Investigation of IoT Camera Defense

With Emphasis on **Password Vulnerabilities**

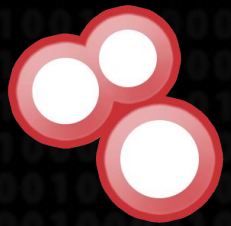
Cyber Key
Madeline Shah

01

Introduction...

Breaching Private Smart Camera Feeds is Simple

Default passwords, weak credentials...



SHODAN

Internet of Things metadata search engine

r/controllablewebcams

Insecam, Camzona

Botnet Creation

Current Policies are Not Working

2018	2019	2020	2021	2025?
California Law (SB-327)	Ring **Breached**	Federal IoT Security Act (Public Law 116-207) Oregon Law (ORS 646A.813)	Verkada **Breached**	

Datasets

01

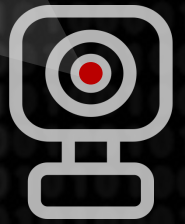
CIC IoT-DIAD 2024 Dataset

- 6 traffic types focusing on credential misuse attacks
- 12 specific camera models

02

InternetDB API - Info on Unique IP Addresses

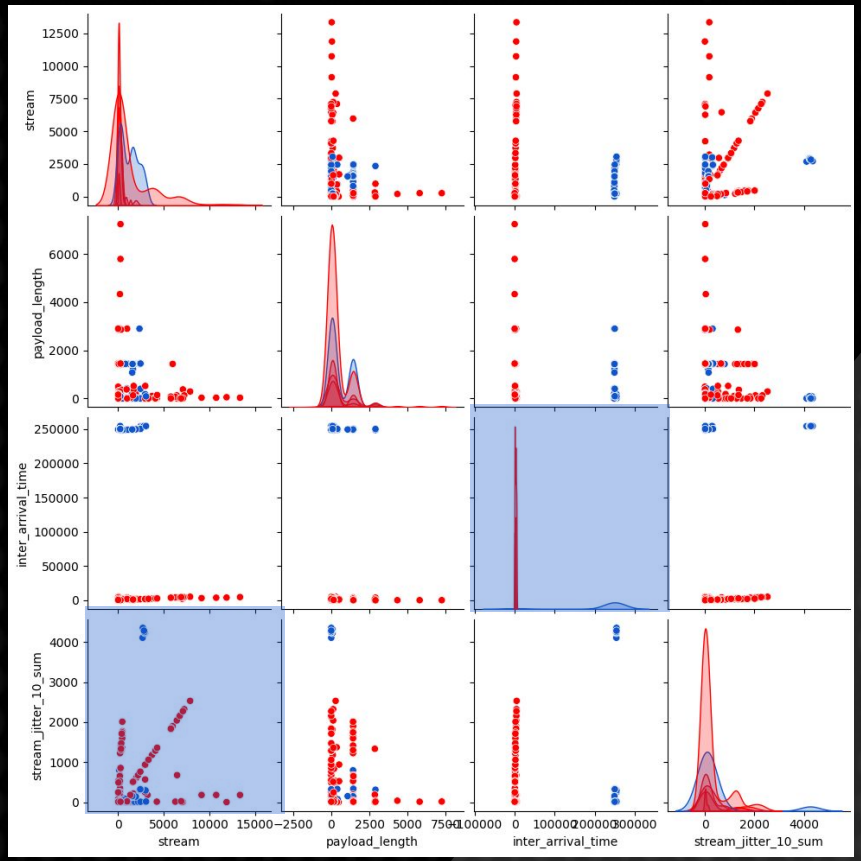
- Open ports
- Known Vulnerabilities
- Associated Services



03

Approach...

*Pairplot: **Brute Force** vs **Other Attacks***



(Small example of many features with this trend)

Approach

Test a “2-Model-System” against the usual “1-Model-System”

Hypothesis: The proposed system will classify all attacks more efficiently

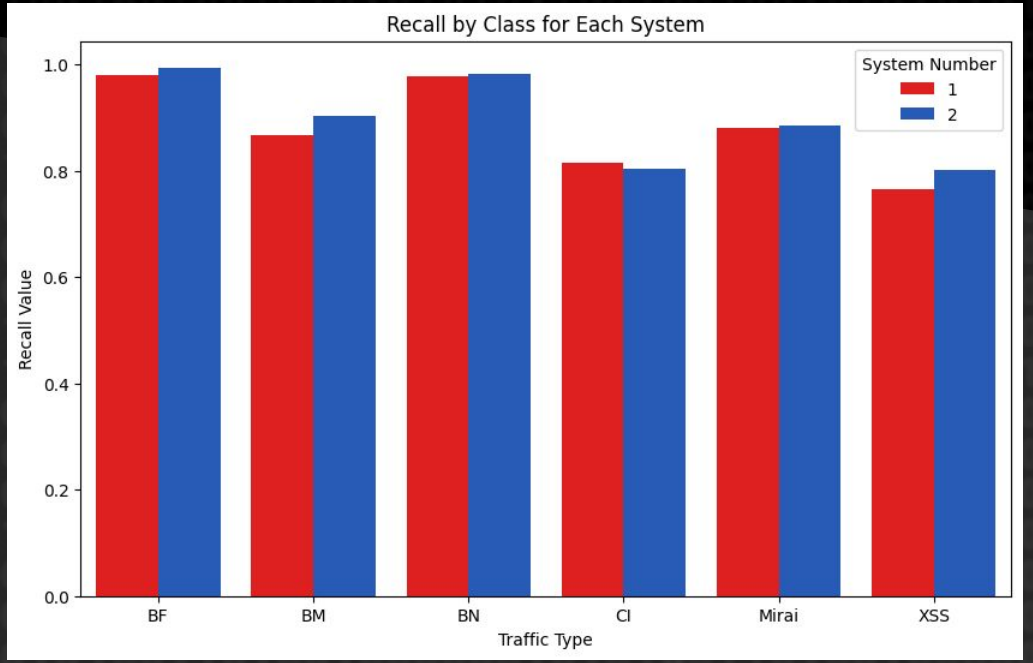
Model Comparison

Recall Scores - *Choosing Models*

System	Random Forest	SVM	Logistic Regression	Decision Trees
1-Model	0.88	-	-	-
2-Model	0.87	0.97	0.97	0.99

note*

Amazon Echo Show and **Arlo Q Indoor** were classified best in both models in ALL performance scores



Significant Vulnerabilities

(p < 0.05)

In Apache HTTP Server (versions 2.4.17 to 2.4.38), allowing access to root

In Apache HTTP Server (versions 2.4.38 and prior), allowing users to authenticate as another user

In Apache HTTP Server (2.2.0 to 2.4.29), allowing replay attacks

Significant Open Ports

(p < 0.05)

Port 10001

P2P live-streaming on some cameras like Wyze

Port 32100

Common for P2P communication for many IoT devices

Port 8080

Might suggest web server traffic, proxy server usage, or testing and development activities

01 Introduction

02 Datasets

03 Approach

04 Analysis

05 Conclusion

05

Conclusion...

Recommendations

Amazon Echo Show

Arlo Q Indoor

Manufacturers

Adequate IDS on all IoT Cameras

Recommend a 2-model system, also keeping in mind the time and space constraints of IoT environments

Manage Open Ports and Vulnerabilities

Close unnecessary ports, prioritize updates and patching, and report to CISA

Policymakers

Enhance Policy Enforcement

Give actual penalties for non-compliance, and allow right of action for affected end-users

Mandate Change of Credentials

Like California Law (SB-327), but for ALL devices

Limitations and Further Analysis

Time

Switching models and use of Random Forests

Application

Further studies can collaborate with companies in implementing on actual IoT devices

Dependency

Second model in 2-model system is dependent on first model

Recall

There may be more false alarms than if precision or f1 were used as the metric of interest

Completed.

Thank you!