IoT Security

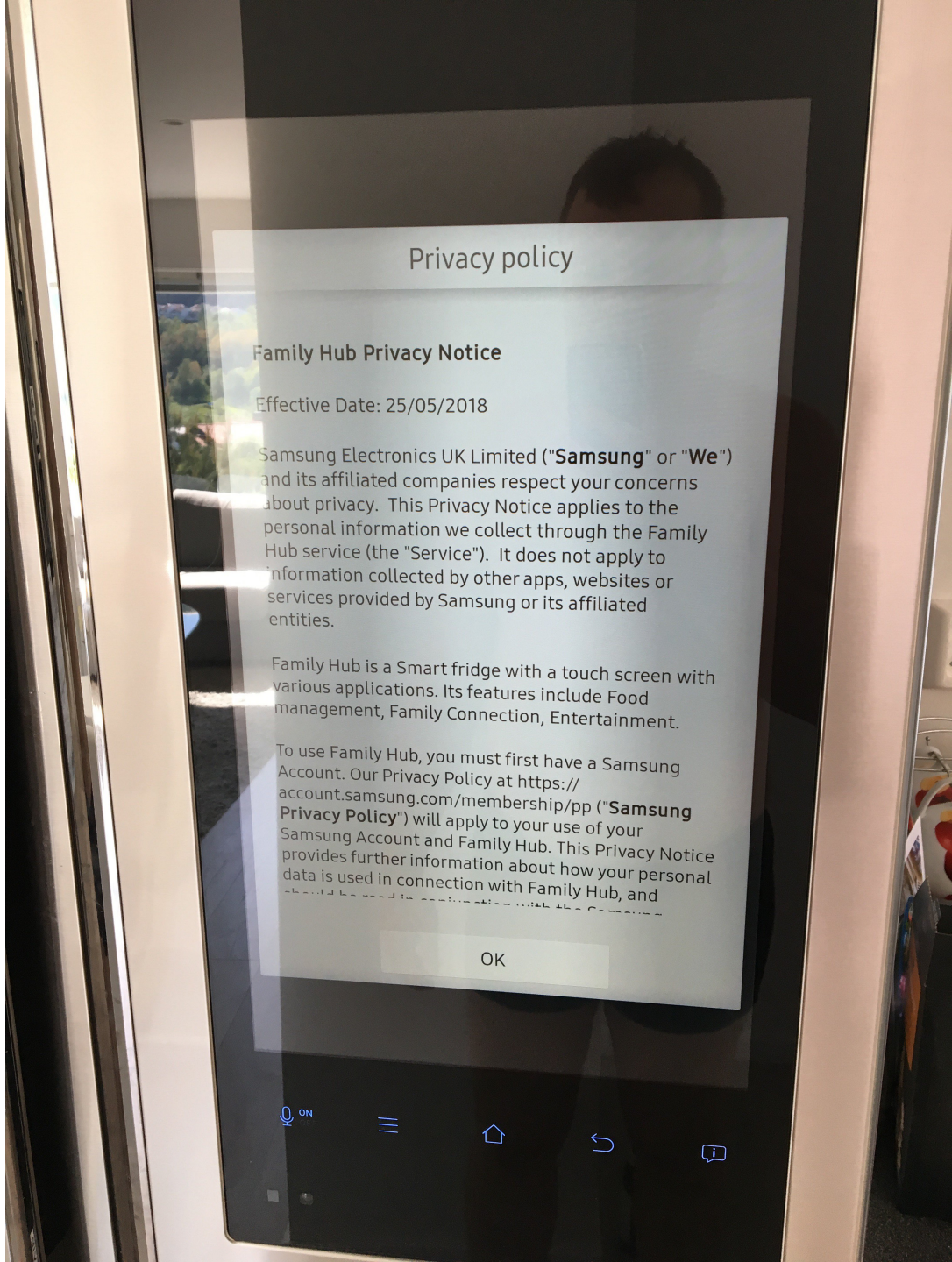
Dr. Viktor Polic

Webster University Geneva

1 June 2018

A fridge and EU GDPR

- Define IoT risk -> Is it a fridge, or is it a “family hub”?
- Potential impact -> Sensors and actuators
- The scope of risk -> Smart nation https://www.smartnation.sg/



From fish tank to a database

- 10 GB database exfiltrated
- video/audio network protocol used over the Internet
- Victim: a casino

Ref: https://www.darktrace.com/resources/wp-global-threat-report-2017.pdf

The most commonly reported (to law enforcement) attacks against critical infrastructures in the EU were DDoS attacks, with over 20% of countries reporting cases. Example: The *WannaCry* attack of May 2017 https://www.europol.europa.eu/iocta/

Examples of cyberattacks leveraging IoT

- Mirai botnet
  - Attack vector: malware exploiting default IoT credentials, weak shell authentication – CCTV cameras, printers, routers
  - Attack weapons: DDoS floods – UDP, DNS amplification, TCP SYN, TCP ACK, GRE, HTTP
  - Attack impact scale: **> 1Tbps DDoS on a single target** company (ISPs – OVH France, Dyn US)
  - Motivation: Financial gain through extortion
  - Follow-up: Justice Department announces charges

https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

Examples of cyberattacks leveraging IoT

- Hajime malware
  - Attack vector: **a worm-class malware** exploiting default or weak IoT credentials, or flow in TR-064 protocol used by ISPs – CCTV cameras, home routers
  - Attack weapons: undetected payload so far but capable of downloading any payload through the encrypted communication
  - Attack impact scale: > 300’000 infected devices by mid 2017
  - Motivation: unclear but FBI started to dismantle the botnet segments

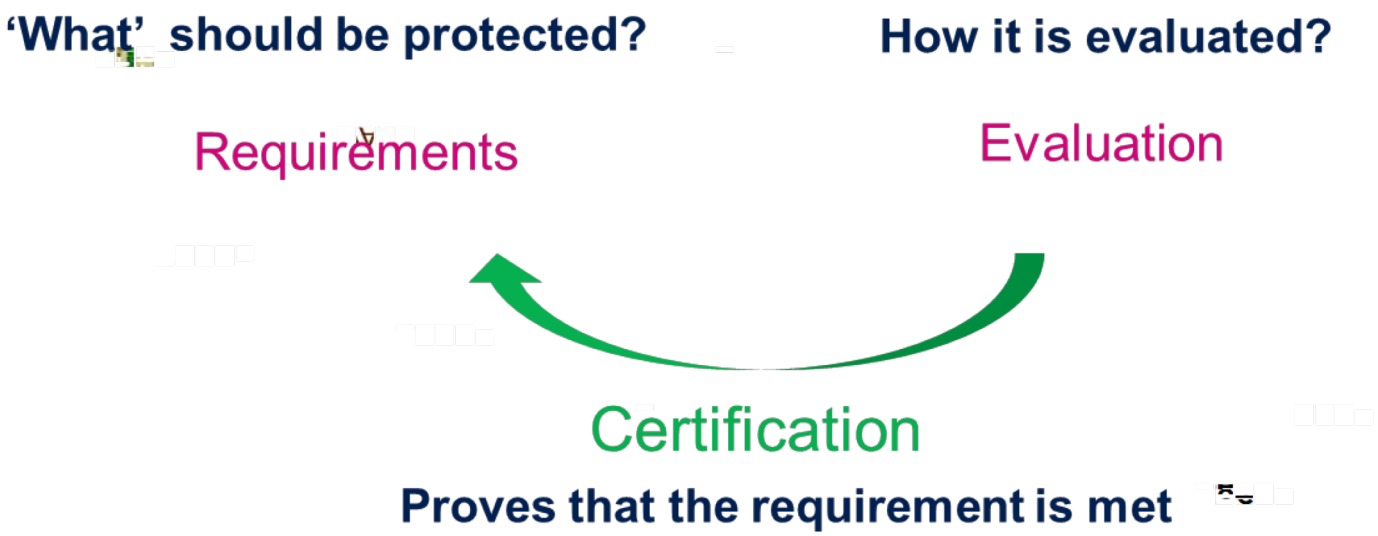
Examples of cyberattacks leveraging IoT

- Hide’n’Seek malware
  - Attack vector: a worm-class malware exploiting default and weak IoT credentials – CCTV cameras
  - Attack weapons: undetected but could be downloaded any moment
  - Attack impact scale: > 90’000 infected devices from January to May 2018
  - Motivation: unknown
  - Particularity:
    - **peer-to-peer communication** rather than star-shaped communication to command-and-control server
    - **Persistence** – can survive device restart


Shodan
Scanhub
Developers
View All...
"default password"
Search
Total Results: 77,425
Top Services
Telnet 20,435
HTTP (8080) 14,672
8081 8,934
Automated Tank Gauge 7,851
HTTP 1,781
Top Countries
TW 11,587
US 8,927
BR 7,561
CN 4,545
TH 2,900
Top Organizations
AboveNet Communica... 4,359
Digital United 3,914
TOT 3,039
Wimax - ZTE New Area 1,005
Telecom Argentina S.A. 593
Island
Sverige
Suomi
Norge
Россия
Danmark
United Kingdom
Беларусь
Deutschland
Україна
France
Қазақстан
Монгол Улс
România
Italia
España
Ελλάδα
Türkiye
O'zbekiston
Тоҷикистон
中国
Pakistan
India
Nepal
Myanmar (Burma)
Việt Nam
Philippines
Sri Lanka
Maldives
Malaysia
Indonesia
Mali
Niger
Tchad
Sénégal
Nigeria
Ghana
Cameroun
Cameroon
South Sudan
Ethiopia
Kenya
République Démocratique du Congo
Tanzania
Angola
Zimbabwe
Botswana
South Africa
Madagascar
Venezuela
Colombia
Ecuador
Perú
Brasil
Bolivia
Paraguay
Uruguay
Argentina
Chile
Australia
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
Arabian Sea
SHODAN MAPS

IoT risk mitigation - globally

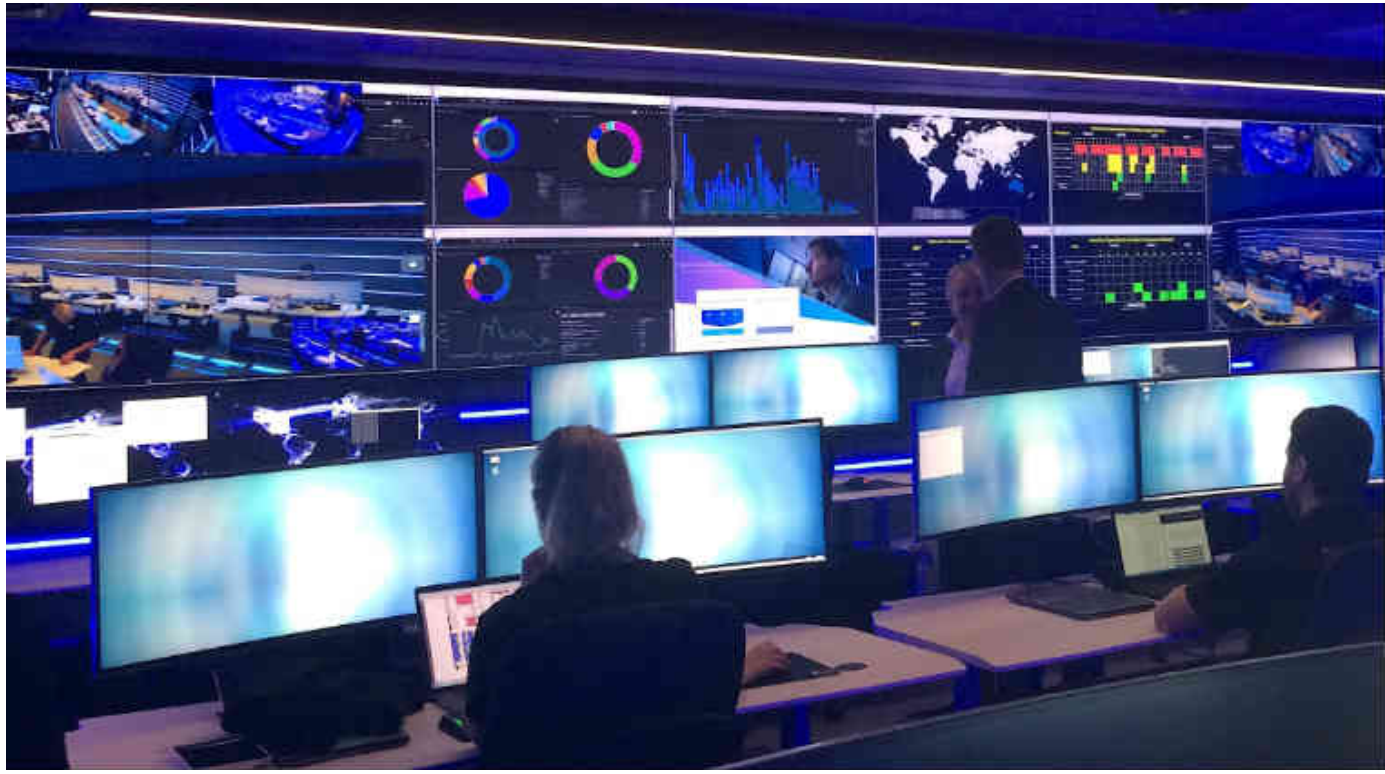
- Regulation - Standards, evaluation, certification



https://aioti.eu/wp-content/uploads/2018/05/AIOTI_Position_on_Cybersecurity_Act_180503.pdf

IoT risk mitigation - globally

- Organized collaborative response
- Industry specific Computer Emergency Response Teams (CERT)



IoT risk mitigation – at organizational level

- Assess and monitor external IoT footprint with tools such as Shodan
- Monitor internally for shadow IoT (non-compliant devices)
- Segregate network segments with different security levels
- Perform continuous vulnerability scanning and management
- Establish internal Computer Emergency Response and exchange threat intelligence
- Maintain high information security hygiene
- Raise risk awareness and educate people in information security

Q&A

Dr. Viktor Polic

https://cybersymbiosis.com

@ViktorPolic