The 22nd IEEE International Conference on Dependable, Autonomic and Secure Computing

Wiki-IoT: Registering and Evaluating the Security and Resilience of Internet of Things and Connected Devices Using a Collaborative Platform

Track 1. Dependable and Fault-tolerant Computing

Presenter

Jean Decian
jean.decian1@uqac.ca

Fehmi Jaafar
fehmi.jaafar@uqac.ca

Department of Computer Science and Mathematics,
University of Quebec at Chicoutimi, Quebec, Canada

UQAC
Université du Québec
à Chicoutimi

Agenda

- Introduction
- Proposed Tool
- Results
- Discussion
- Conclusion

Introduction

Definition

Physical objects that can connect to other systems via wired and wireless connections

- Smart home devices (e.g., appliances, thermostats, and lights)
- Wearables (e.g., fitness trackers, headphones, and smartwatches)

Numbers

- More than 15.9 billion IoT and Connected Devices in 2023
  - **39.6 billion in 2033 (+149%)***
- Estimated global spending to be $805.7 billion in 2023
  - **$1 trillion in 2026 (+24%)**
- Estimated global market to be $293.2 billion in 2023
  - **$621 billion in 2030 (+112%)**

* latest numbers

Security Challenges

- 98% of all IoT traffic is unencrypted*
- 57% of devices are vulnerable to medium- or high-severity attacks*
- 41% of attacks exploit device vulnerabilities*
- 1 million IoT devices generated 40% of all DDoS traffic**

* Unit 42, 2020 ** Nokia, 2023

Standards

- ETSI EN 303 645 ”Cyber Security for Consumer Internet of Things: Baseline Requirements”
- NIST IR 8425 ”Profile of the IoT Core Baseline for Consumer IoT Products”
- ITU X.1352 ”Security requirements for Internet of things devices and gateways”
- ISO ISO/IEC 27402 ”Cybersecurity — IoT security and privacy — Device baseline requirements”

Regulations

United Kingdom

- Product Security and Telecommunications Infrastructure (PSTI) Regulation came into force in April 2024
- **First country to ban any IoT devices with default passwords**

Labeling Programs and Registry of Certified Devices

UQAC
Université du Québec
à Chicoutimi

Initiated or Planned

- Australia
- Brazil
- Finland
- Germany
- Japan
- Singapore
- South Korea
- United Kingdom
- United States

UQAC
Université du Québec
à Chicoutimi

Complexity of Multiple Labeling Programs

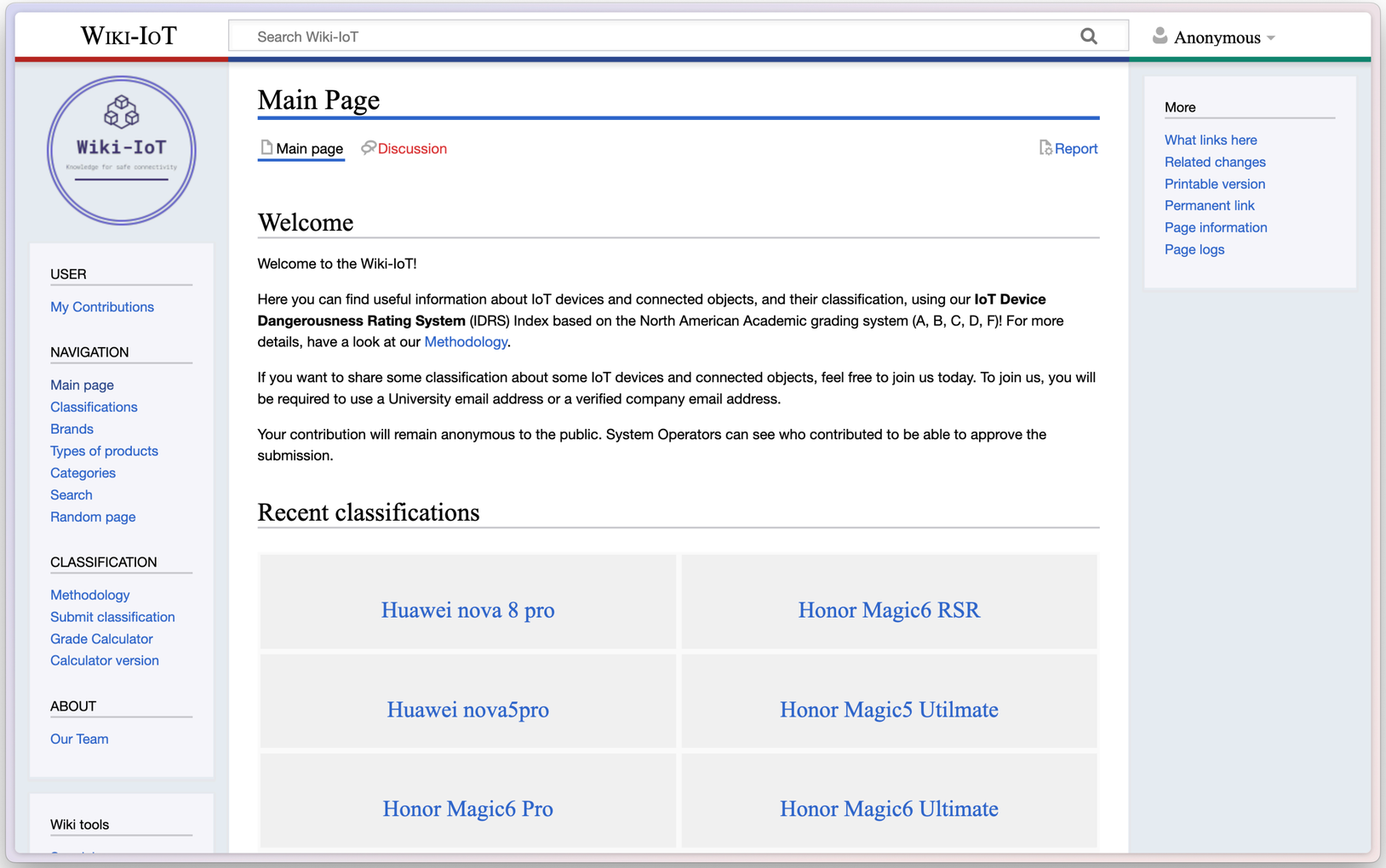
- Most labeling programs refers to the same standard (ETSI EN 303 645)
- Countries sign mutual recognition between their respective programs
  - 3 weeks ago: Singapore and South Korea
- Additional labeling programs adds complexity
- Available information is decentralized in multiple programs

Proposed Tool

MediaWiki

- Powers Wikipedia
  - Familiar to many
  - Easier to use
- Collaborative editing

Wiki-IoT


WIKI-IoT
Search Wiki-IoT
Anonymous
Wiki-IoT
Knowledge for safe connectivity
USER
My Contributions
NAVIGATION
Main page
Classifications
Brands
Types of products
Categories
Search
Random page
CLASSIFICATION
Methodology
Submit classification
Grade Calculator
Calculator version
ABOUT
Our Team
Wiki tools
Main Page
Main page
Discussion
Report
Welcome
Welcome to the Wiki-IoT!
Here you can find useful information about IoT devices and connected objects, and their classification, using our IoT Device Dangerousness Rating System (IDRS) Index based on the North American Academic grading system (A, B, C, D, F)! For more details, have a look at our Methodology.
If you want to share some classification about some IoT devices and connected objects, feel free to join us today. To join us, you will be required to use a University email address or a verified company email address.
Your contribution will remain anonymous to the public. System Operators can see who contributed to be able to approve the submission.
Recent classifications
Huawei nova 8 pro
Honor Magic6 RSR
Huawei nova5pro
Honor Magic5 Utilmate
Honor Magic6 Pro
Honor Magic6 Ultimate
More
What links here
Related changes
Printable version
Permanent link
Page information
Page logs

Evaluation Review

Measures to limit submissions of erroneous data

- Restricted the signup to academic and official domains (e.g., government, corporations, and research centers)
  - Approximately 10,000 allowed domain names
  - Over 1 million possible contributors
- Contributors can submit proofs to support their submission
- Submissions and modifications require manual approval
- Evaluations are timestamped

Evaluation Criteria

12 criteria across 3 categories

Device Security

- Documented Hardware Tampering
- **Documented Vulnerabilities**
- Frequency of Software Updates
- Prior History in IoT Attacks

System Security

- Authentication Measures with Other Systems
- **Communications' Level of Encryption**
- Storage's Level of Encryption

User Authentication

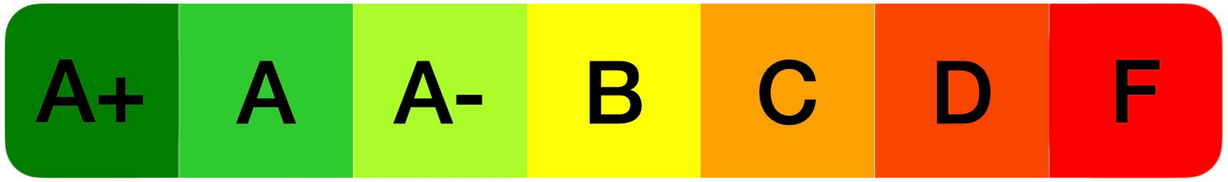
- Account Management Capabilities
- Authentication Measures
- Brute-force Protection
- Event Logging
- **Password Change Requirements After Setup**

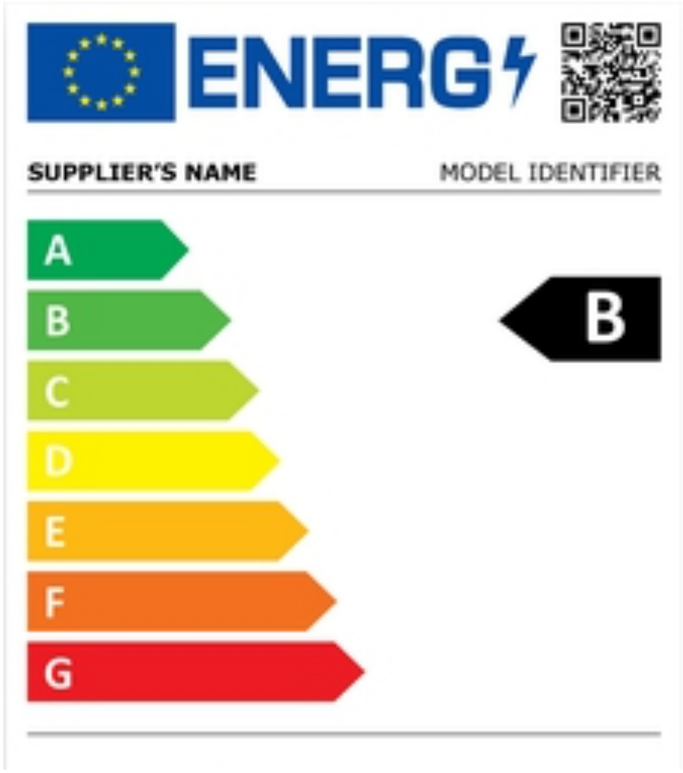
Evaluation Method

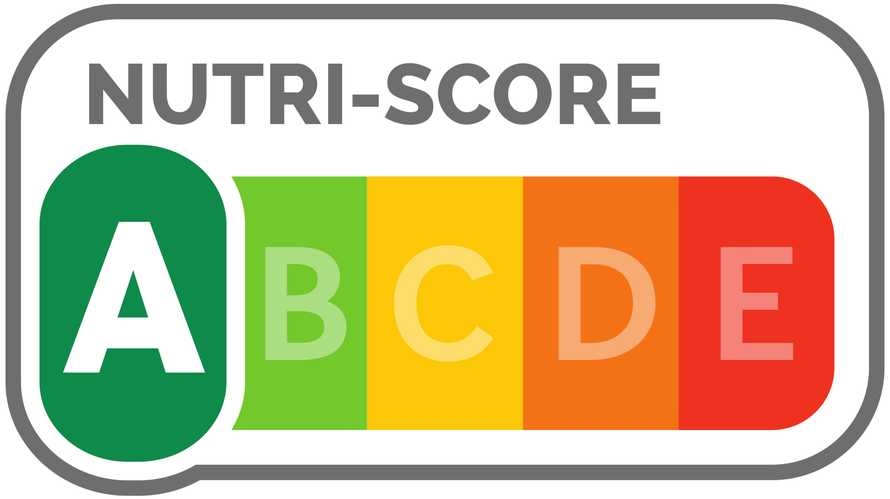
$$\text{Score}_{\text{Grade}} = \sum_{j=1}^{m} \left\lceil \frac{1}{n_j} \sum_{i=1}^{n_j} \text{Score}_{\text{Criterion}_{ij}} \right\rceil \in [0, 2m]$$

- $Score_{Criterion_{ij}}$ is the score for the i-th criterion in the j-th category, ranging from 0 (best) to 2 (worst)
- n_j is the number of criteria in the j-th category
- m is the total number of categories
- $\lceil x \rceil$ denotes the ceiling function, which rounds x up to the nearest integer

Color Coding

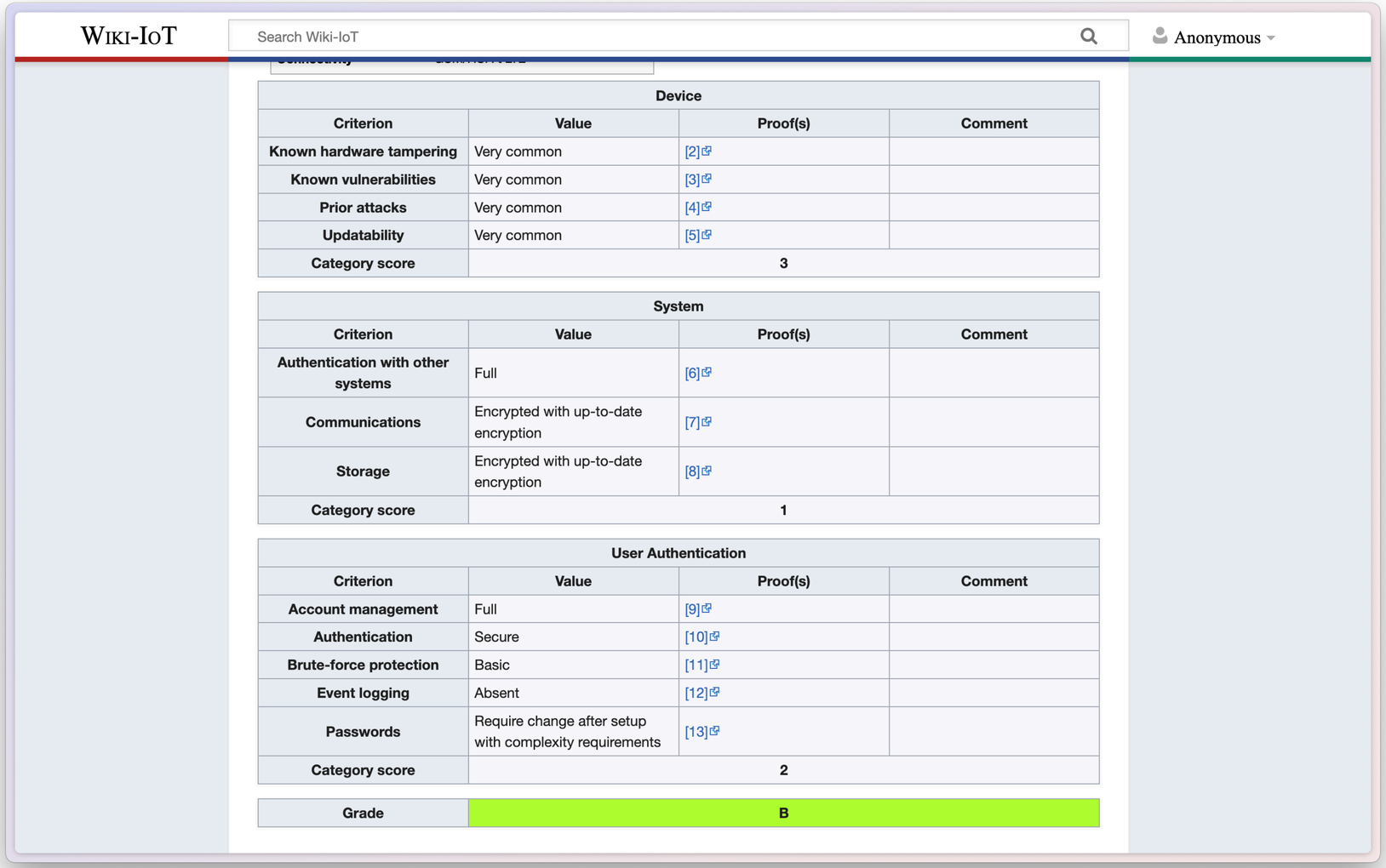






Wiki-IoT

UQAC
Université du Québec
à Chicoutimi



WIKI-IOT

Search Wiki-IoT

Anonymous

Device			
Criterion	**Value**	**Proof(s)**	**Comment**
Known hardware tampering	Very common	[2]	
Known vulnerabilities	Very common	[3]	
Prior attacks	Very common	[4]	
Updatability	Very common	[5]	
Category score	3		

System			
Criterion	**Value**	**Proof(s)**	**Comment**
Authentication with other systems	Full	[6]	
Communications	Encrypted with up-to-date encryption	[7]	
Storage	Encrypted with up-to-date encryption	[8]	
Category score	1		

User Authentication			
Criterion	**Value**	**Proof(s)**	**Comment**
Account management	Full	[9]	
Authentication	Secure	[10]	
Brute-force protection	Basic	[11]	
Event logging	Absent	[12]	
Passwords	Require change after setup with complexity requirements	[13]	
Category score	2		

Grade	**B**

Results

+ 255%

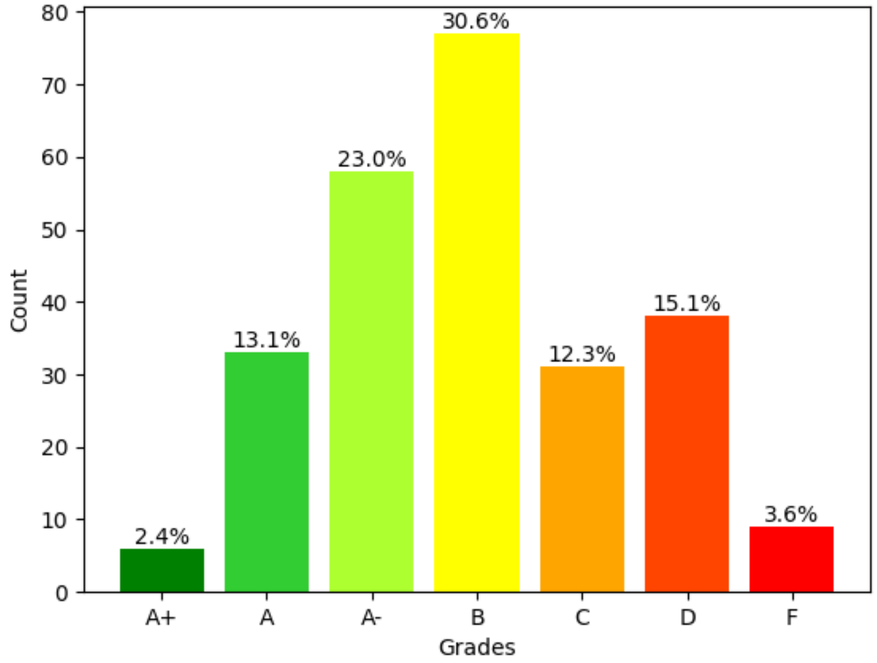
Classifications since July 20th, 2024

UQAC
Université du Québec
à Chicoutimi

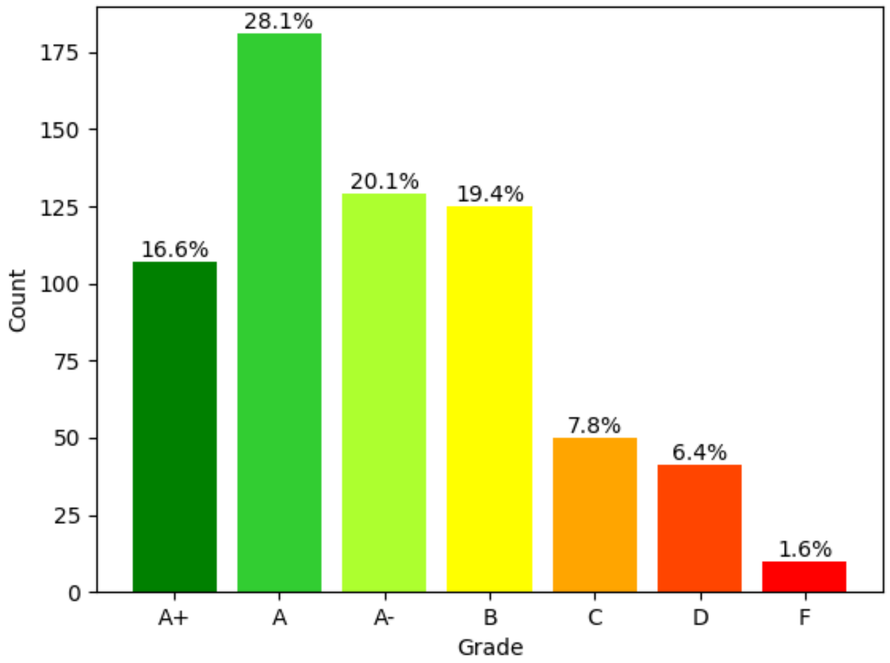
Distribution of grades

Comparison of results

July 20th, 2024



November 2nd, 2024

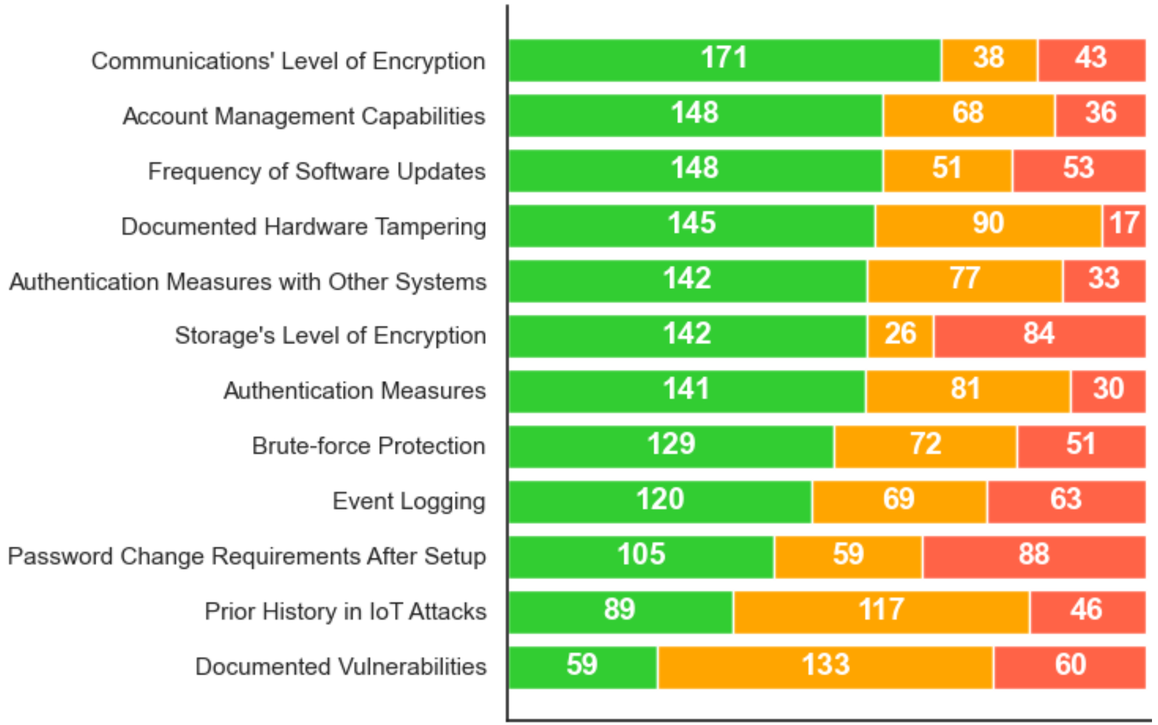


UQAC
Université du Québec
à Chicoutimi

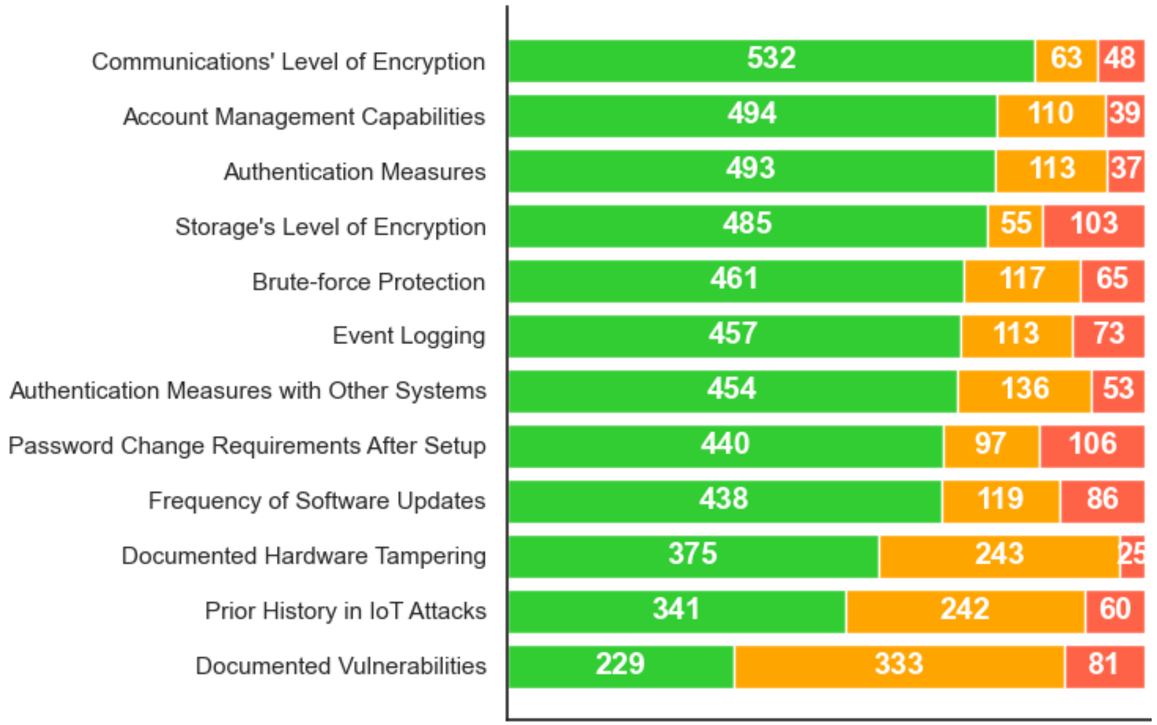
Distribution of count by Criterion Score

Comparison of results

July 20th, 2024



November 2nd, 2024



Discussion

UQAC
Université du Québec
à Chicoutimi

Discussion on criteria

Password Change Requirements After Setup

July 20th, 2024

34.9% doesn’t require password change after setup

November 2nd, 2024

16.5% doesn’t require password change after setup

A study established that more than 13% of devices were configured with factory default root passwords

UQAC
Université du Québec
à Chicoutimi

Discussion on criteria

Communications' Level of Encryption

July 20th, 2024

17% doesn't use encryption

November 2nd, 2024

7.5% doesn't use encryption

Symantec observed in 2015 that 19% of devices communicated without encryption

UQAC
Université du Québec
à Chicoutimi

Discussion on most submitted categories

- Smartphone remains the most submitted category
  - 16.3% (41/252) vs 42.6% (274/643)
- Other most submitted categories:
  - Computer
  - Tablet
  - Smartwatch
  - Camera
  - Earphone

Conclusion

Conclusion and Future Directions

- Answer the challenges posed by different national registries having to sign mutual recognition of their respective labels
- Viable solution as a collaborative labeling registry
- Selected 12 criteria from multiple standards to evaluate an IoT device

Future Directions

- Expand the Criterion Score to have more nuances
  - Currently 0 (best) to 2 (worst)

Platform Availability

Give it a try!

- Available and accessible at https://fehmijaafar.net/wiki-iot/

Thank you!

Questions?

Wiki-IoT