An Investigation of Vulnerabilities in Smart Connected Cameras

Joseph Bugeja

Désirée Jönsson

Andreas Jacobsson

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

KK-stiftelsen

verisure
ALARMS WITH IQ

AGENDA

1. Introduction
2. Related Work
3. Research Method
4. Results
5. Reflections
6. Closing Remarks & Future Work

THE INTERNET OF THINGS

- Recent surveys estimate the number of IoT devices to exceed 20 billion by 2020
- In 2017, 98 million network surveillance cameras and 29 million HD CCTV cameras
- Increasingly, homes, offices, and smart living spaces, are being fitted with smart camera systems

SMART CONNECTED CAMERAS

What are the different types of smart cameras that exist in the consumer market?

Different forms

SMART CONNECTED CAMERAS

Do the cameras differ in terms of their usage and features?

Different purposes

Different capabilities

SMART CONNECTED CAMERAS

What is the technical composition of a modern smart connected camera?

Unboxing a smart connected camera

SOME RECENT ATTACKS ON CAMERAS

Are there reported attacks on smart connected cameras?

- In *2014*, over *73,000* private video cameras were found to be streaming live footage over the Internet

SOME RECENT ATTACKS ON CAMERAS

Are there reported attacks on smart connected cameras?

- In *2017*, researchers at *Bitdefender* identified a buffer overflow in over *100,000* Internet-connected cameras
- Their PoC attack allows for calling the “system” function with any attacker command

RESEARCH QUESTIONS

What are the research questions the paper is looking into?

1. What *kind of data* is publically accessible from Internet-connected cameras

data

2. Whether the discovered data can be used to cause *privacy and security risks* in a smart living space

risks

3. Approximate the *number of network-enabled cameras* that can be retrieved and potentially accessed with Shodan

n

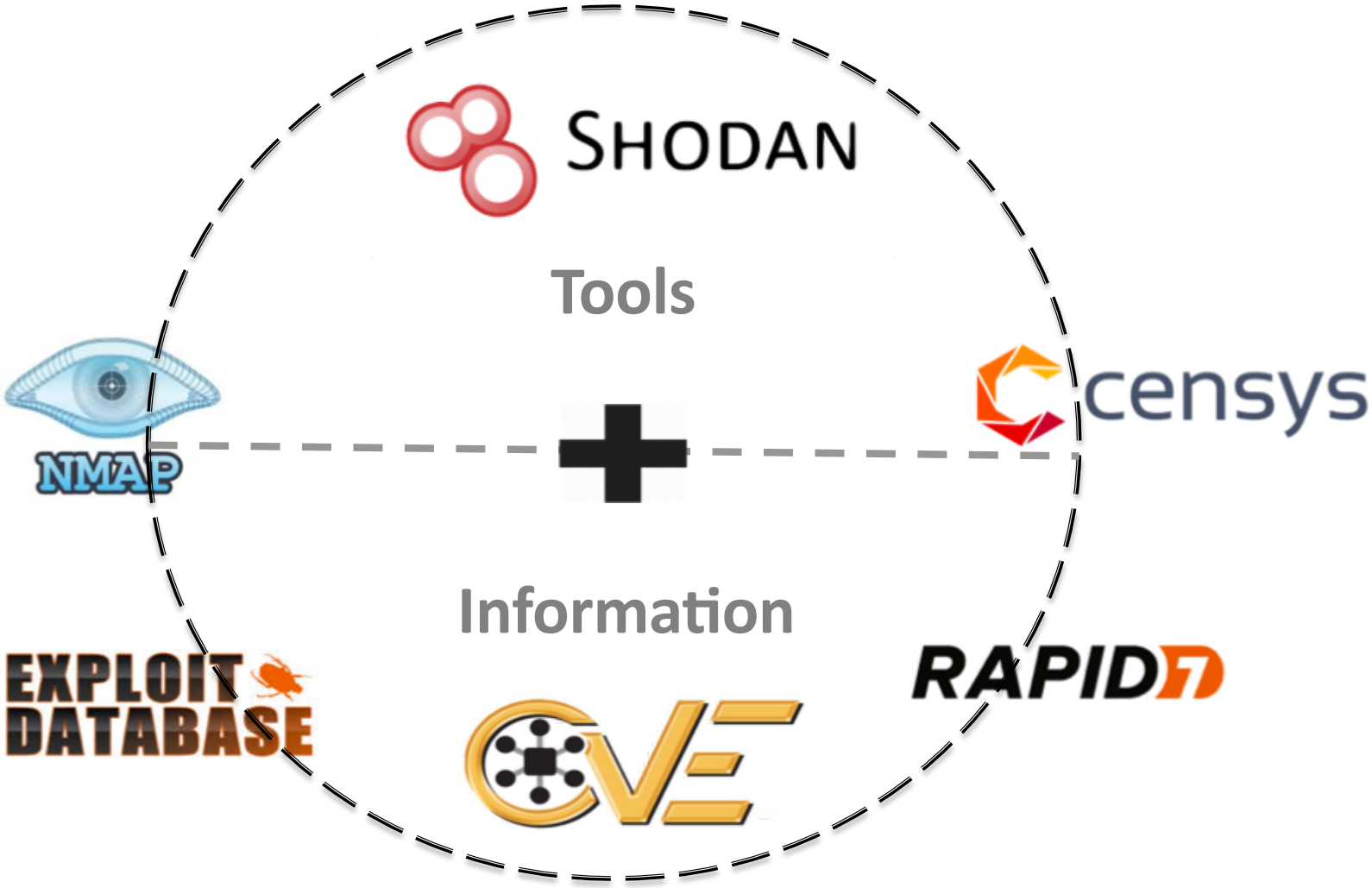
RESEARCH FOCUS

What are the assumptions of this study, that is what is the threat model?

- “Hobby hackers” that include script kiddies, malicious persons, and nosy employees
- Primarily motivated by curiosity
- Tend to use ready-made tools and applications that others develop, and public (Internet) information

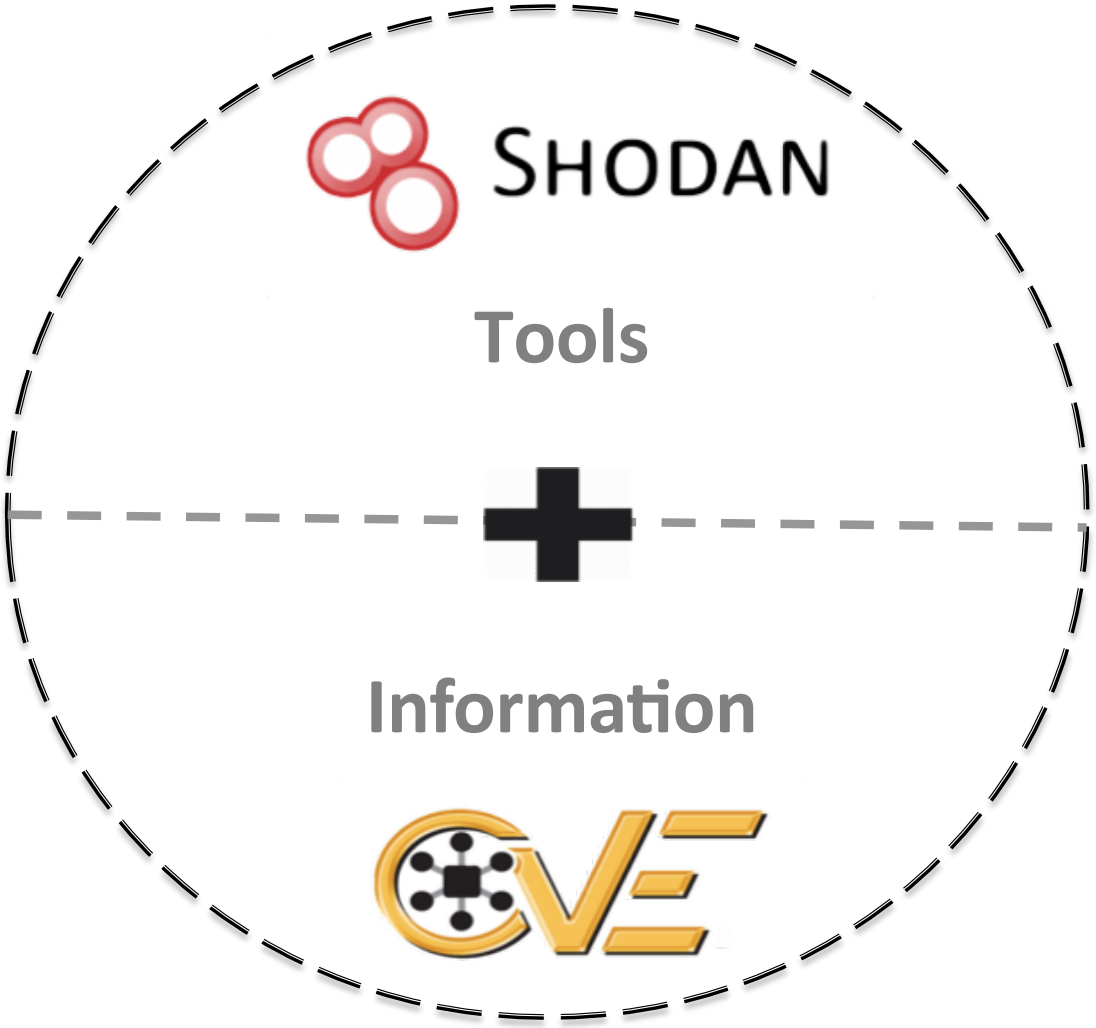
VULNERABILITIES DATABASE AND TOOLS

What vulnerability database and tools can a hacker utilize to conduct reconnaissance?



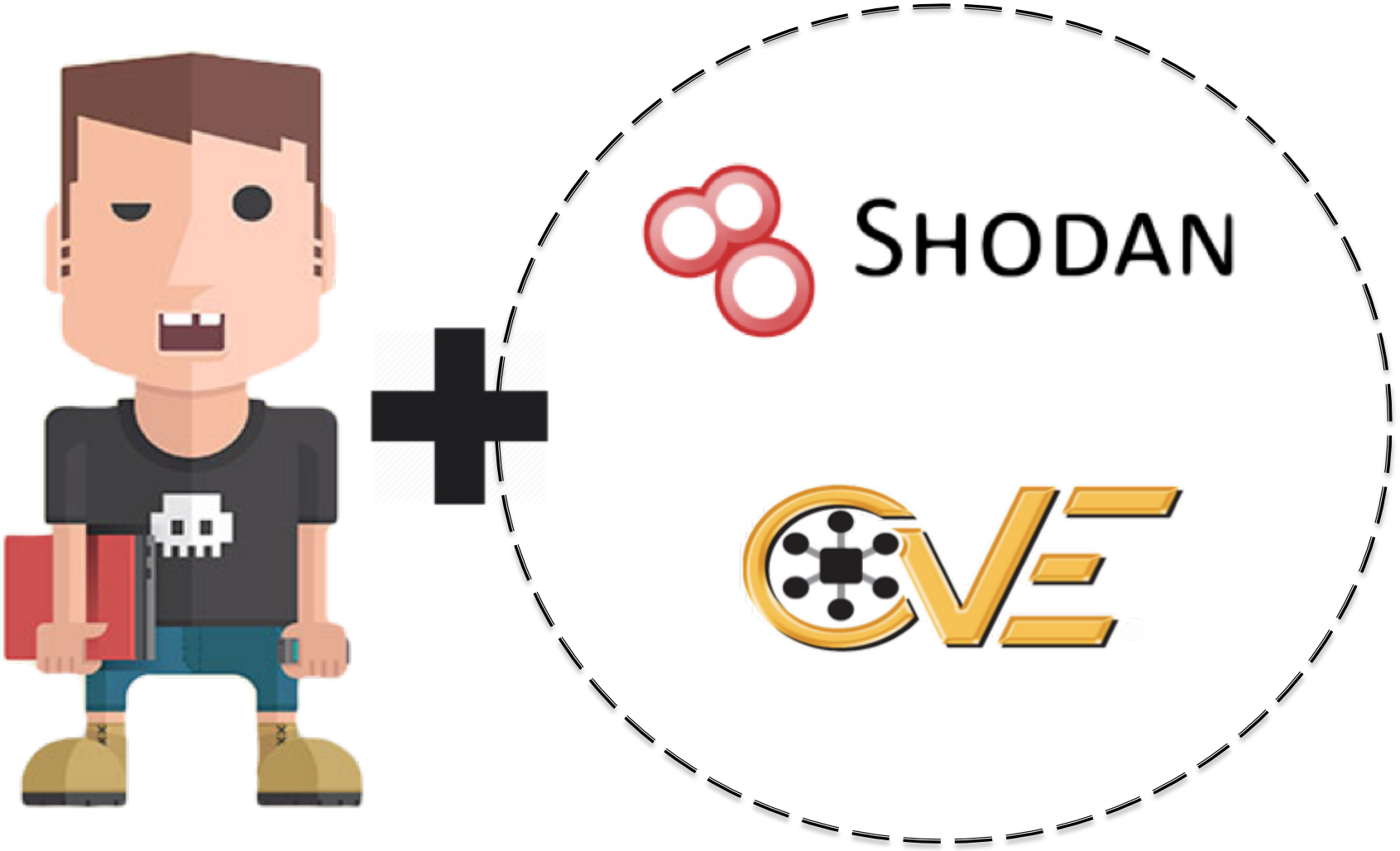
VULNERABILITIES DATABASE AND TOOLS

What tools and information were used to answer our posed questions?



RESEARCH FOCUS

What tools and information were used to answer our posed research questions?



RELATED WORK

- In *2014*, Patton et. al., checked for default passwords against SCADA devices, printers, and health network

- In *2015*, Papp et al., conducted review of existing threats and vulnerabilities in embedded systems

- In *2016*, Moody and Hunter, investigated how hackers can take advantage of weakly protected devices

- In *2017*, Williams et al., performed a large-scale vulnerability assessment of consumer IoT devices

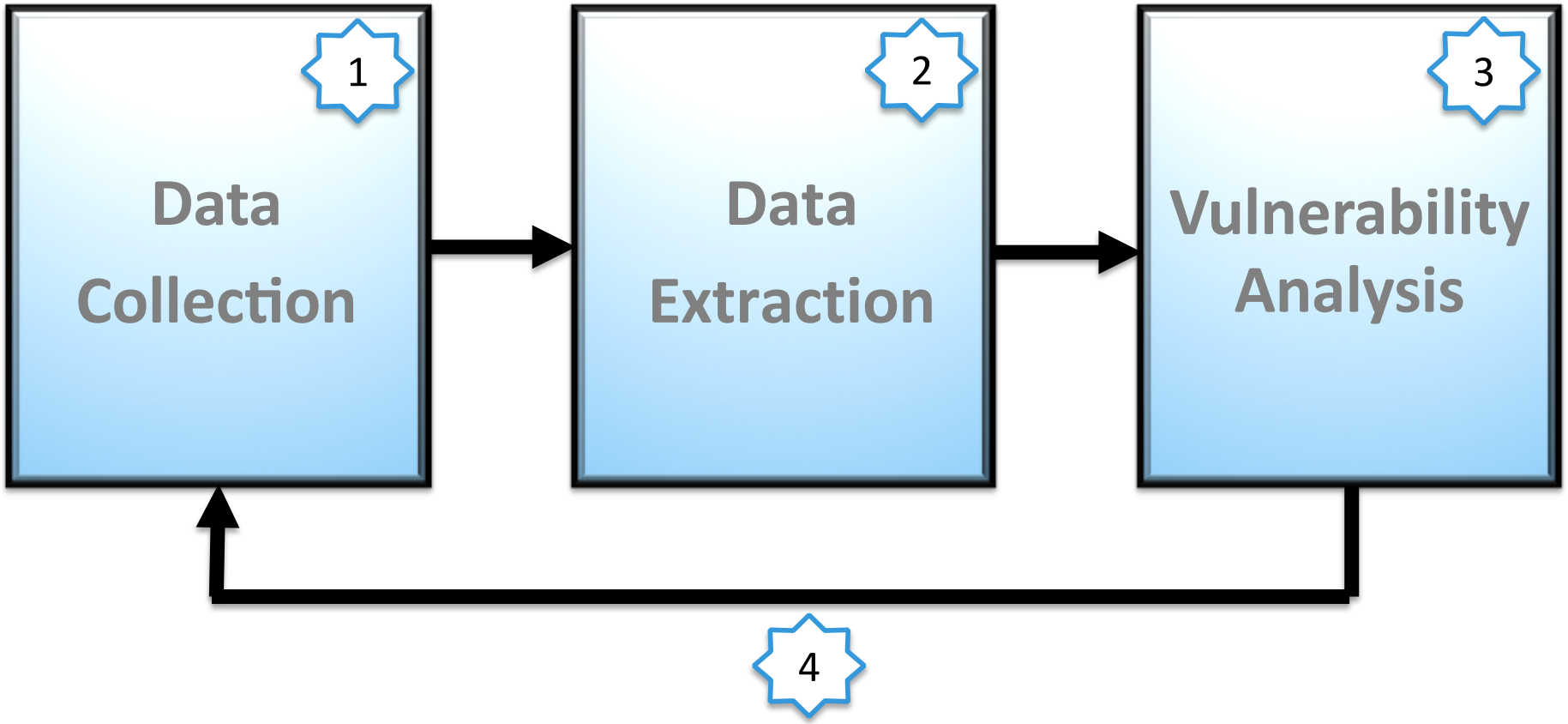
RESEARCH FOCUS

What is the threat model used for answering the posed research questions?

- **Remote**
- **Passive**
- **Smart Connected Cameras**
- **Shodan**
- **CVE**

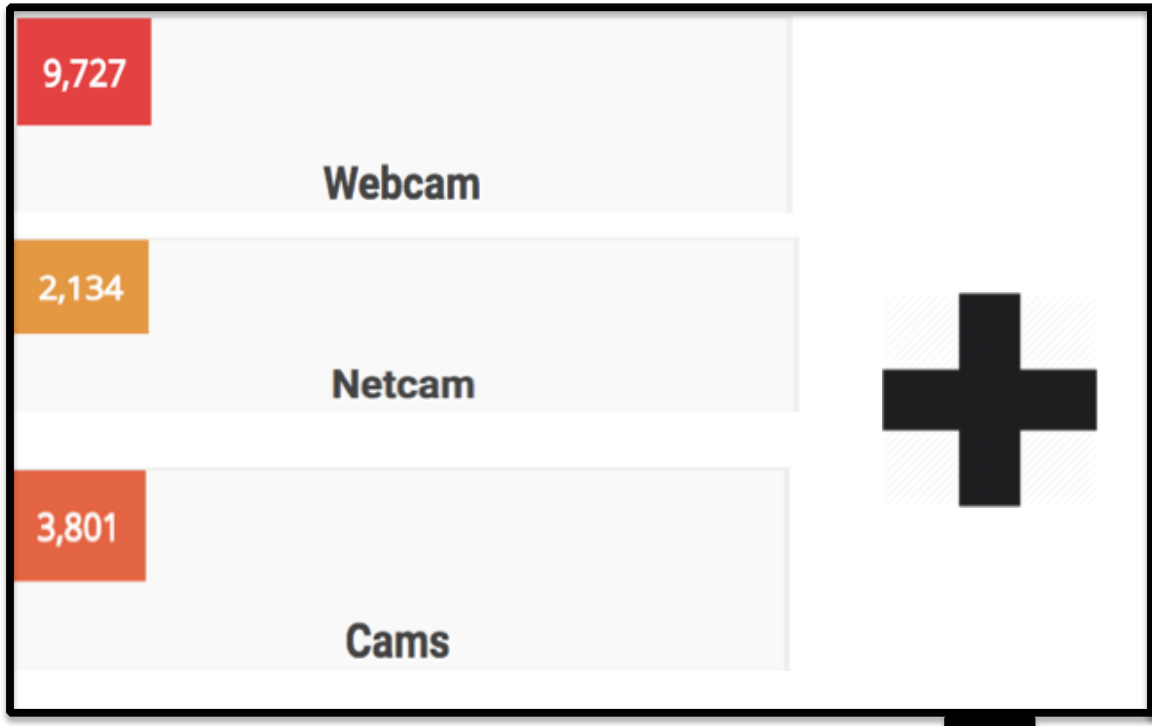
RESEARCH METHOD

What is the adopted research method?



DATA COLLECTION

What comprises the data collection stage?

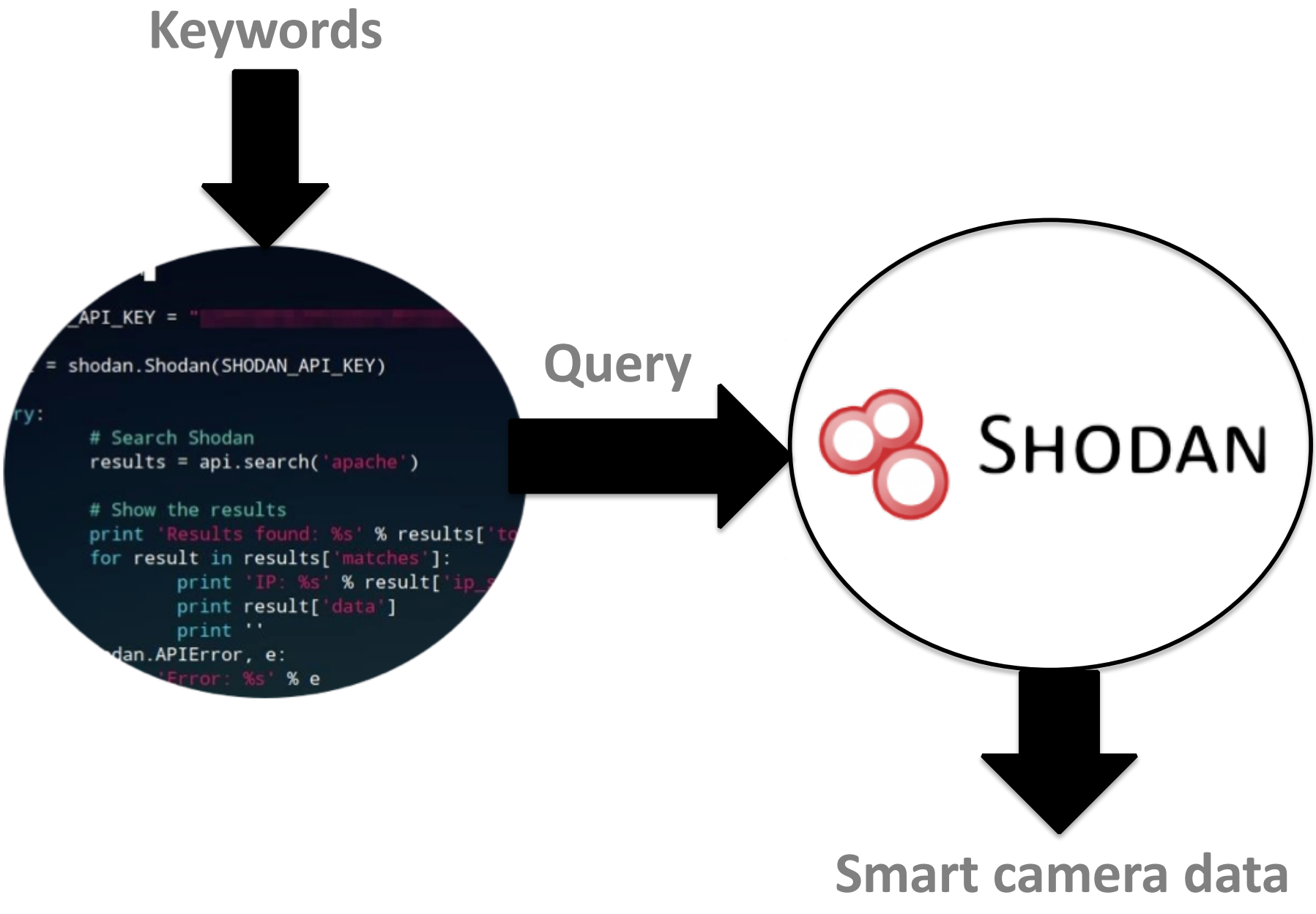


Inspection of documentation, e.g., PT reports, scientific literature, blogs, etc.

Keywords (“search filters”)

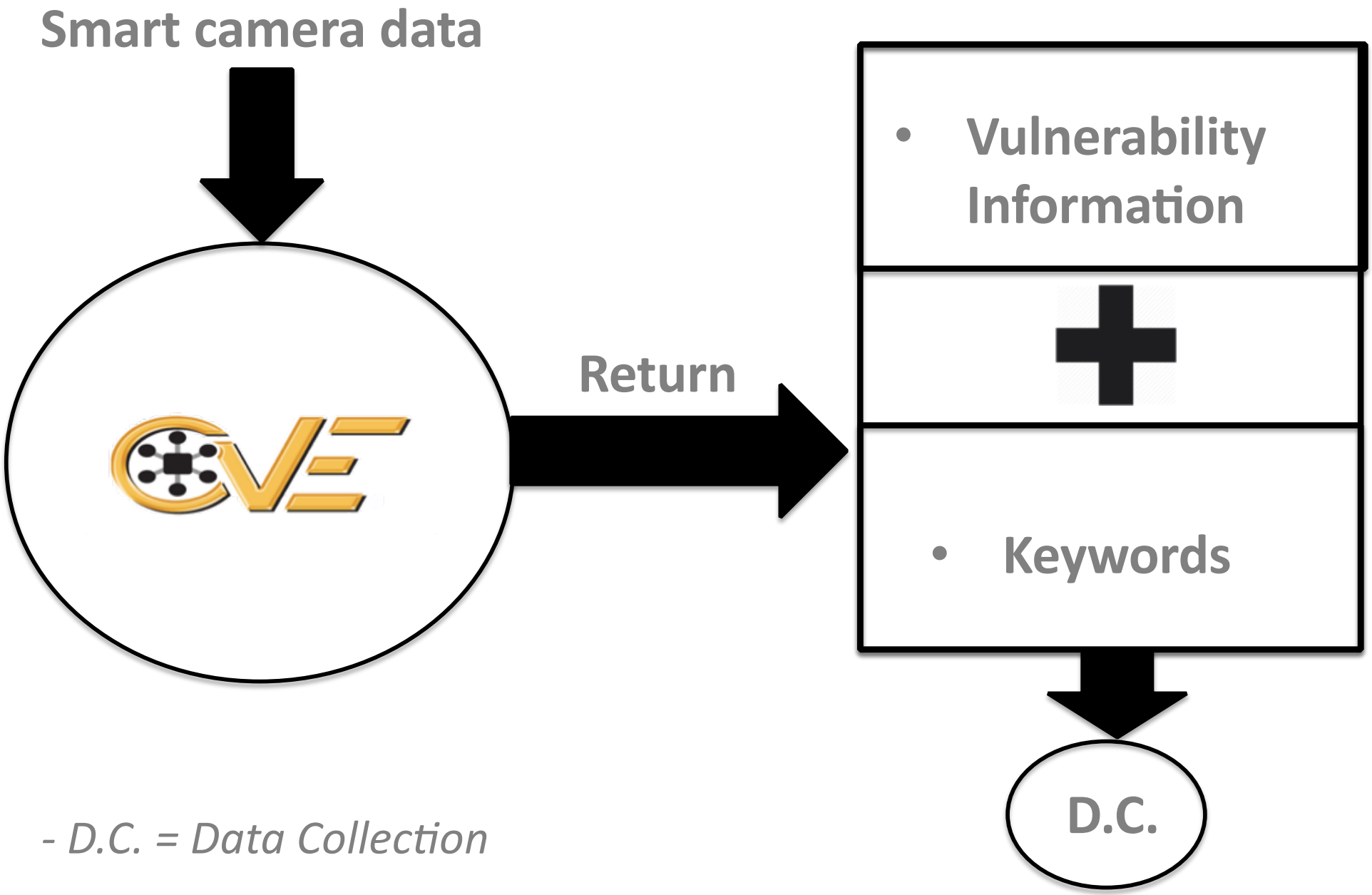
DATA EXTRACTION

What comprises the data extraction stage?



VULNERABILITY ANALYSIS

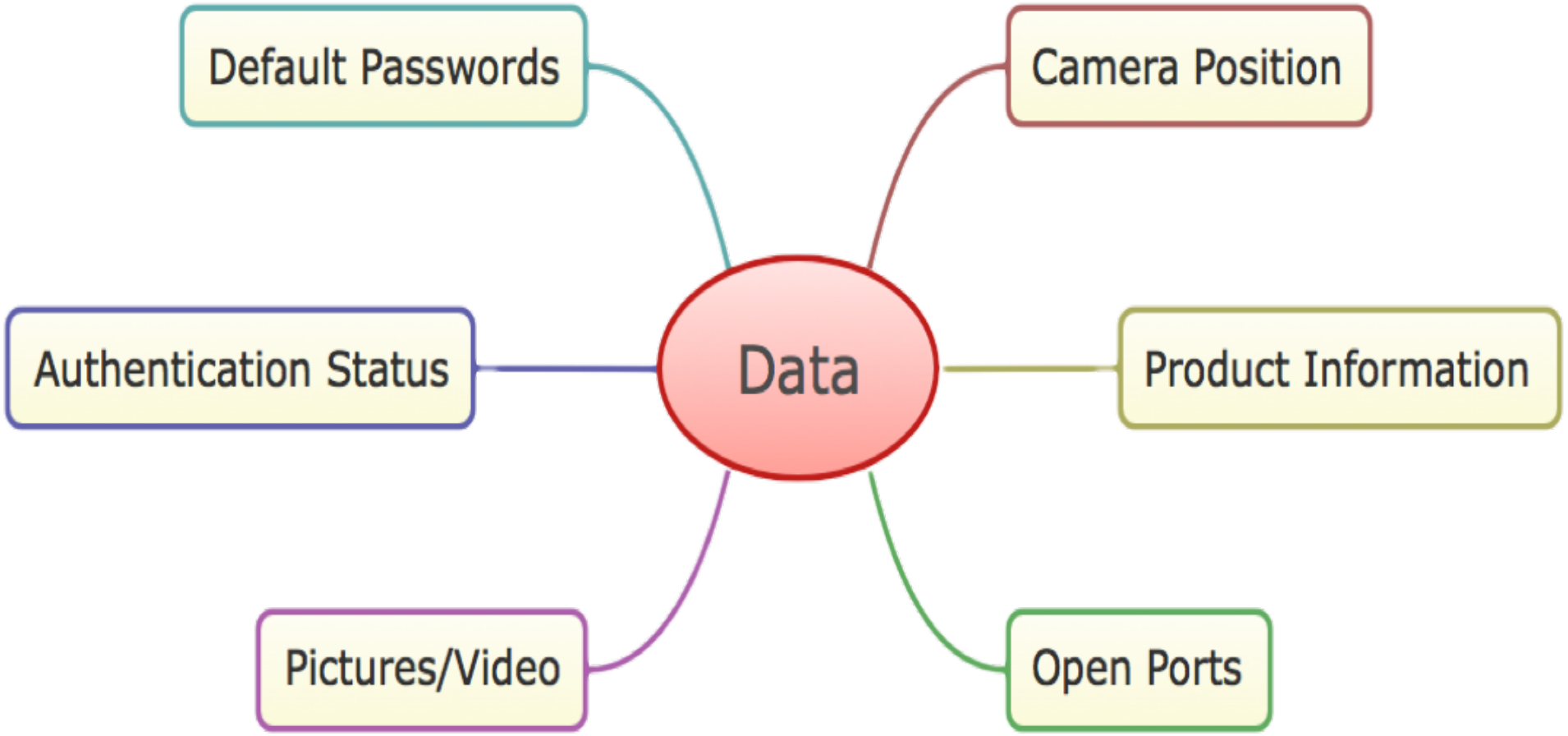
What comprises the vulnerability analysis stage?



- D.C. = Data Collection

RETRIEVED DATA

What *kind of data* is publically accessible from Internet-connected cameras?



RETRIEVED DATA

What *kind of data* is publically accessible from Internet-connected cameras?

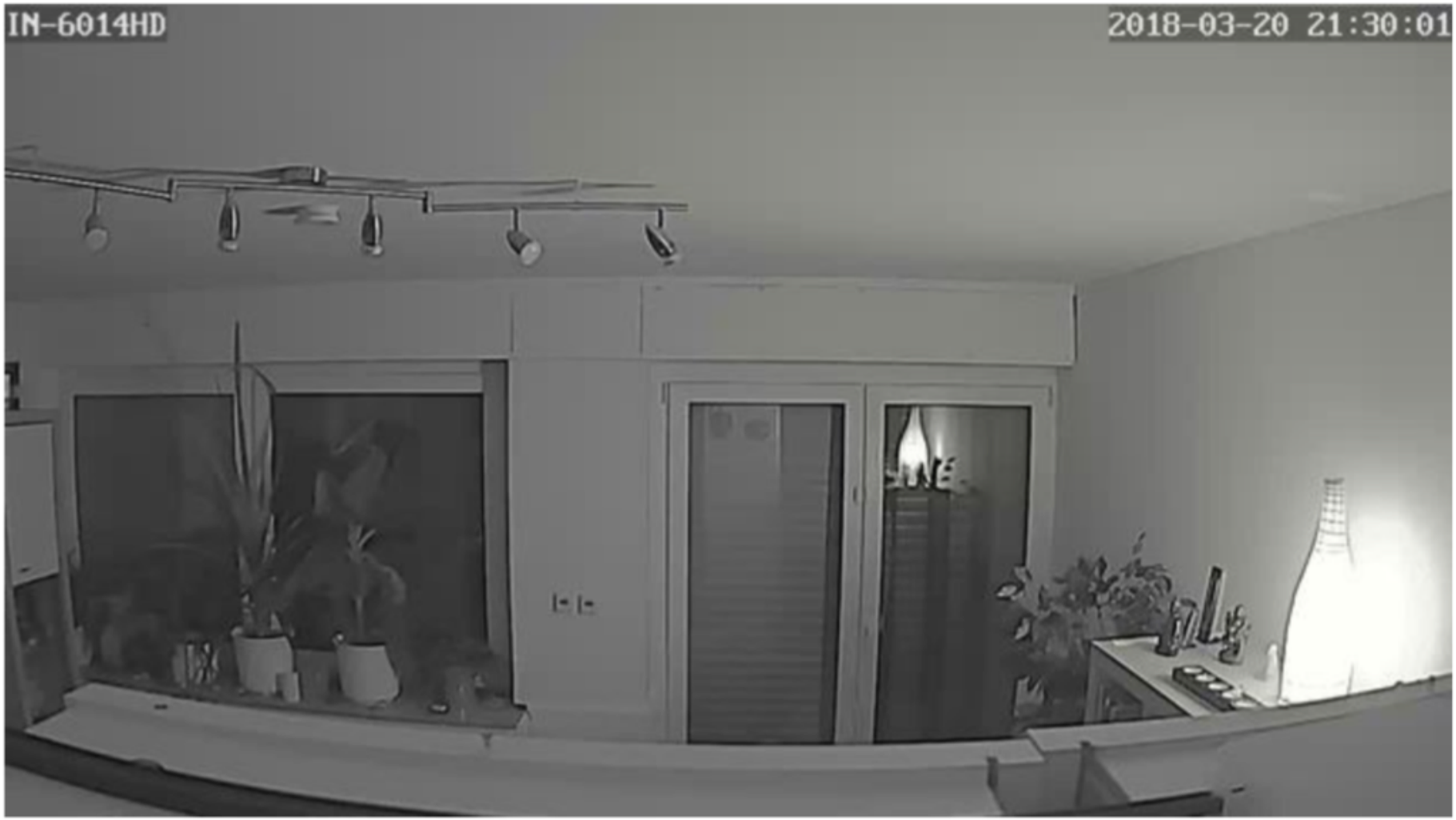
62.[redacted]

Property Name	Value
area_code	null
asn	AS6830
city	Gelsenkirchen
country_code	DE
country_code3	DEU
country_name	Germany
data.0._shodan.crawler	264b5a9d15a64f96a4768e9d8081b
data.0._shodan.id	null
data.0._shodan.module	rtsp-tcp
data.0.data	RTSP/1.0 200 OK CSeq: 1 Server: Hipcam RealServer/V1.0 Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
data.0.domains	['unitymediagroup.de']

ip	1049610876
ip_str	62.143.202.124
isp	Unitymedia
last_update	2018-03-20T19:29:37.676273
latitude	51.5221
longitude	7.0575
org	Unitymedia
os	null
ports	[554]
postal_code	45883
region_code	07

RETRIEVED DATA

What *kind of data* is publically accessible from Internet-connected cameras?



RETRIEVED DATA

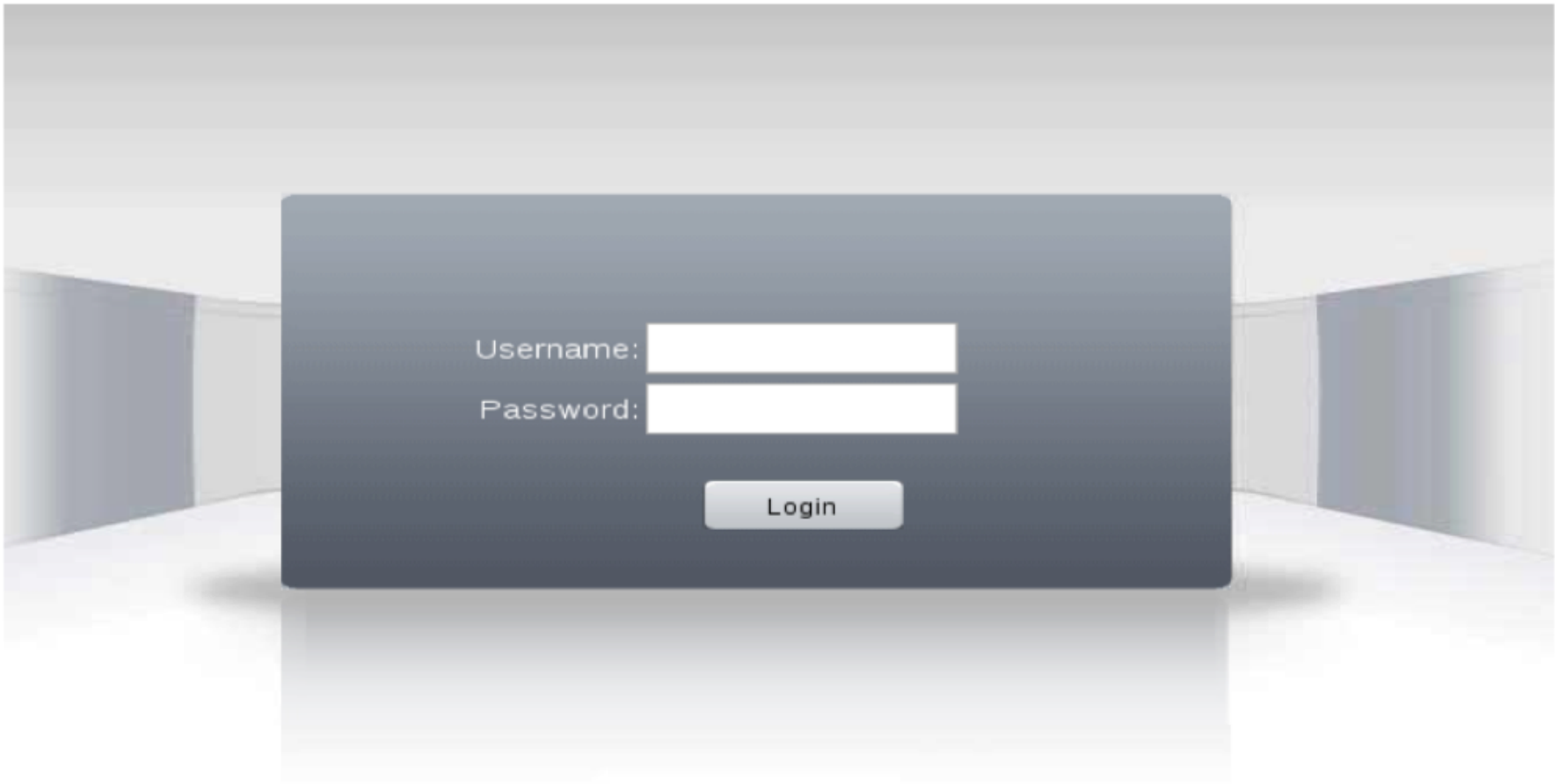
What *kind of data* are obtained from cameras?

Keywords	Number of Hits	Operating System	Top Services
Server: SQ-WEBCAM	151	/	HTTP, NAS Web Interfaces
linux upnp avtech	78,586	Linux 3.x, Linux 2.6.x	HTTP, Kerberos, Qconn
netcam	8,655	Linux 2.4.x	HTTP, Qconn
webcamxp	1,174	Windows 7/8, Windows XP	HTTP, AndroMouse

VULNERABLE SMART CAMERAS

What is the number of network-enabled cameras that can be retrieved and are potentially accessed?

≈ 542,270 devices, mostly IoT security cameras, were running “uc-httpd” (*Nov 2017*)



SECURITY AND PRIVACY VULNERABILITIES

What type of vulnerabilities exist in actual real-life deployments?

Critical

CVE-2015-2887

- Video baby monitor
- Complete compromise of security and privacy

High

CVE-2015-2886
CVE-2007-5213

- Video baby monitor
- Obtain sensitive information
- Perform tasks with full privileges

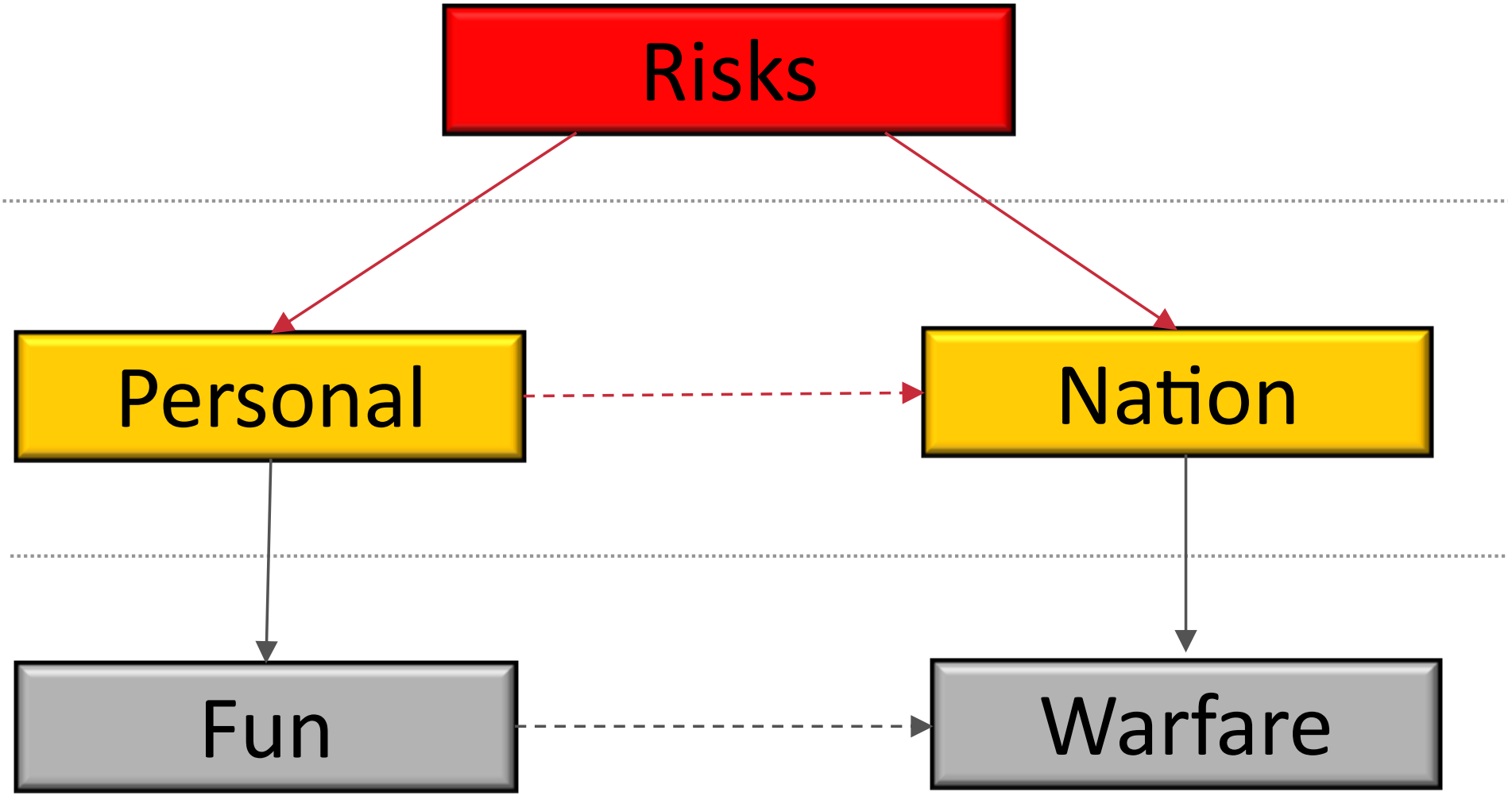
Medium

CVE-2011-5261

- Small business camera
- Unauthorized modification of data

SECURITY AND PRIVACY RISKS

What type of risks exists with smart connected cameras?



OBSERVED ENABLING FACTORS

What are the vulnerabilities the attacks are targeting?

1 **WEAK AUTH/AUTHZ**

- Easily guessable or default passwords, including hard-coded (and privileged) accounts

2 **INSECURE WEB INTERFACES**

- Weak session management, and insecure configurations allowing access to all through RSTP network protocol

3 **UNPATCHED SOFTWARE**

- Devices rarely patched, even though there were (sometimes) available patches

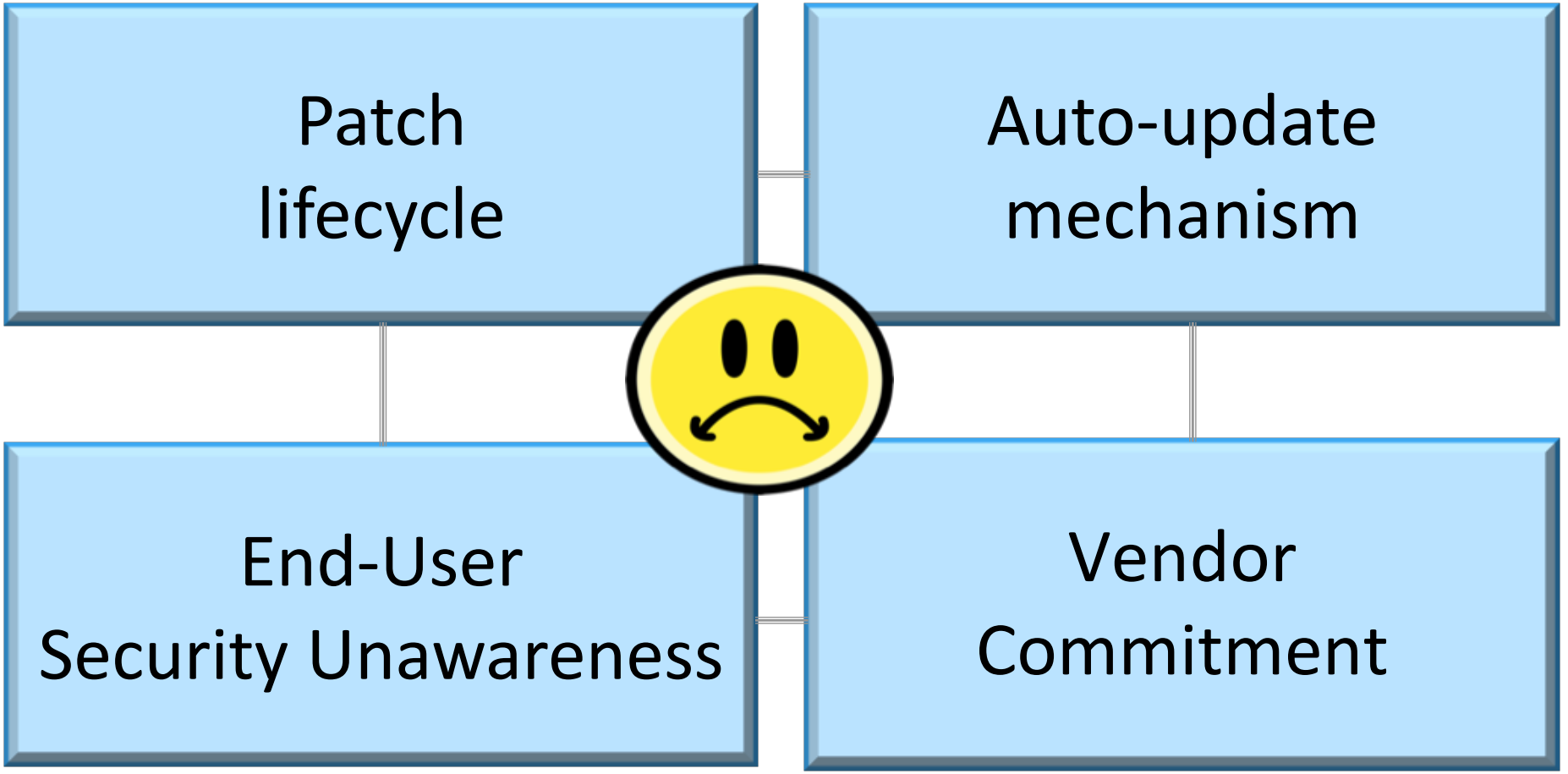
SOME END-USER MITIGATIONS

What can be done to mitigate the observed risks?

1	WEAK AUTH/AUTHZ	• Change default passwords
2	INSECURE WEB INTERFACES	• Disable old (unsupported) and insecure protocols
3	UNPATCHED SOFTWARE	• Update system software/firmware

SOME CHALLENGES

What are the prominent areas where further investigation and effort is required?



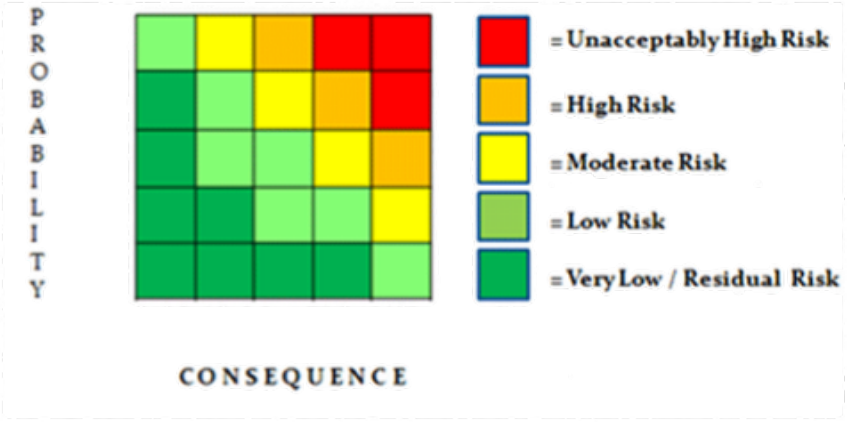
CLOSING REMARKS

- Home and business owners are increasingly relying on smart connected cameras
- Numerous cameras were found to be broadcasting granular data of various kinds
- The data and risks were found using free tools and openly accessible information
- Risks are there but the burden of mitigation is mostly left to the individual user

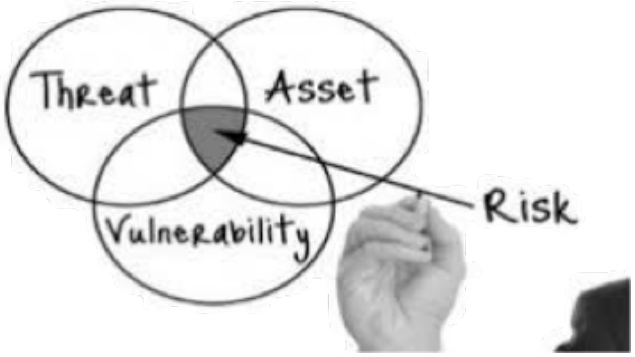
FUTURE WORK

What are possible avenues for future work?

- Extend the study to include other device types



- Classifying and ranking risks



- Designing holistic and effective security measures

Thank you for your attention!

joseph.bugeja@mau.se

@BugejaJoseph

https://www.bugejajoseph.com