

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

Cyber Defence

Smart Data

Kritische
Infrastruktur

Mobile Security

e-Health

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

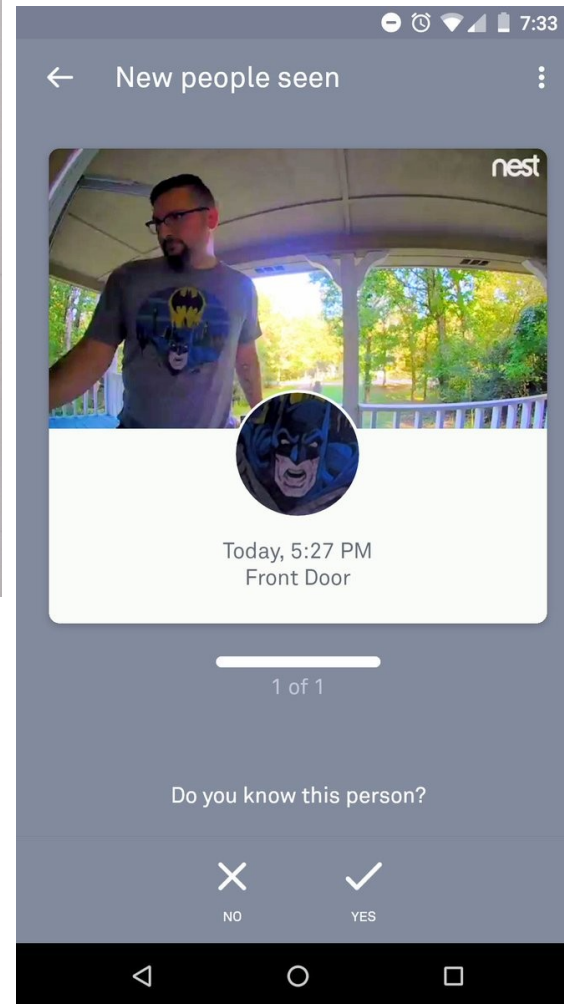
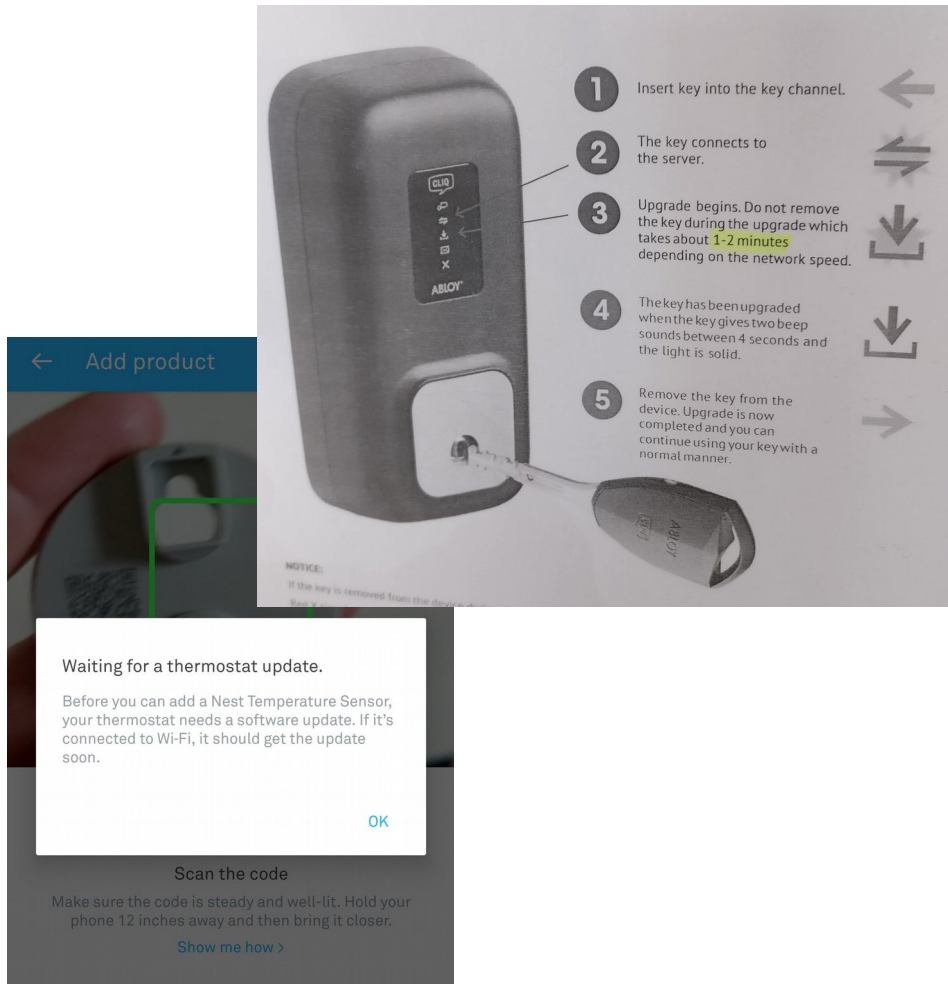
- Malware
- Web-based attacks
- Web application attacks
- Phishing
- Spam
- Denial of Service
- Ransomware
- Botnets
- Insider Threat
- Cyber-Espionage

ENISA Threat Landscape 2017

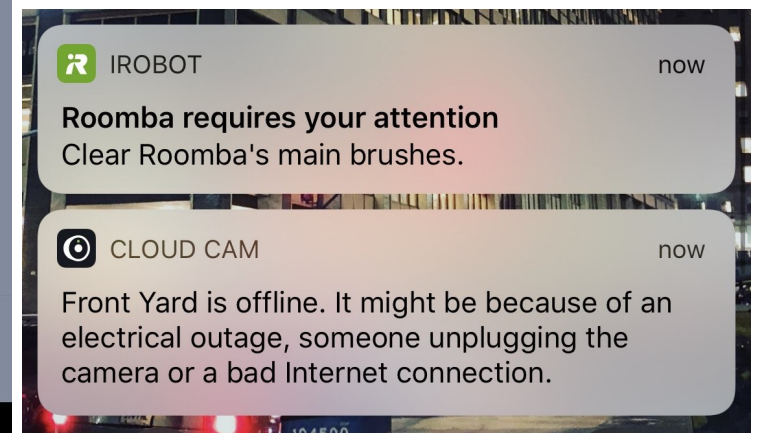
Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	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

Internet of Shit hat retweetet

 **Internet of Shit** @internetofshit · 21. Juni
a whole bunch of people are exposing their philips hue lights to the internet 🤖

TOTAL RESULTS
625

TOP COUNTRIES



United States	317
Norway	85
United Kingdom	38
Canada	26
France	22

TOP SERVICES

UPnP	580
02609	1
02601	1
02091	1
58793	1

TOP ORGANIZATIONS

Time Warner Cable	86
Webpos	37
Airbox AS	31
Free SAS	0
Buddenlink Communications	8

74.215.110.151
max-seet-7a-215-110-151.kyo.net
Fixed Internet Access
Added on 2017-05-18 23:10:43 GMT
United States, South Lebanon
[Details](#)

HTTP/1.1 200 OK
HOST: 239.255.255.258:1990
EXT:
CACHE-CONTROL: max-age=100
LOCATION: http://192.168.208.129:88/description.xml
SERVER: Linux/3.14.0 UPnP/1.0 IpBridge/1.19.0
hue-bridgeid: 001788FFFE4E85C5
ST: upnp:rootdevice
USN: uuid:2f402f88-da58-11e1-9b23-0017884e85c5::upnp:rootdevice

184.59.137.240
cpe-184-59-137-240.neo.net.com
Time Warner Cable
Added on 2017-05-18 22:00:59 GMT
United States, Chagrin Falls
[Details](#)

HTTP/1.1 200 OK
HOST: 239.255.255.258:1990
EXT:
CACHE-CONTROL: max-age=100
LOCATION: http://192.168.0.3:88/description.xml
SERVER: Linux/3.14.0 UPnP/1.0 IpBridge/1.16.0
hue-bridgeid: 001788FFFE254D58
ST: upnp:rootdevice
USN: uuid:2f402f88-da58-11e1-9b23-001788254d58::upnp:rootdevice

87.211.62.60
p050-82-211-67.wdc2.static.veranet.nl
Tele2 Nederland
Added on 2017-05-18 21:15:36 GMT
Netherlands, Rotterdam
[Details](#)

HTTP/1.1 200 OK
HOST: 239.255.255.258:1990
EXT:
CACHE-CONTROL: max-age=100
LOCATION: http://192.168.1.7:88/description.xml
SERVER: Linux/3.14.0 UPnP/1.0 IpBridge/1.19.0
hue-bridgeid: 001788FFFE47ACEE
ST: upnp:rootdevice
USN: uuid:2f402f88-da58-11e1-9b23-00178847acee::upnp:rootdevice

63 484 758

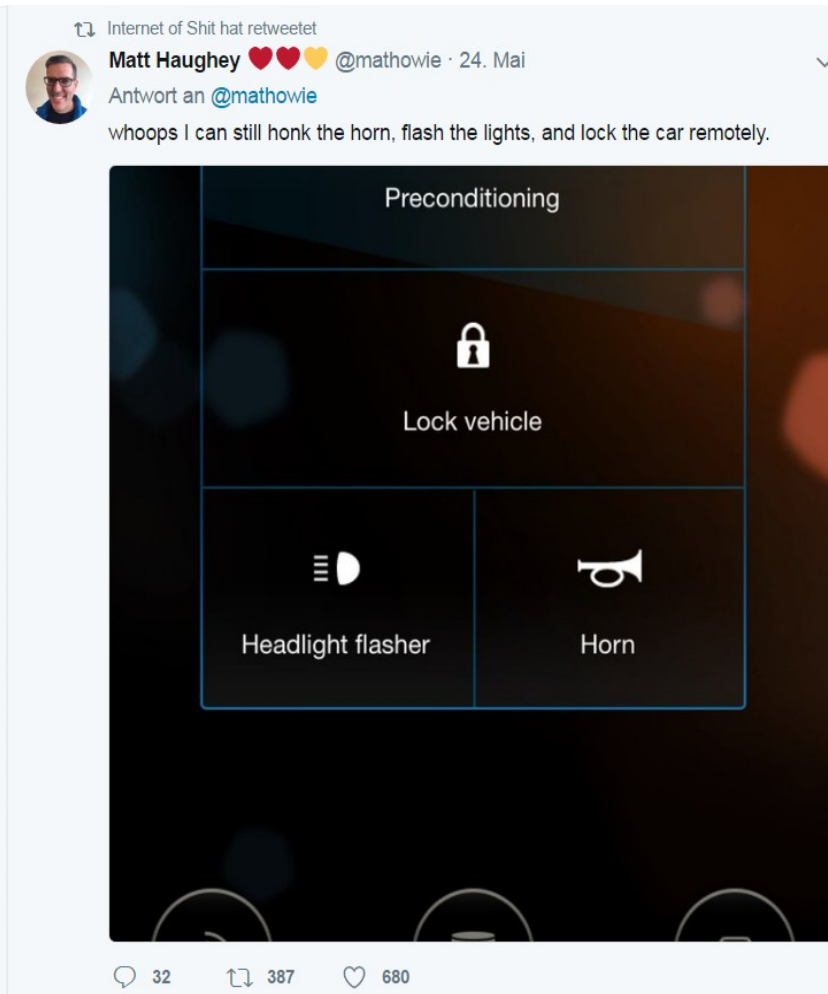
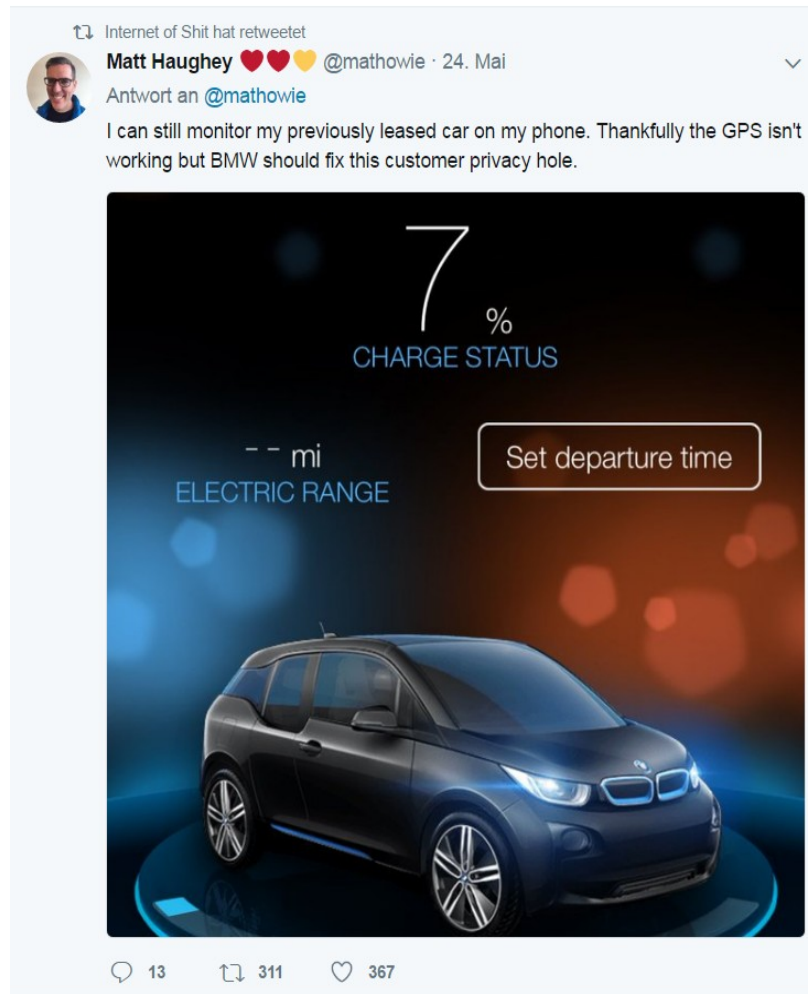
Shodan.io

- <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