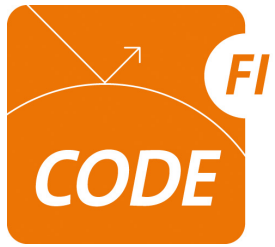
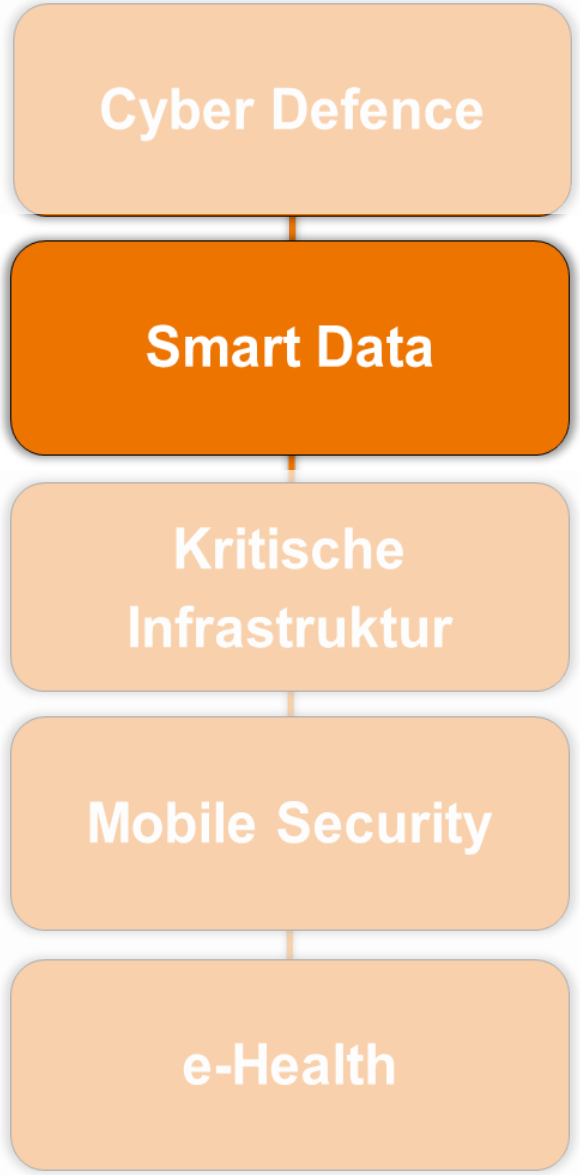
Cybersecurity



Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Introduction: Daniela Pöhn

- GÉANT JRA3 TL in GN4-1 and GN4-2 (first part)
- Researcher at Leibniz Supercomputing Centre
- Project Leader at Fraunhofer AISEC
- Currently Postdoc at Bundeswehr University, Research Center Cyber Defence



Research Center Cyber Defense

- Most projects currently in Cyber Defence
- Cyber Range (currently at the beginning)
- CTF
- Paper-based Simulation of attacks (Banking sector)
- Trend analysis based on Twitter and other sources
- And many more

ENISA Threat Landscape 2017

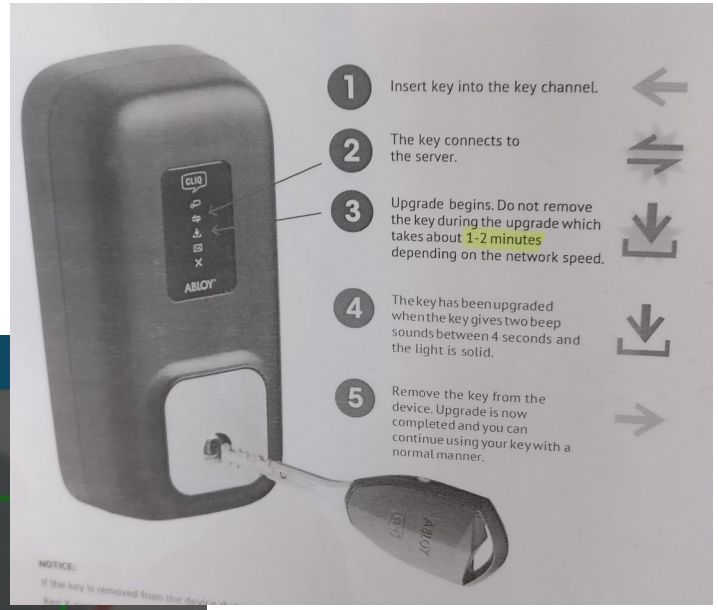
- Malware
- Web-based attacks
- Web application attacks
- Phishing
- Spam
- Denial of Service
- Ransomware
- Botnets
- Insider Threat
- Cyber-Espionage

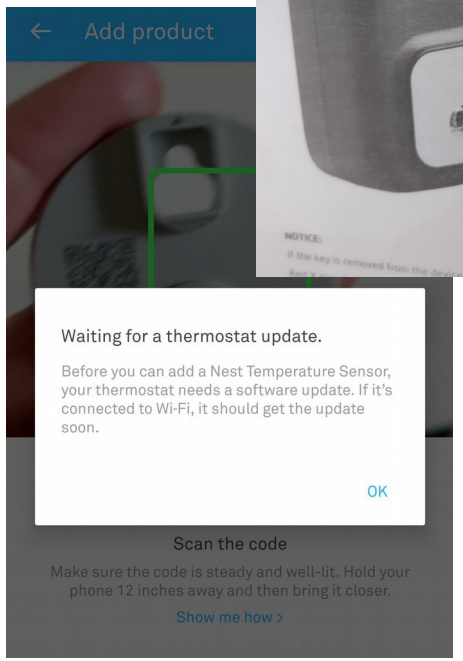
ENISA Threat Landscape 2017

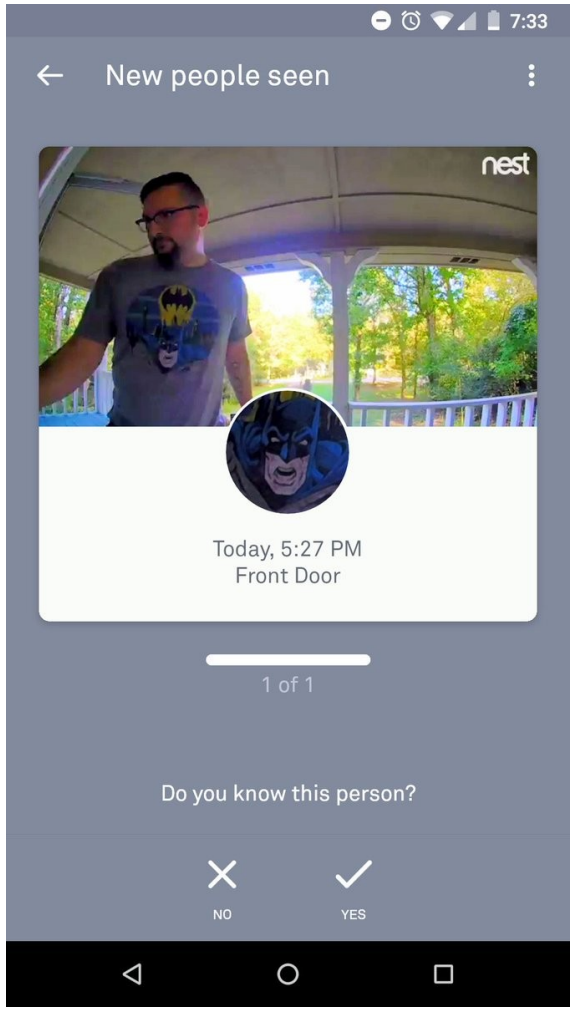
Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

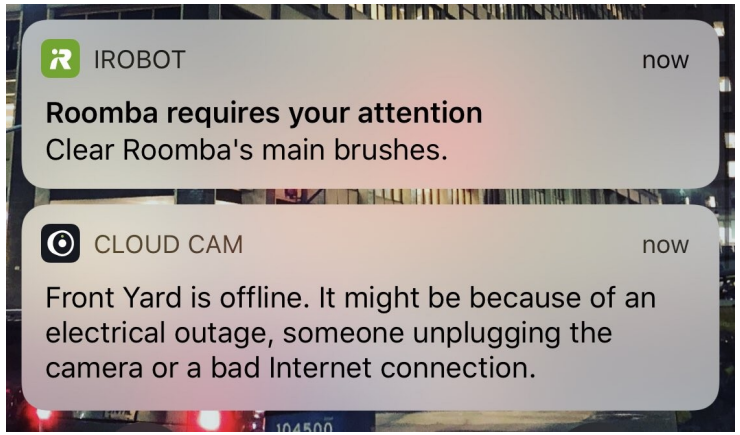
ENISA Threat Landscape 2017







6. Denial of service	↓	
7. Ransomware	↑	
8. Botnets	↓	



Internet of Things

- Cameras in
  - Smart Home
  - Monitoring Systems
  - Notebooks
- Sensors in IoT
- Security vs. Price
- Testing

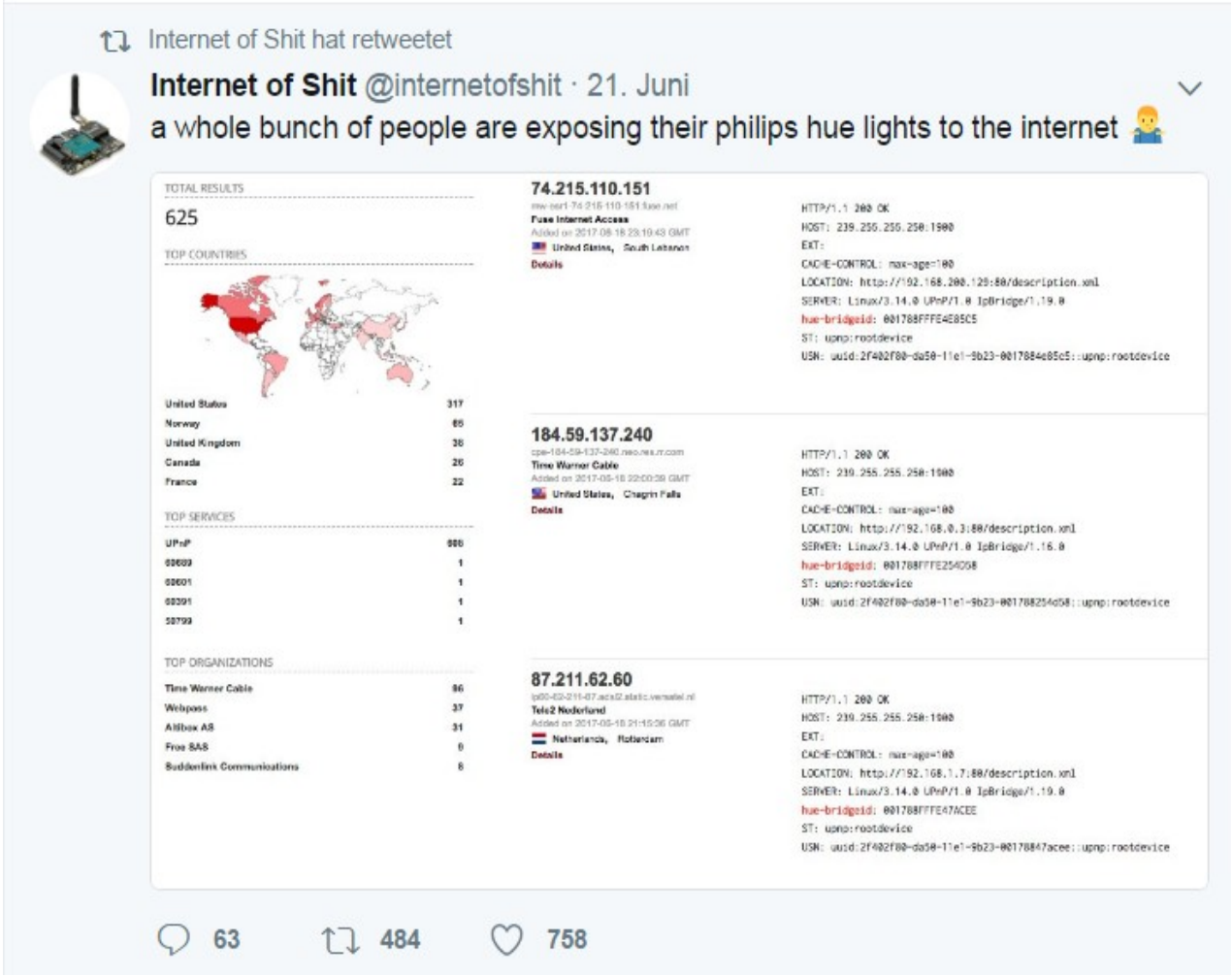
Internet of Things

- Cameras in Cloud
- Feasible attacks from local network
  - Eavesdropping of video stream
  - Enabling periodic upload of images to an external storage
  - Bricking the camera (invalid configuration → crash during boot)
  - Finding the hidden Backdoor Setup feature

Internet of Things

- Cameras in Cloud
  - → Attacker may gain full control over the device
  - → Replace video streams by any images
  - → Eavesdropping of real video streams
  - → Scalable to hundreds of devices

Internet of Things



Shodan.io

- https://www.shodan.io
- Sentient Hyper-Optimized Data Access Network
- Port Scans
- Results are open for public, API
- Find relevant exploits → Penetration Testing
- Banners inform about Name, Sort, Version of Server, Device, Software
- Filter criteria e.g. Name, Network, Port, Time, Place

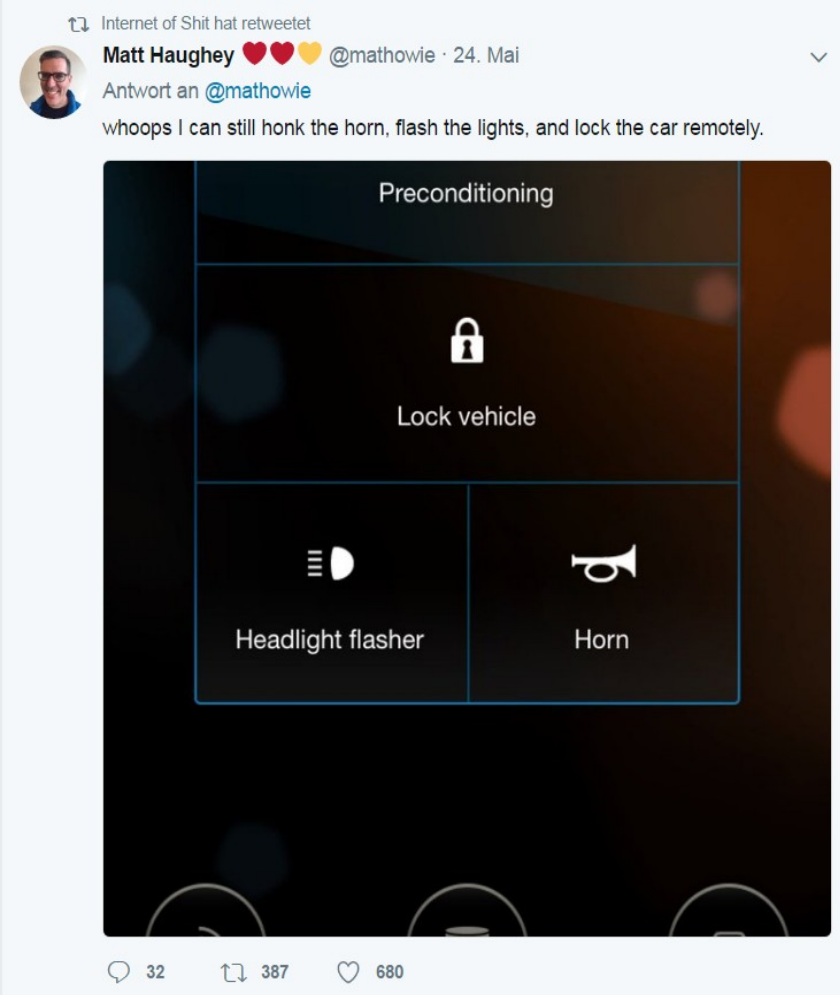
  → geolocation service (plus some other sources)

Google Hacking

- Google finds information, which are publicly available
- e.g. Vulnerable Software Versions, Log Files, Unprotected Webcams and other Hardware, Logins
- Banners of Software and hardware release: Product + Version
- Special Search Criterion (Google Dorks)

  → DDoS attacks

Internet of Things



Federated Identity Management

- In NRENs typically SAML
- Changing to OAuth and OpenID Connect (OIDC)
- Differences:
  - Names (Identity Provider vs. OpenID Provider and Service Provider vs. Relying Party)
  - XML vs. JSON
  - Solid vs. Dynamic Federation
  - Big Federations vs. Apps and Dynamic
  - Authenticaiton and Authorization vs. Authorization (plus Authentication)

Federated Identity Management

- Federation as a Service by GÉANT
  - Easy set up of SAML federation
  - Costs covered by NREN subscription to GÉANT
  - Advantage reduced manpower needed to start and run a federation as infrastructure
  - 4-5 NRENs participate so far
  - https://wiki.geant.org/display/eduGAIN/Federation+as+a+Service+-+FaaS
  - Questions? faas@lists.geant.org or nebojsa.ilic@amres.ac.rs

Other services by GÉANT

- InAcademia
- eduroam
- eduCONF
- eduPKI
- GÉANT Cloud Brokerage Service
- Multidomain VPN

Some Ideas and Possible Topics for Open Space

- DDoS protection
- Machine Learning in IDS
- Pentesting
- Training
- Federation as a Service
- IoT
- CERT
- Outsourcing Services
- Blockchain