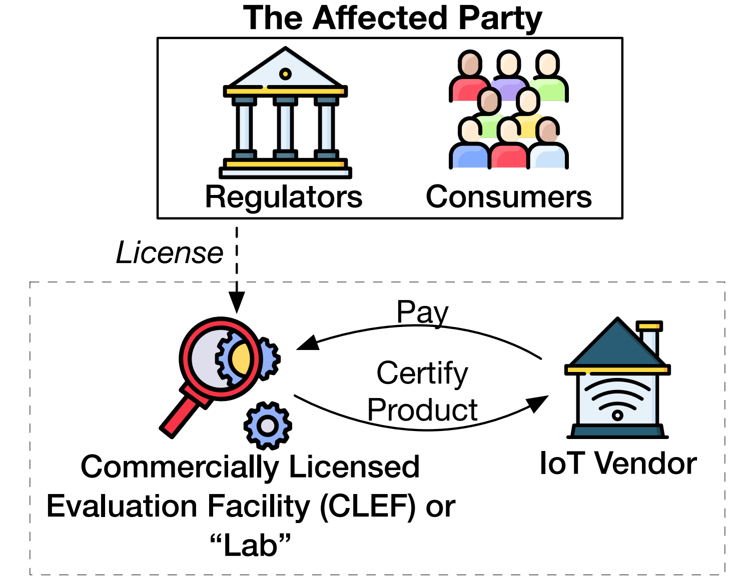
1. **Certified IoT products have vulnerabilities** that are both within scope of standards *in spirit* and affect sensitive data.

2. **Vulnerabilities do not make products non-compliant** due to vague and discretionary criteria.

What incentive do vendors have to *select a lab that would be thorough in finding vulnerabilities*, as opposed to one that will provide quick certification?

We may not be able to use compliance and security certification to hold vendors accountable, or to get them to fix vulnerabilities.

Liability: *Who is liable for harm due to security failures in an IoT product?*



The ***traditional*** model for compliance enforcement

Studying **liability** will help us:

- **Understand the implications** of the vulnerabilities we find and report
- **Pave way for incentivizing vendors and CLEFs** to take vulnerabilities seriously.