BUGATTI:

Embedded Security Testing and Automation

Kick-off meeting, May 15th 2025

Jorn Lapon

KU LEUVEN DistriNet

VUB SOFTWARE LANGUAGES LAB

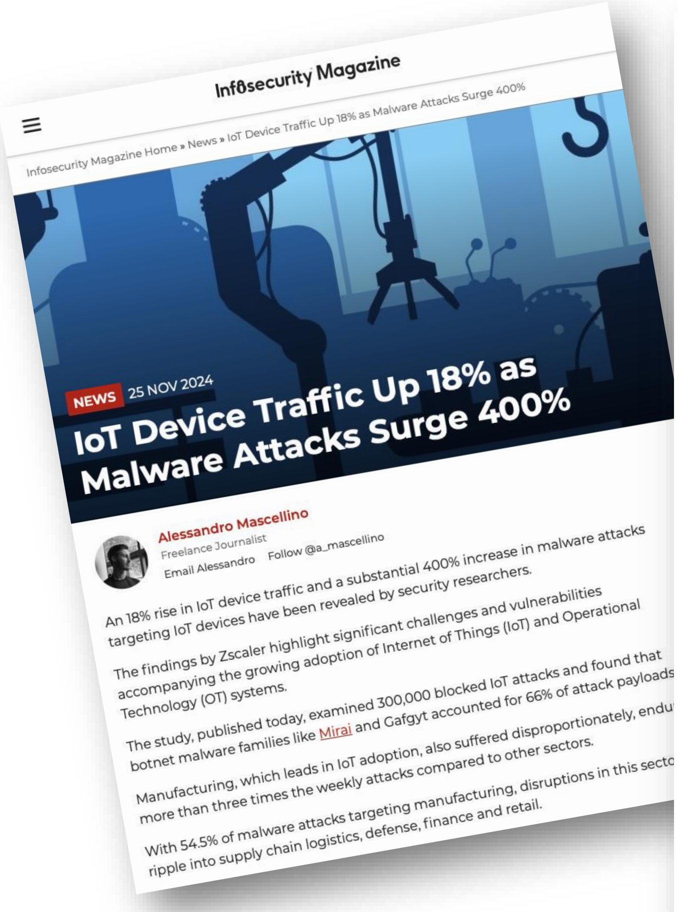
Agenda

- Introduction
- Project Goals & Approach
- DistriNet@Ghent, KU Leuven
- Soft Languages Lab, VUB + Demo
- Discussion, AOB

BUGATTI:

Embedded Security Testing and Automation

WHY？



Infosecurity Magazine

Infosecurity Magazine Home » News » IoT Device Traffic Up 18% as Malware Attacks Surge 400%

NEWS 25 NOV 2024

IoT Device Traffic Up 18% as Malware Attacks Surge 400%

Alessandro Mascellino
Freelance Journalist
Email Alessandro Follow @a_mascellino

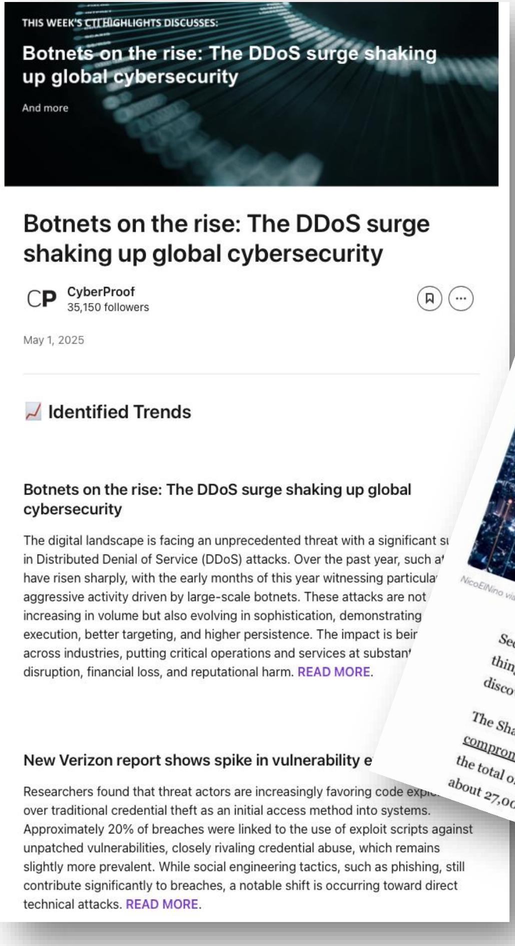
An 18% rise in IoT device traffic and a substantial 400% increase in malware attacks targeting IoT devices have been revealed by security researchers.

The findings by Zscaler highlight significant challenges and vulnerabilities accompanying the growing adoption of Internet of Things (IoT) and Operational Technology (OT) systems.

The study, published today, examined 300,000 blocked IoT attacks and found that botnet malware families like Mirai and Gafgyt accounted for 66% of attack payloads

Manufacturing, which leads in IoT adoption, also suffered disproportionately, endu more than three times the weekly attacks compared to other sectors.

With 54.5% of malware attacks targeting manufacturing, disruptions in this secto ripple into supply chain logistics, defense, finance and retail.



THIS WEEK'S CTI HIGHLIGHTS DISCUSSES:

Botnets on the rise: The DDoS surge shaking up global cybersecurity

And more

Botnets on the rise: The DDoS surge shaking up global cybersecurity

CP CyberProof
35,150 followers

May 1, 2025

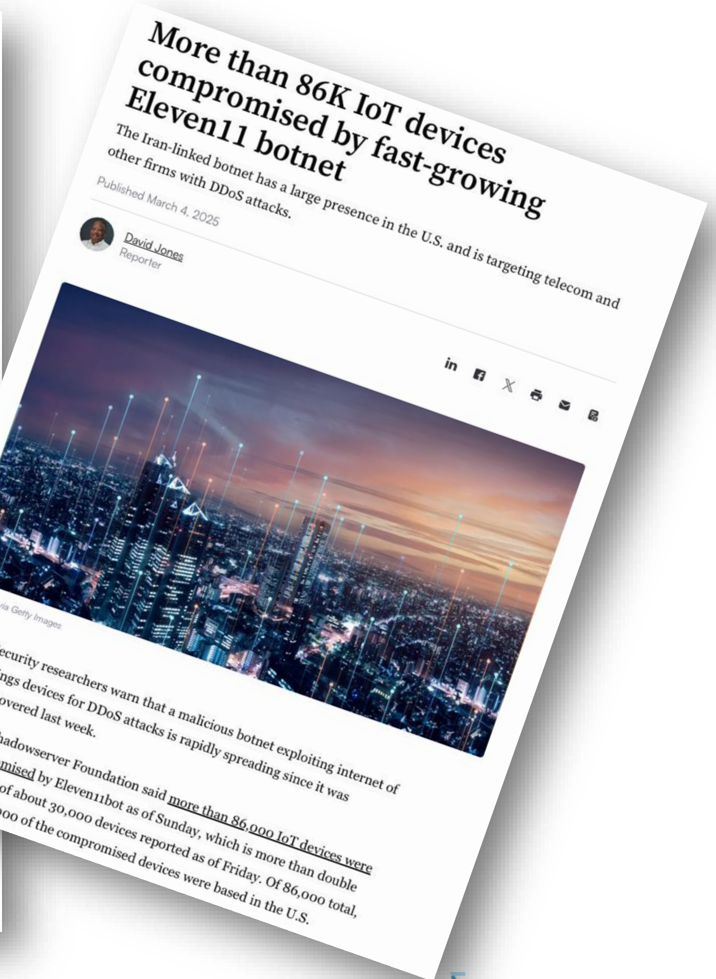
📈 Identified Trends

Botnets on the rise: The DDoS surge shaking up global cybersecurity

The digital landscape is facing an unprecedented threat with a significant su in Distributed Denial of Service (DDoS) attacks. Over the past year, such at have risen sharply, with the early months of this year witnessing particula aggressive activity driven by large-scale botnets. These attacks are not increasing in volume but also evolving in sophistication, demonstrating execution, better targeting, and higher persistence. The impact is bein across industries, putting critical operations and services at substant disruption, financial loss, and reputational harm. READ MORE.

New Verizon report shows spike in vulnerability e

Researchers found that threat actors are increasingly favoring code explo over traditional credential theft as an initial access method into systems. Approximately 20% of breaches were linked to the use of exploit scripts against unpatched vulnerabilities, closely rivaling credential abuse, which remains slightly more prevalent. While social engineering tactics, such as phishing, still contribute significantly to breaches, a notable shift is occurring toward direct technical attacks. READ MORE.



More than 86K IoT devices compromised by fast-growing Eleven11 botnet

The Iran-linked botnet has a large presence in the U.S. and is targeting telecom and other firms with DDoS attacks.

Published March 4, 2025

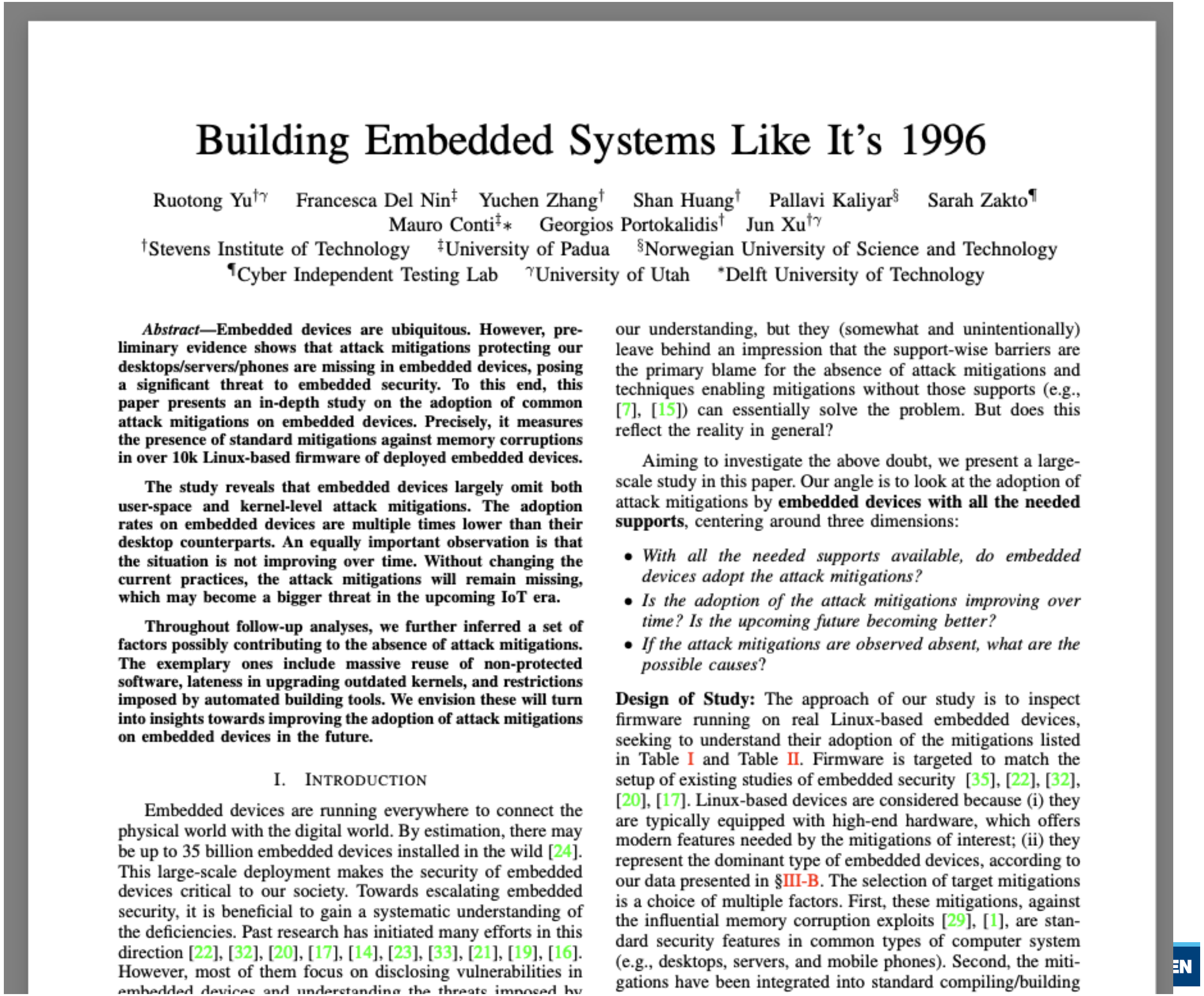
David Jones
Reporter

NicoElNino via Getty Images

Security researchers warn that a malicious botnet exploiting internet of things devices for DDoS attacks is rapidly spreading since it was discovered last week.

The Shadowserver Foundation said more than 86,000 IoT devices were compromised by Eleven11bot as of Sunday, which is more than double the total of about 30,000 devices reported as of Friday. Of 86,000 total, about 27,000 of the compromised devices were based in the U.S.

Convincing for Industry?



Building Embedded Systems Like It's 1996

Ruotong Yu[†γ] Francesca Del Nin[‡] Yuchen Zhang[†] Shan Huang[†] Pallavi Kaliyar[§] Sarah Zakto[¶]
Mauro Conti[‡∗] Georgios Portokalidis[†] Jun Xu[†γ]
[†]Stevens Institute of Technology [‡]University of Padua [§]Norwegian University of Science and Technology
[¶]Cyber Independent Testing Lab [γ]University of Utah [∗]Delft University of Technology

***Abstract*—Embedded devices are ubiquitous. However, preliminary evidence shows that attack mitigations protecting our desktops/servers/phones are missing in embedded devices, posing a significant threat to embedded security. To this end, this paper presents an in-depth study on the adoption of common attack mitigations on embedded devices. Precisely, it measures the presence of standard mitigations against memory corruptions in over 10k Linux-based firmware of deployed embedded devices.**

The study reveals that embedded devices largely omit both user-space and kernel-level attack mitigations. The adoption rates on embedded devices are multiple times lower than their desktop counterparts. An equally important observation is that the situation is not improving over time. Without changing the current practices, the attack mitigations will remain missing, which may become a bigger threat in the upcoming IoT era.

Throughout follow-up analyses, we further inferred a set of factors possibly contributing to the absence of attack mitigations. The exemplary ones include massive reuse of non-protected software, lateness in upgrading outdated kernels, and restrictions imposed by automated building tools. We envision these will turn into insights towards improving the adoption of attack mitigations on embedded devices in the future.

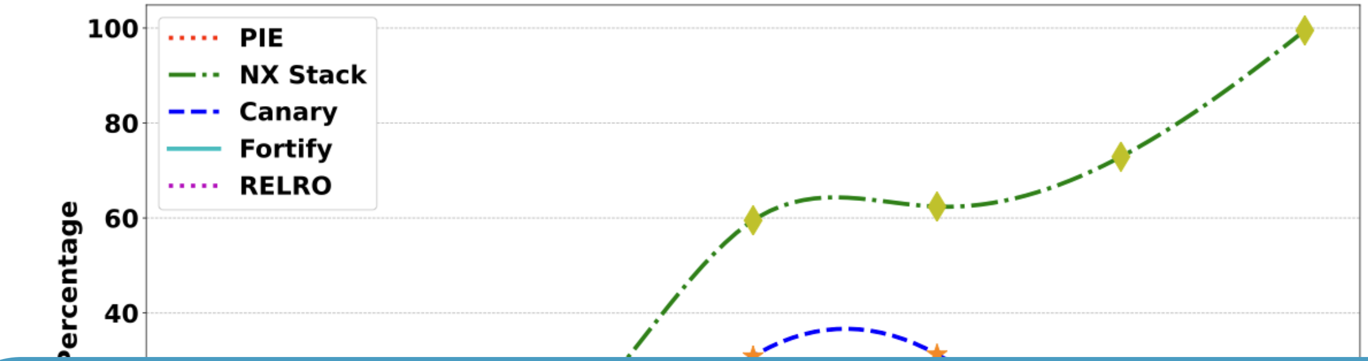
I. Introduction

Embedded devices are running everywhere to connect the physical world with the digital world. By estimation, there may be up to 35 billion embedded devices installed in the wild [24]. This large-scale deployment makes the security of embedded devices critical to our society. Towards escalating embedded security, it is beneficial to gain a systematic understanding of the deficiencies. Past research has initiated many efforts in this direction [22], [32], [20], [17], [14], [23], [33], [21], [19], [16]. However, most of them focus on disclosing vulnerabilities in embedded devices and understanding the threats imposed by our understanding, but they (somewhat and unintentionally) leave behind an impression that the support-wise barriers are the primary blame for the absence of attack mitigations and techniques enabling mitigations without those supports (e.g., [7], [15]) can essentially solve the problem. But does this reflect the reality in general?

Aiming to investigate the above doubt, we present a large-scale study in this paper. Our angle is to look at the adoption of attack mitigations by **embedded devices with all the needed supports**, centering around three dimensions:

- *With all the needed supports available, do embedded devices adopt the attack mitigations?*
- *Is the adoption of the attack mitigations improving over time? Is the upcoming future becoming better?*
- *If the attack mitigations are observed absent, what are the possible causes?*

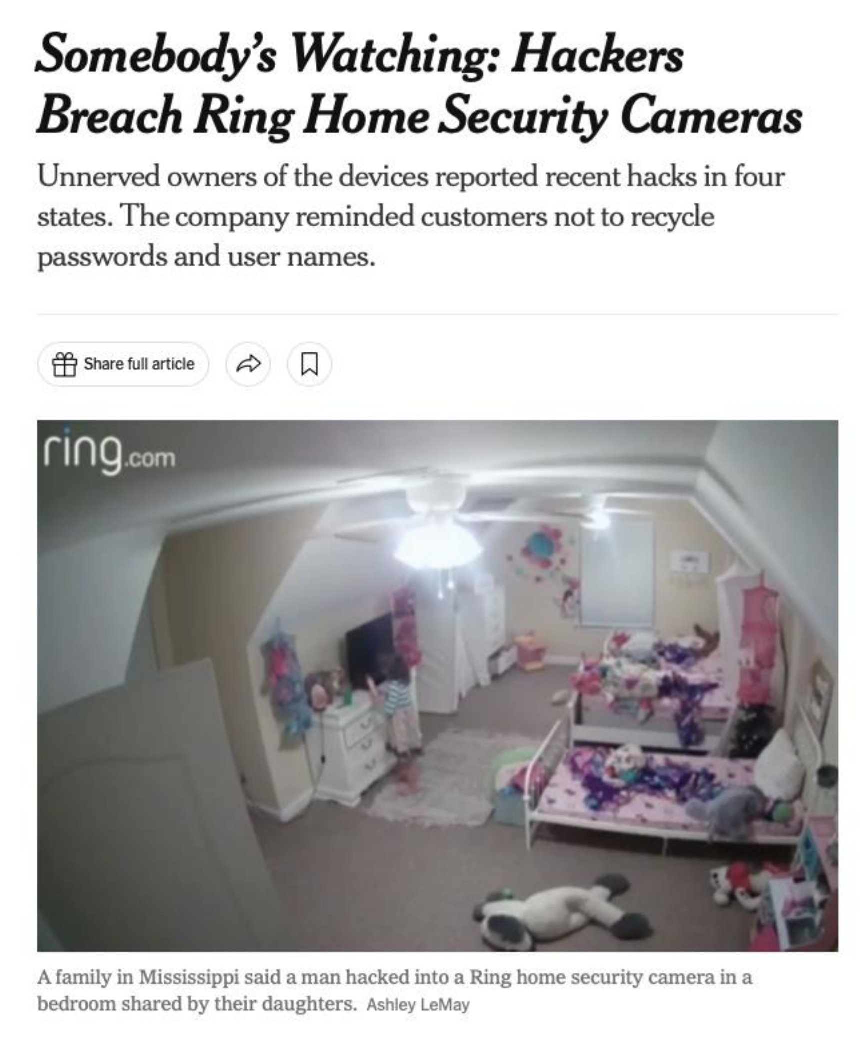
Design of Study: The approach of our study is to inspect firmware running on real Linux-based embedded devices, seeking to understand their adoption of the mitigations listed in Table I and Table II. Firmware is targeted to match the setup of existing studies of embedded security [35], [22], [32], [20], [17]. Linux-based devices are considered because (i) they are typically equipped with high-end hardware, which offers modern features needed by the mitigations of interest; (ii) they represent the dominant type of embedded devices, according to our data presented in §III-B. The selection of target mitigations is a choice of multiple factors. First, these mitigations, against the influential memory corruption exploits [29], [1], are standard security features in common types of computer system (e.g., desktops, servers, and mobile phones). Second, the mitigations have been integrated into standard compiling/building



Summary: Embedded devices have a low rate of adopting user-space mitigations, despite these devices broadly have the needed supports. The low adoption rate is **partially** attributed to the **restrictions of architectures and runtime environments**, but it **in general reflects the “decisions” of vendors**.

SO WHY???

BAD
MODERATE
GOOD
EXCELLENT
REPUTATION

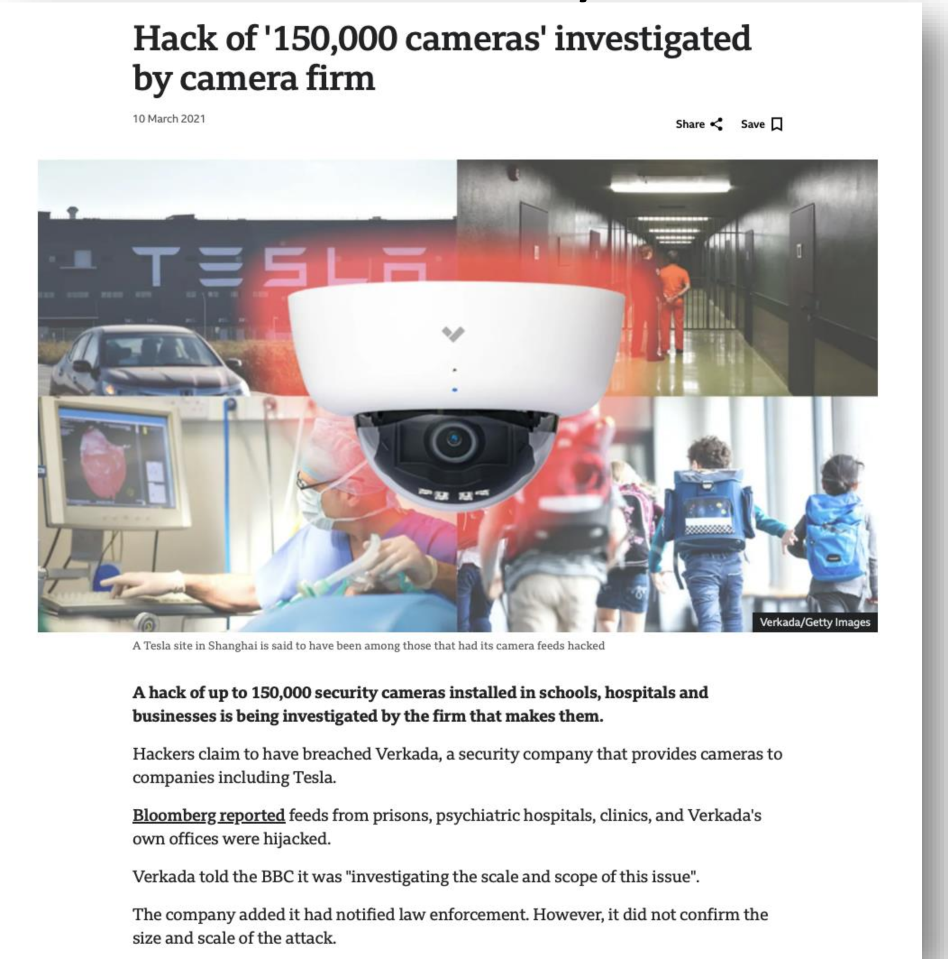


Somebody's Watching: Hackers Breach Ring Home Security Cameras

Unnerved owners of the devices reported recent hacks in four states. The company reminded customers not to recycle passwords and user names.

A family in Mississippi said a man hacked into a Ring home security camera in a bedroom shared by their daughters. Ashley LeMay

Verkada Security Camera



Hack of '150,000 cameras' investigated by camera firm

10 March 2021

A Tesla site in Shanghai is said to have been among those that had its camera feeds hacked

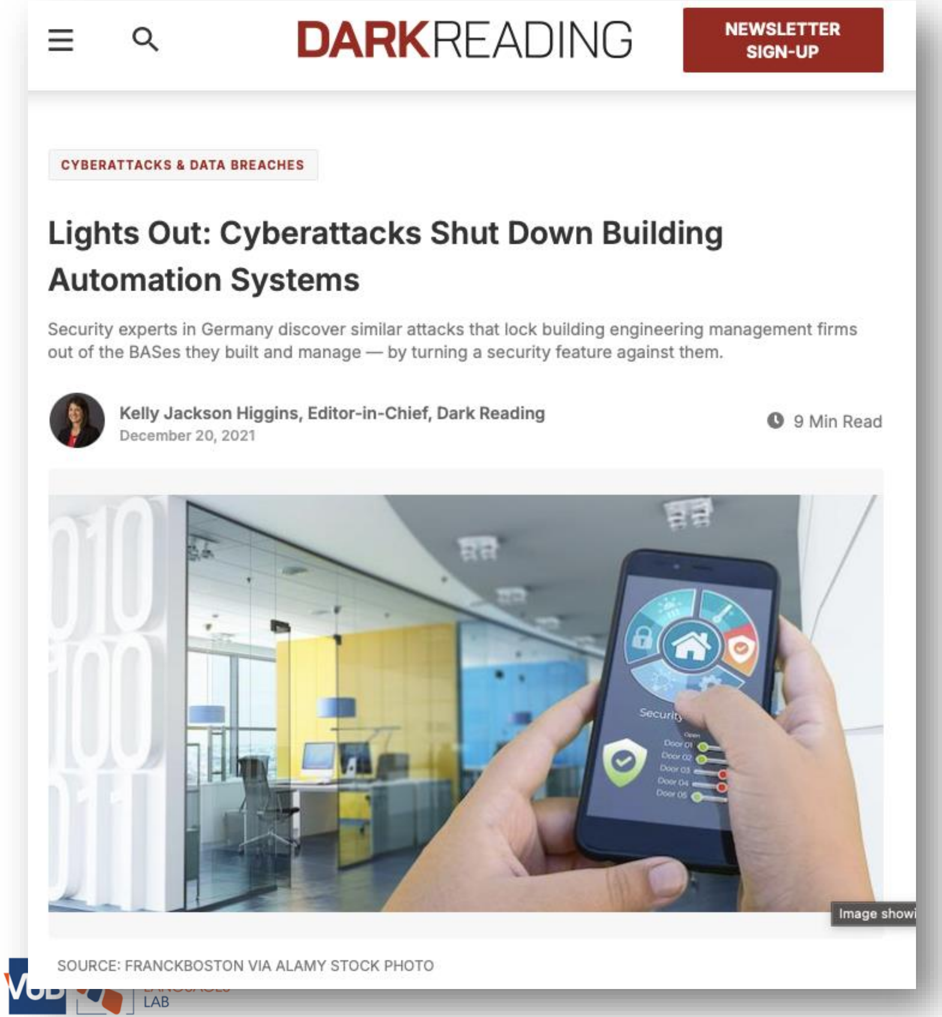
A hack of up to 150,000 security cameras installed in schools, hospitals and businesses is being investigated by the firm that makes them.

Hackers claim to have breached Verkada, a security company that provides cameras to companies including Tesla.

Bloomberg reported feeds from prisons, psychiatric hospitals, clinics, and Verkada's own offices were hijacked.

Verkada told the BBC it was "investigating the scale and scope of this issue".

The company added it had notified law enforcement. However, it did not confirm the size and scale of the attack.



DARKREADING

NEWSLETTER SIGN-UP

CYBERATTACKS & DATA BREACHES

Lights Out: Cyberattacks Shut Down Building Automation Systems

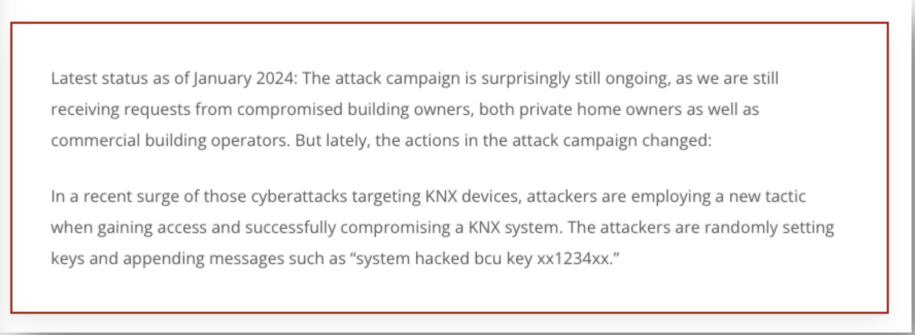
Security experts in Germany discover similar attacks that lock building engineering management firms out of the BASes they built and manage — by turning a security feature against them.

Kelly Jackson Higgins, Editor-in-Chief, Dark Reading
December 20, 2021

9 Min Read

Image showi

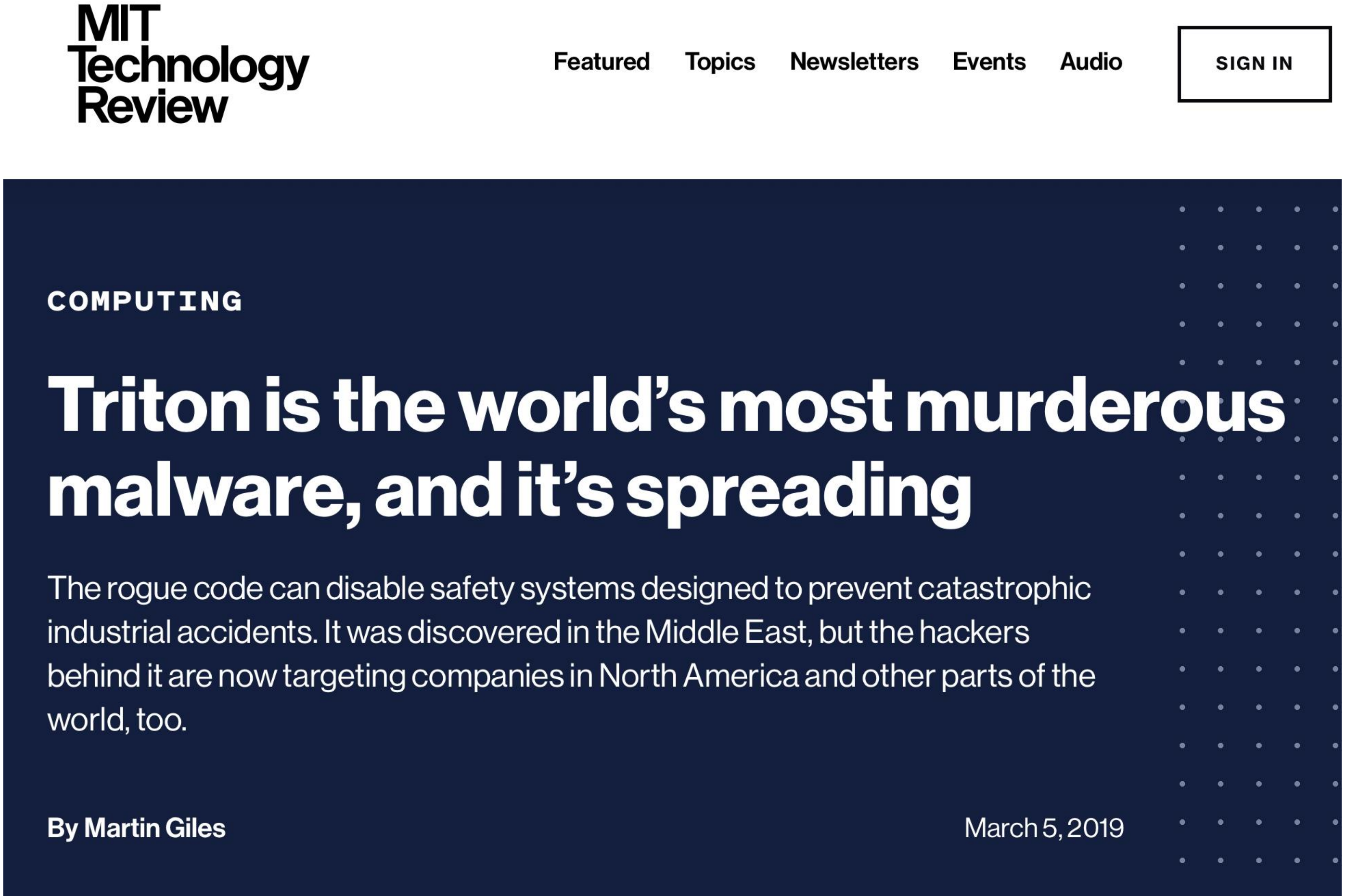
SOURCE: FRANCKBOSTON VIA ALAMY STOCK PHOTO



Latest status as of January 2024: The attack campaign is surprisingly still ongoing, as we are still receiving requests from compromised building owners, both private home owners as well as commercial building operators. But lately, the actions in the attack campaign changed:

In a recent surge of those cyberattacks targeting KNX devices, attackers are employing a new tactic when gaining access and successfully compromising a KNX system. The attackers are randomly setting keys and appending messages such as “system hacked bcu key xx1234xx.”

Critical Infrastructure



COMPUTING

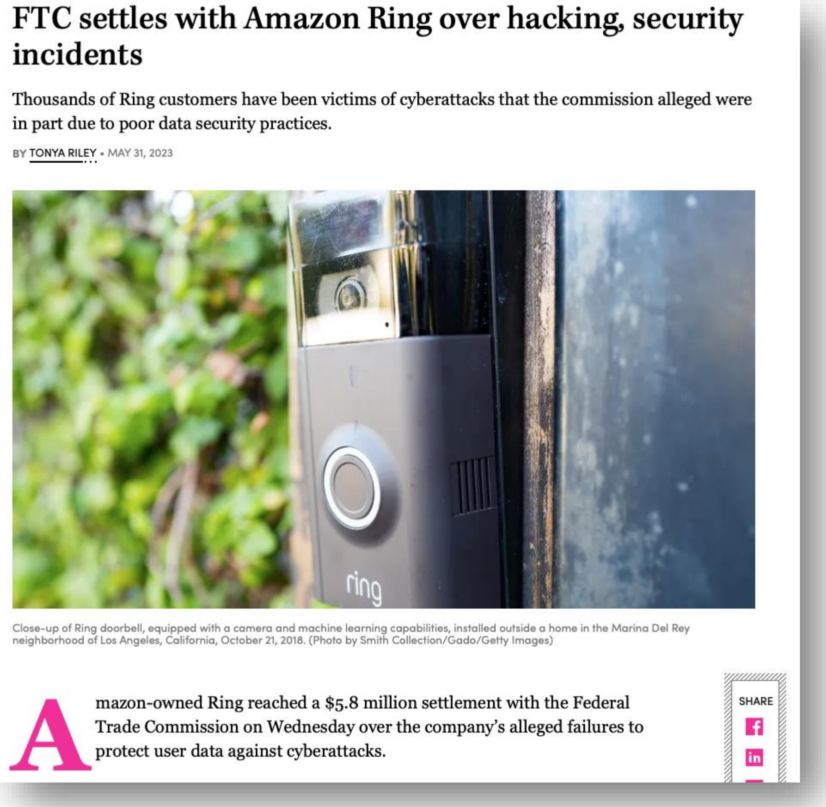
Triton is the world’s most murderous malware, and it’s spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

By Martin Giles

March 5, 2019

REGULATION



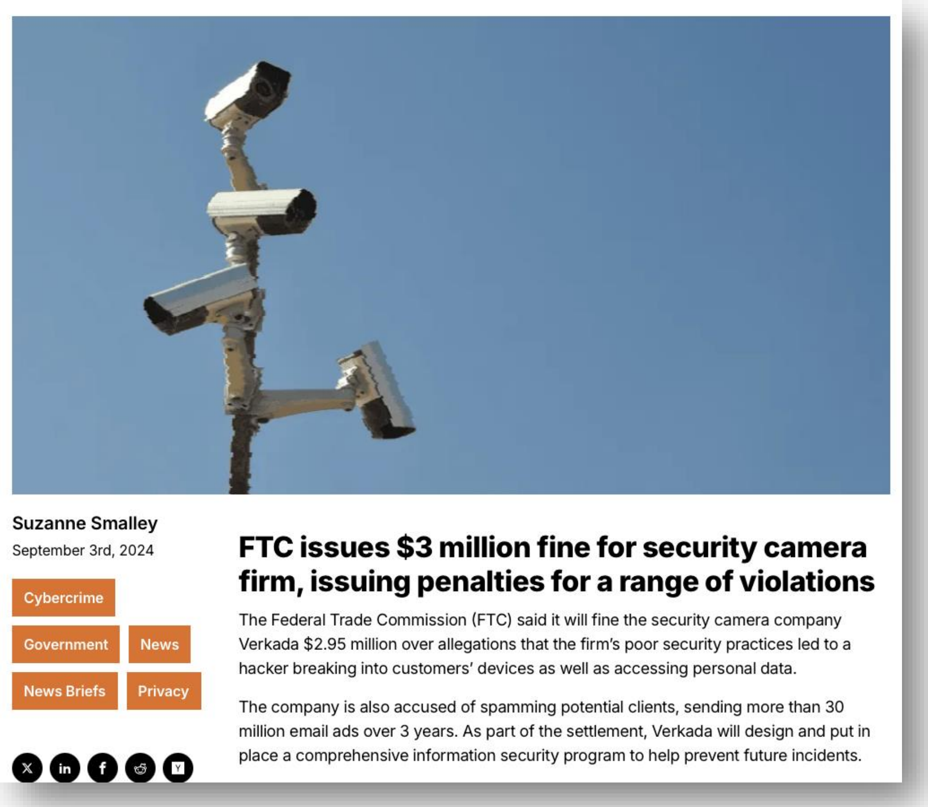
FTC settles with Amazon Ring over hacking, security incidents

Thousands of Ring customers have been victims of cyberattacks that the commission alleged were in part due to poor data security practices.

BY TONYA RILEY • MAY 31, 2023

Close-up of Ring doorbell, equipped with a camera and machine learning capabilities, installed outside a home in the Marina Del Rey neighborhood of Los Angeles, California, October 21, 2018. (Photo by Smith Collection/Gado/Getty Images)

Amazon-owned Ring reached a $5.8 million settlement with the Federal Trade Commission on Wednesday over the company's alleged failures to protect user data against cyberattacks.



Suzanne Smalley

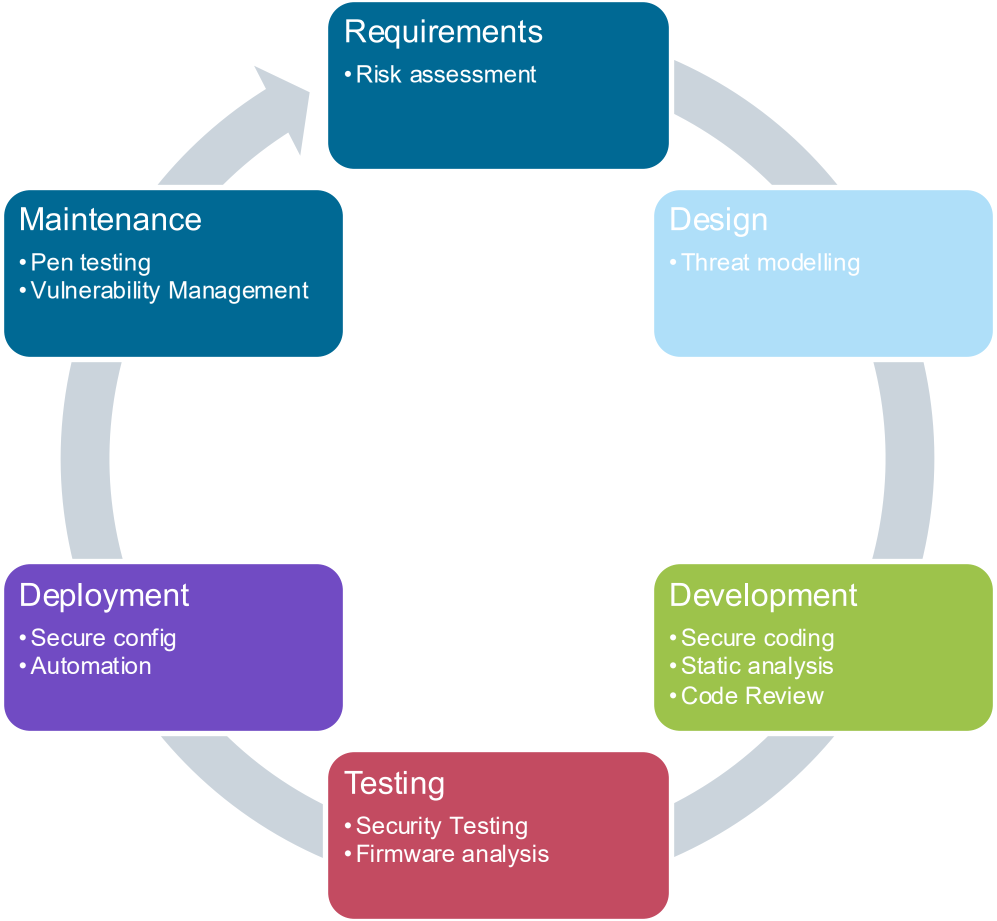
September 3rd, 2024

FTC issues $3 million fine for security camera firm, issuing penalties for a range of violations

The Federal Trade Commission (FTC) said it will fine the security camera company Verkada $2.95 million over allegations that the firm's poor security practices led to a hacker breaking into customers' devices as well as accessing personal data.

The company is also accused of spamming potential clients, sending more than 30 million email ads over 3 years. As part of the settlement, Verkada will design and put in place a comprehensive information security program to help prevent future incidents.

How ???



Requirements
- Risk assessment

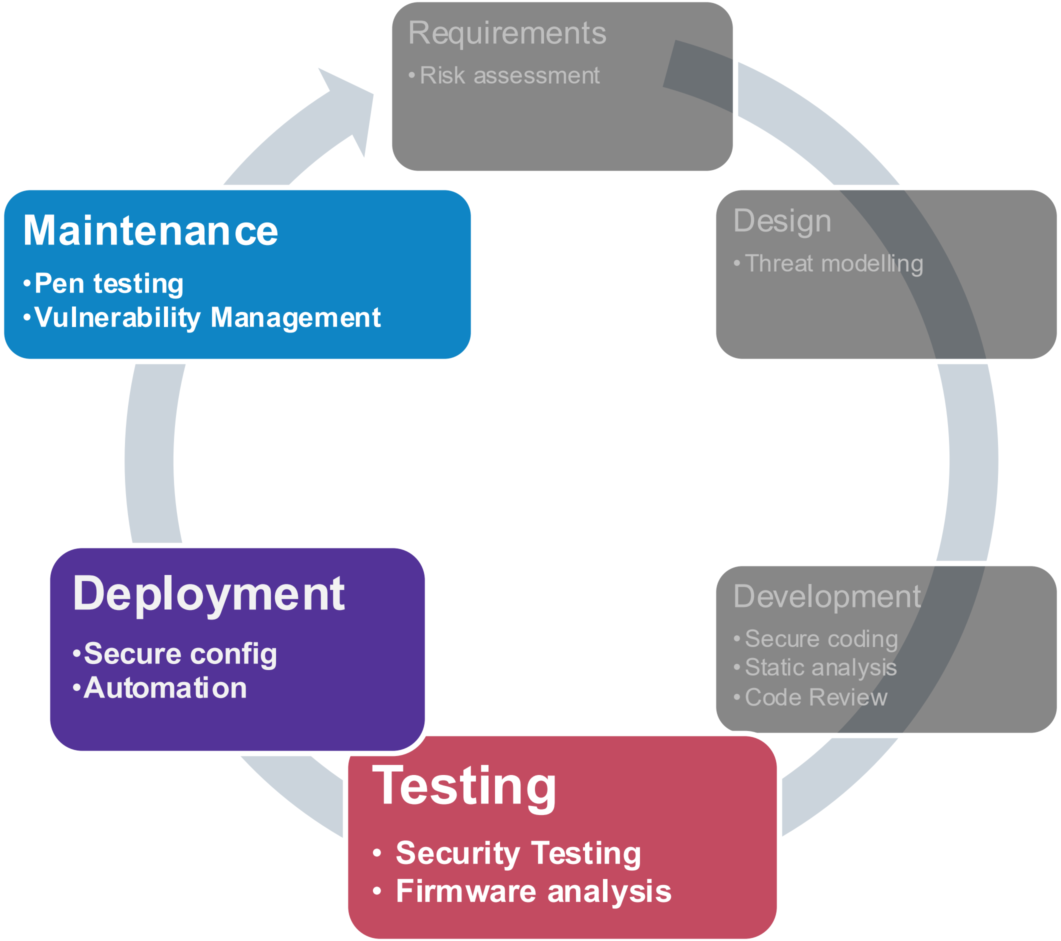
Design
- Threat modelling

Development
- Secure coding
- Static analysis
- Code Review

Testing
- Security Testing
- Firmware analysis

Deployment
- Secure config
- Automation

Maintenance
- Pen testing
- Vulnerability Management



Requirements
- Risk assessment

Design
- Threat modelling

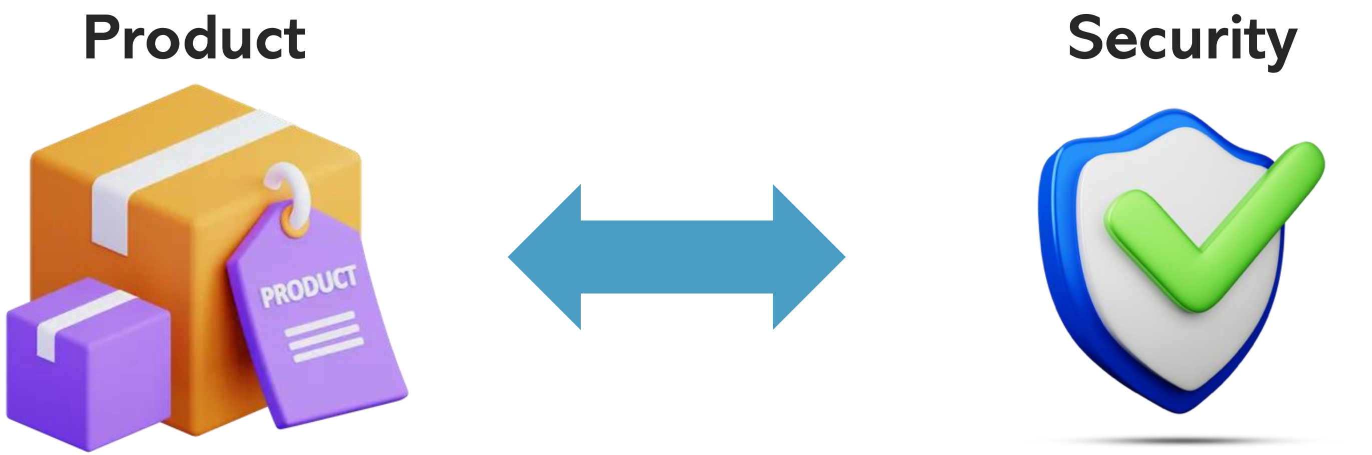
Development
- Secure coding
- Static analysis
- Code Review

Testing
- Security Testing
- Firmware analysis

Deployment
- Secure config
- Automation

Maintenance
- Pen testing
- Vulnerability Management

Why Software Security Testing is Hard?



Product

Security

Why Software Security Testing is Hard?

Product

- Clear requirements

Test what the system should do on expected inputs

Why Software Security Testing is Hard?

Security

- Negative Framing and Constraints
  - Testing for the absence of vulnerabilities
  - Test every possible input

Hard to test **all the ways** an attacker might try **to break the system**

Why Software Security Testing is Hard?

Security

Hardware simulation / Device emulation?

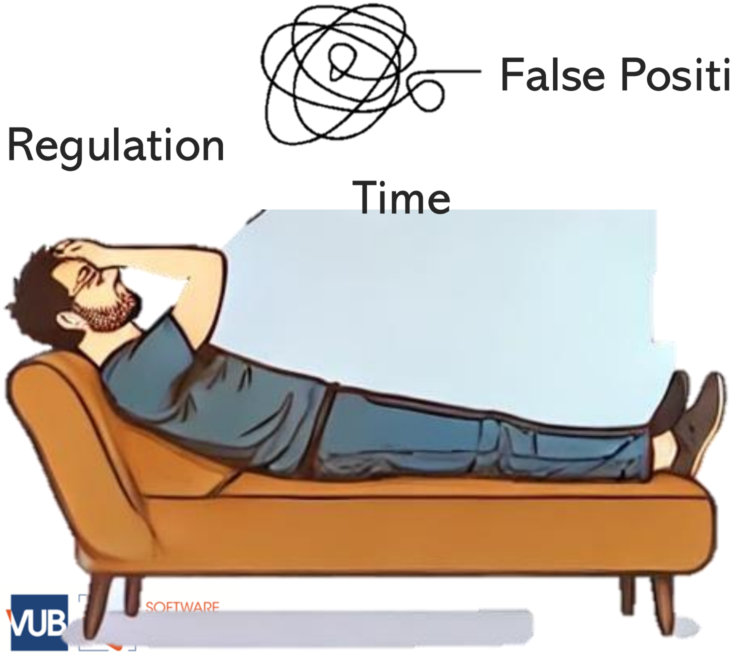
False Positives

Exploitability

Reproducability

Prioritization and Risk Management

Developer Fatigue



Reported bugs

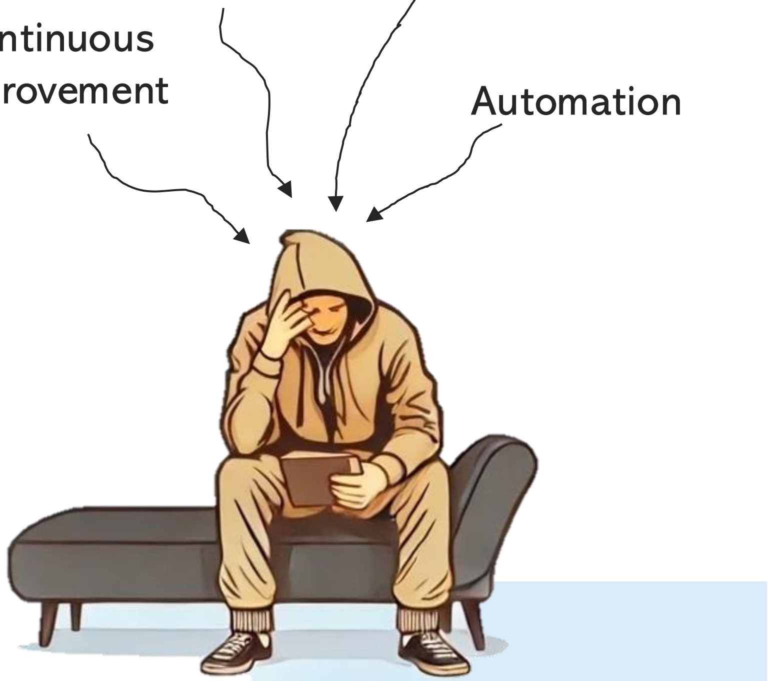
Manual Testing

False Positives

Regulation

Time

Hacker Fatigue



Qualitative Security Testing Tools

Prioritization

Continuous Improvement

Automation