Risk Prediction of IoT Devices Based on Vulnerability Analysis

By: James Baumhardt

IoT Defined

- IoT (Internet of Things) is not a vision or research topic, its reality.
- **IoT Device**: are nonstandard computing hardware such as sensors, actuators or appliances that connect wirelessly to a network and can transmit data.
- Estimated 75 Billion IoT devices by 2025

Problem:

- IoT devices have a growing number of vulnerabilities. A first step toward mitigation is to assess the risk such devices pose to a network.

- 2017 – simple scripts were developed to automate security testing…
  - Scalability and very limited accuracy

- **What is needed:**
  - A new framework that is automated for risk assessment that "can deal with a broad variety of devices and is easily extensible for new devices is needed to cope with the plethora of models and firmware versions, to provide a time-saving, reproducible, and consistent assessment."
  - Also indicates whether a device is likely to create security problems in the future because the manufacturer or model has a history of critical vulnerabilities and patches were not provided in a timely manner.

A Solution

- **European Organization for Nuclear Research (CERN)**
  - A large multinational research organization where thousands of visiting researchers bring IoT devices into the network for research purposes.
  - Framework: ***SAFER*** - Security Assessment Framework for Embedded-device Risks.
- What does ***SAFER*** do?
  - Assesses the security risks of IoT devices and predicts how the security of such devices may evolve in the future with a very high degree of automation.
- 2022

How Does SAFER Work?

1. SAFER tries to automatically infer the IoT's device model and firmware versions.

2. SAFER retrieves and analyzes corresponding firmware images and compares signatures from online data bases like the **National Vulnerability Database (NVD)**.

3. Based on identified vulnerabilities, SAFER determines **current device security risk indicator (CDSRI)**.

4. **Future device security risk indicator (FDSRI)** is calculated from looking at the **NVD** and firmware release notes.

Design of SAFER

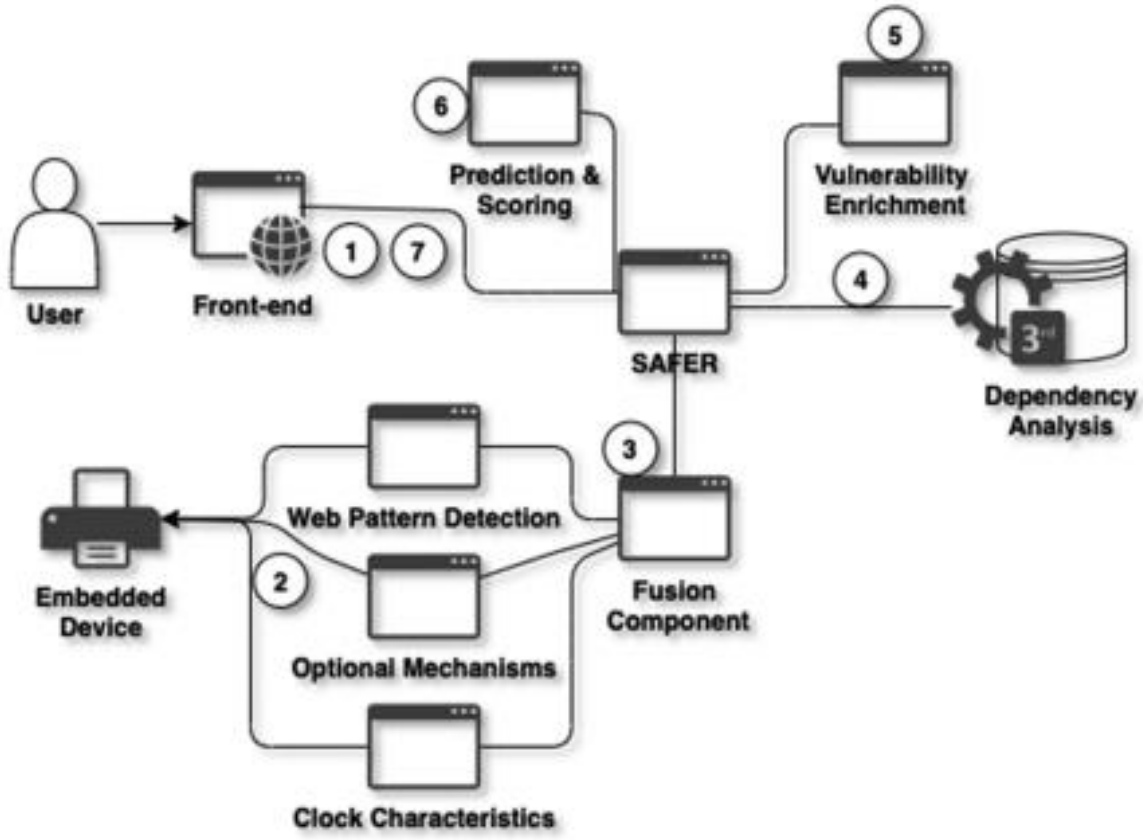

Fig. 1. SAFER consists of different components working together to identify devices, fetch their vulnerabilities and score the results.

Research Methods

- CERN developed and tested SAFER in their environment.

Identification Approaches:

- **CCD Approach**: Clock Characteristics Detection
  - Universal approach to identification mechanisms given broad variety of IoT devices.

- **WPD Approach**: Web Pattern Detection
  - Focuses on IoT web pages

CCD - Clock Characteristics Detection

Table 1. Model and Device Identifications Using CCD

Category	Models	Physical Hosts	Scans
CCTV	12	65	6,675
NAS	16	37	6,816
Printer	13	406	5,853,523
Projector	4	14	1,621
Routers	1	3	56
PLCs	1	11	1056
Streaming	2	26	47,561
Telepresence	4	38	58,141
Oscilloscopes	1	2	144
IP-phones	1	2	196
IP2Serial	1	9	1,684
SOC	1	4	416

Testing:
5,993,052 unique scans, each containing 576 TCP timestamp samples taken over 48 hours – CERN Network

- CCD probes an internal clock of a device over the network using timestamps in TCP.
  - Nearly all IoT devices use TCP for functionality.
  - Assumption - All devices of the same model share the same clock-related characteristics

WPD - Web Pattern Detection

Table 2. Diversity of Detected Device Types Using WPD

Categories	Physical Devices	Manufacturers	Models	Firmware Versions
CCTV	39	6	19	10
KVM-Switch	5	1	1	0
Infoscreen	1	1	1	0
IP-phone	6	5	3	3
IP-to-Serial	18	3	3	2
IP-to-USB	2	1	2	3
IPMI	67	3	6	9
NAS	32	4	5	4
Oscilloscope	16	4	13	18
PLC	71	3	13	15
Printer	97	9	30	47
Projector	23	1	3	0
Router	31	3	3	0
SoC	9	1	1	0
Switch	2	1	2	3
Telepresence	101	3	4	10
Thermometer	6	1	1	0

- WPD uses patterns in the user interfaces of IoT devices, which are typically web pages, to automatically identify the device model and firmware

- HTML pages
- JavaScript snippets
- Hash values

$$fw\_detected = \begin{cases} 0.0, & \text{not detected} \\ 0.4, & \text{detected} \end{cases}$$

$$b(x) = \left(amount\_text\_patterns \cdot \frac{1}{6} + amount\_hashes \cdot 0.3\right) + \left(amount\_config\_patterns \cdot \frac{1}{6} + amount\_config\_patterns \cdot 0.1\right) + fw\_detected$$

$$b(x) = \min\{b(x), 1.0\},$$

Firmware equation

Vulnerability Analysis

- SAFER automates:
  - Obtaining IoT firmware images from vendor websites.
  - Analyzing images to extract vulnerable material
  - Concluding vulnerabilities of the IoT device model (even public vulnerabilities not documented)

Firmware release dates from examination

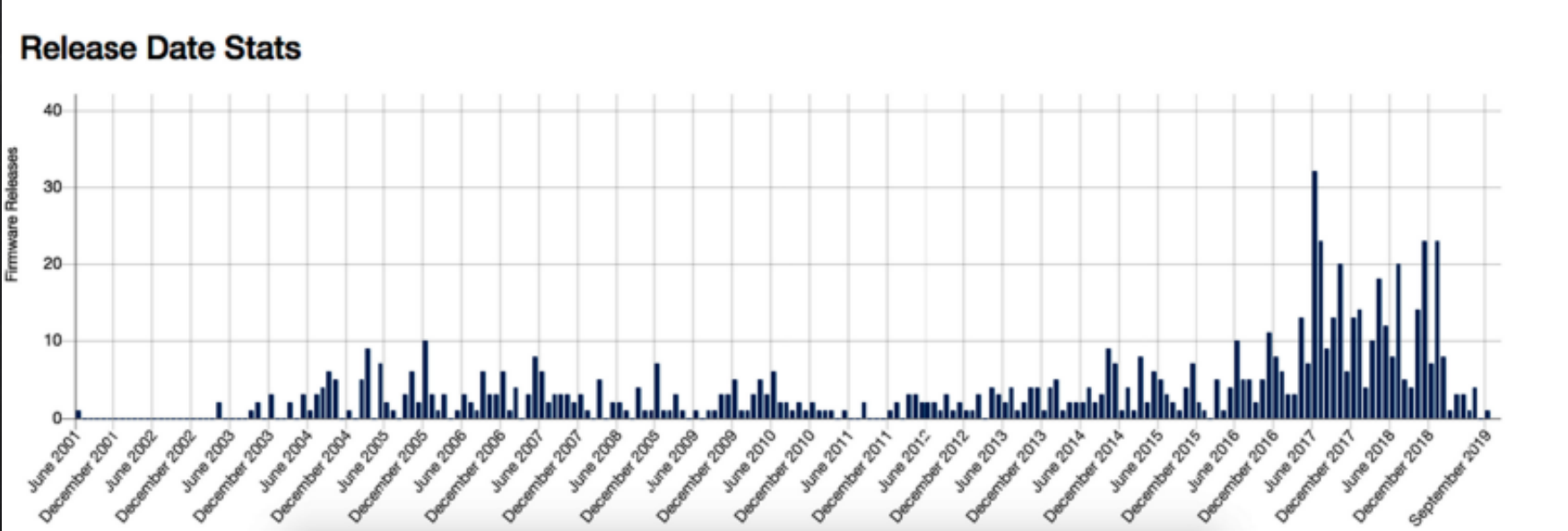

Fig. 3. Release date distribution over all firmware images in the firmware unpacking component.

Risk Metric Overview

- Based on found security vulnerabilities, SAFER assesses the risk of a device by:
  - Calculating **CDSRI** to show users the level of risk that is currently associated with operating the device in the network.
  - Indicating security problems that may arise from the device in the future.

Current Device Security Risk Indicator Scoring

- Uses low, medium, high scoring with CVSS 3.0 – calculated with all unpatched vulnerabilities

$$\text{CDSRI} = \begin{cases} \text{None} & max_{cvss} = 0.0 \\ \text{Low} & 0.1 \leq max_{cvss} \leq 3.9 \\ \text{Medium} & 4.0 \leq max_{cvss} \leq 6.9 \\ \text{High} & 7.0 \leq max_{cvss} \leq 8.9 \\ \text{Critical} & 9.0 \leq max_{cvss} \leq 10.0 \end{cases}$$

CVSS = Common Vulnerability Scoring System

Future Device Security Risk Indicator Scoring

- Calculating future trends:
  - Predict the severity level of potential future vulnerabilities
  - Getting patch times of vulnerability patches published by vendors to get patch trend

$$X^{patch\_time\_spans} = pts_{past} \cup pts_{future}$$

$$pt_{median} = \text{median}\{X^{patch\_time\_spans}\}$$

$$patch\_trend = \begin{cases} \text{Fast} & 0 < pt_{median} \leq c1 \\ \text{Medium} & c1 < pt_{median} \leq c3 \\ \text{Slow} & pt_{median} \geq c3 \end{cases}$$

pt = patch trend

$$X^{vulnerabilities} = v_{past} \cup v_{future}$$

$$vt_{cvss} = \text{median}(X^{vulnerabilities})$$

$$vt = \begin{cases} \text{Low} & 0.0 \leq vt_{cvss} \leq 3.9 \\ \text{Medium} & 4.0 \leq vt_{cvss} \leq 6.9 \\ \text{High} & 7.0 \leq vt_{cvss} \leq 10.0 \end{cases}$$

vt = vulnerability trend

Future Security Scoring Table

Table 4. Future Device Security Risk Indicators

		Patch Trend		
		Fast	**Medium**	**Slow**
Vulnerability Trend	**Low**	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

All Together

The authors shared their results in this table.

Identified that 21 out of 38 checked IoT device models at CERN have a high likelihood to expose critical vulnerabilities to the network.

Example of *SAFER* output given in the paper

Table 5. Assessed Devices of the Organization Grouped by Device Model

Type	CDSRI	Models	VT	Models	PT	Models	FDSRI	Models
CCTV	Low	4	Low	4	Slow	0	Low	4
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	4	High	0
	Critical	0					Critical	0
IP-2-X	Low	1	Low	2	Slow	0	Low	2
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	2	High	0
	Critical	1					Critical	0
IPMI	Low	4	Low	8	Slow	0	Low	8
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	8	High	0
	Critical	4					Critical	0
NAS	Low	3	Low	3	Slow	0	Low	3
	Medium	0	Medium	0	Medium	0	Medium	0
	High	0	High	0	Fast	3	High	0
	Critical	0					Critical	0
Printer	Low	3	Low	15	Slow	0	Low	15
	Medium	0	Medium	0	Medium	15	Medium	0
	High	0	High	0	Fast	0	High	0
	Critical	12					Critical	0
Telepresence	Low	2	Low	4	Slow	0	Low	6
	Medium	0	Medium	2	Medium	1	Medium	0
	High	0	High	0	Fast	5	High	0
	Critical	4					Critical	0

Analysis to Cybersecurity

- This paper describes a new way of looking at IoT devices, not as tools but as vulnerabilities.
- Since IoT devices are relatively new and are growing every year, this subject in cybersecurity should absolutely not be overlooked.
- A device that can connect to a network can lead to the entire network being compromised given the right circumstances.

Pros and Cons of Article

- Pros:
  - Detail Oriented
  - Informative & Progress Based
  - Neatly Organized
  - Graphics + Equations
  - Scalability + Future Work
- Cons:
  - Lengthy
  - Complex Language

Questions

Paper Link

- https://dl.acm.org/doi/pdf/10.1145/3510360
- Authors shown below

Risk Prediction of IoT Devices Based on Vulnerability Analysis

PASCAL OSER, Ulm University and European Organization for Nuclear Research (CERN)
RENS W. VAN DER HEIJDEN, Independent Researcher
STEFAN LÜDERS, European Organization for Nuclear Research (CERN)
FRANK KARGL, Ulm University

ACM Transactions on Privacy and Security, Vol. 25, No. 2, Article 14. Publication date: May 2022.