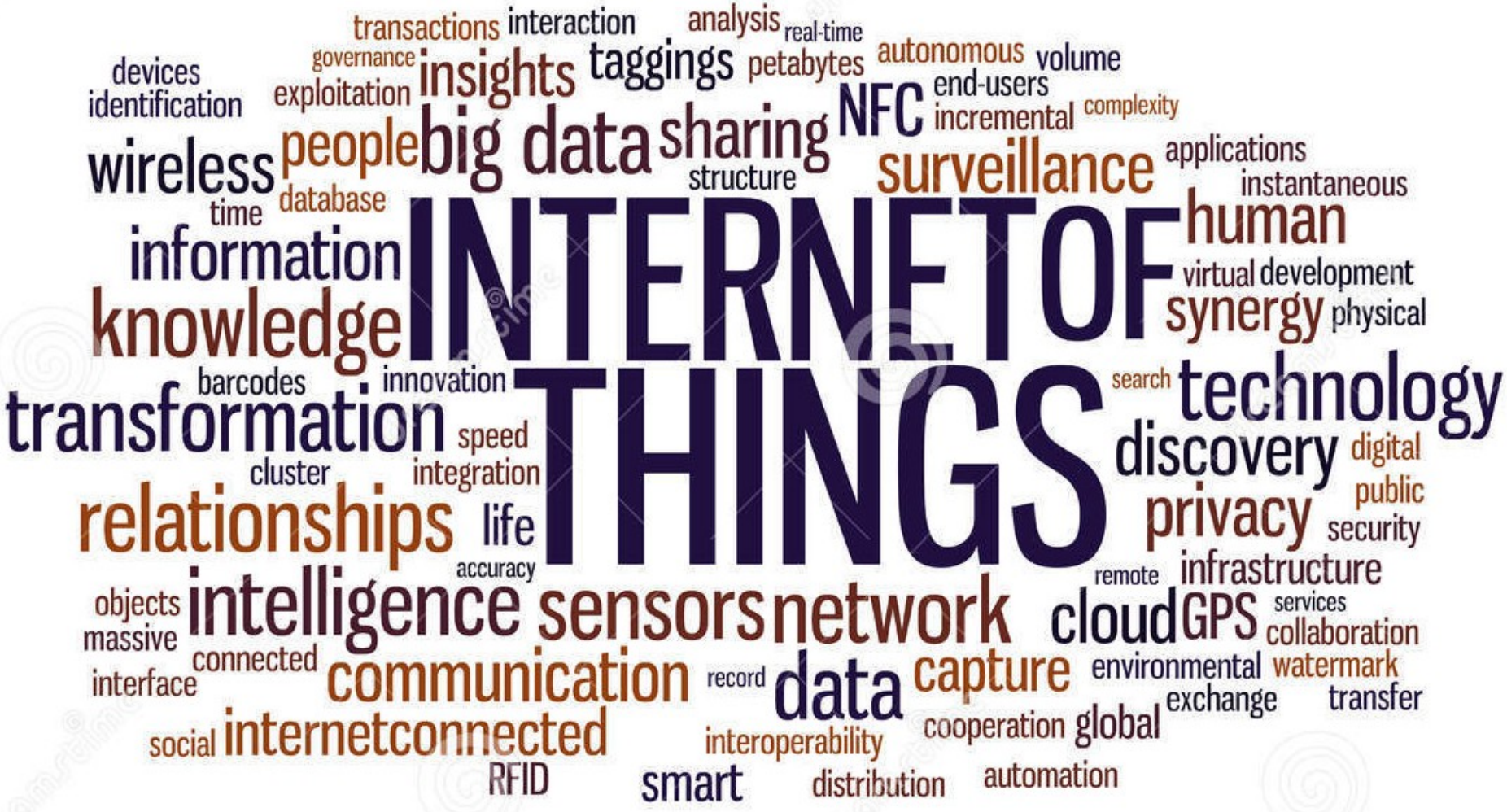
(Security)-Stolpersteine auf dem Weg zum IoT

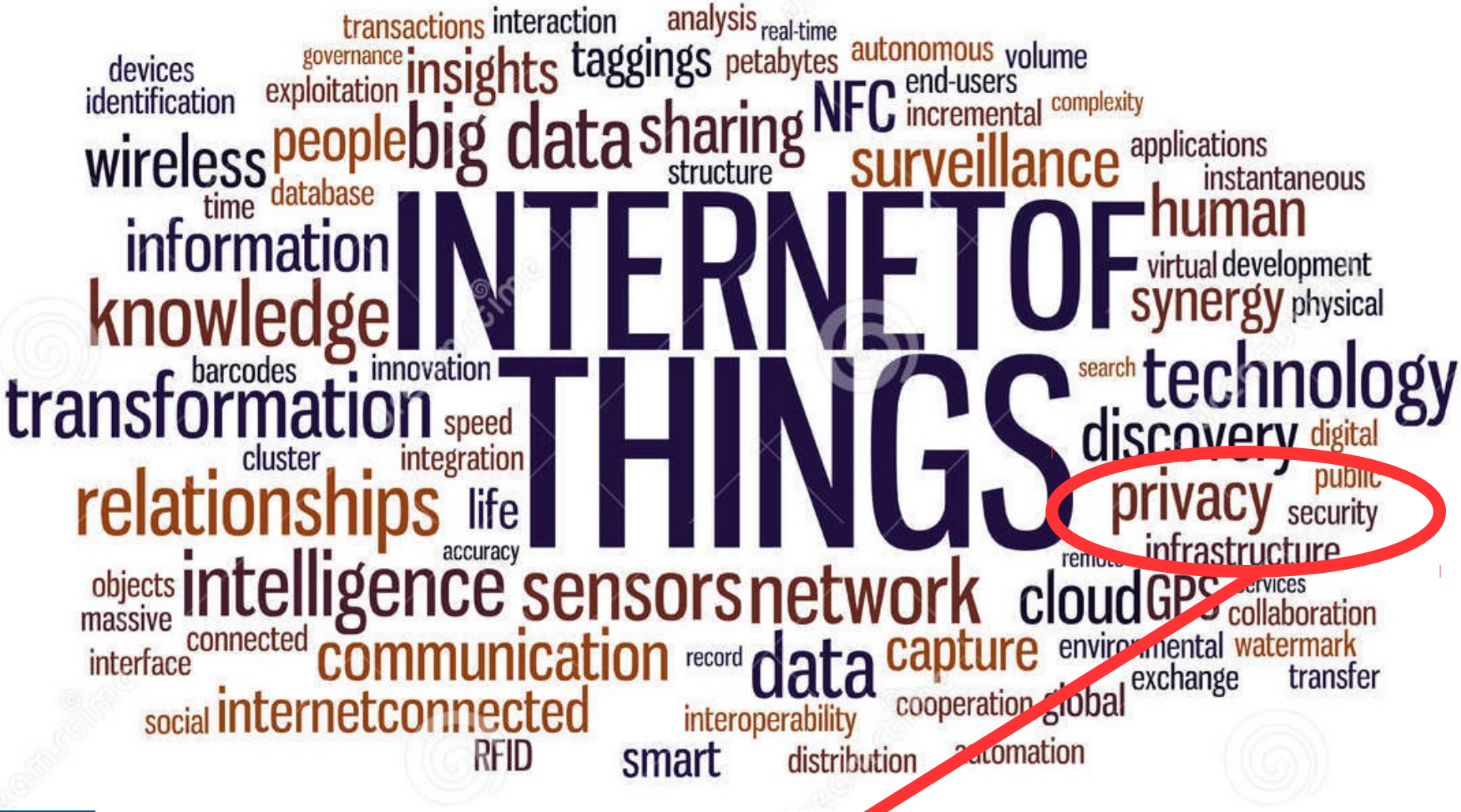
Aljosha Judmayer
ajudmayer@sba-research.org
2014-10-23

SBA Research

Area 1 (GRC): Governance, Risk and Compliance	P1.1: Risk Management and Analysis P1.2: Secure BP Modeling, Simulation and Verification P1.3: Computer Security Incident Response Team P1.4: Awareness and E-Learning
Area 2 (DSP): Data Security and Privacy	P2.1: Privacy Enhancing Technologies P2.2: Enterprise Rights Management P2.3: Digital Preservation
Area 3 (SCA): Secure Coding and Code Analysis	P3.1: Malware Detection and Botnet Economics P3.2: Systems and Software Security P3.3: Digital Forensics
Area 4 (HNS): Hardware and Network Security	P4.1: Hardware Security and Differential Fault Analysis P4.2: Pervasive Computing P4.3: Network Security of the Future Internet



http://thumbs.dreamstime.com/z/internet-things-word-cloud-words-which-related-to-concept-iot-refers-to-uniquely-38616417.jpg



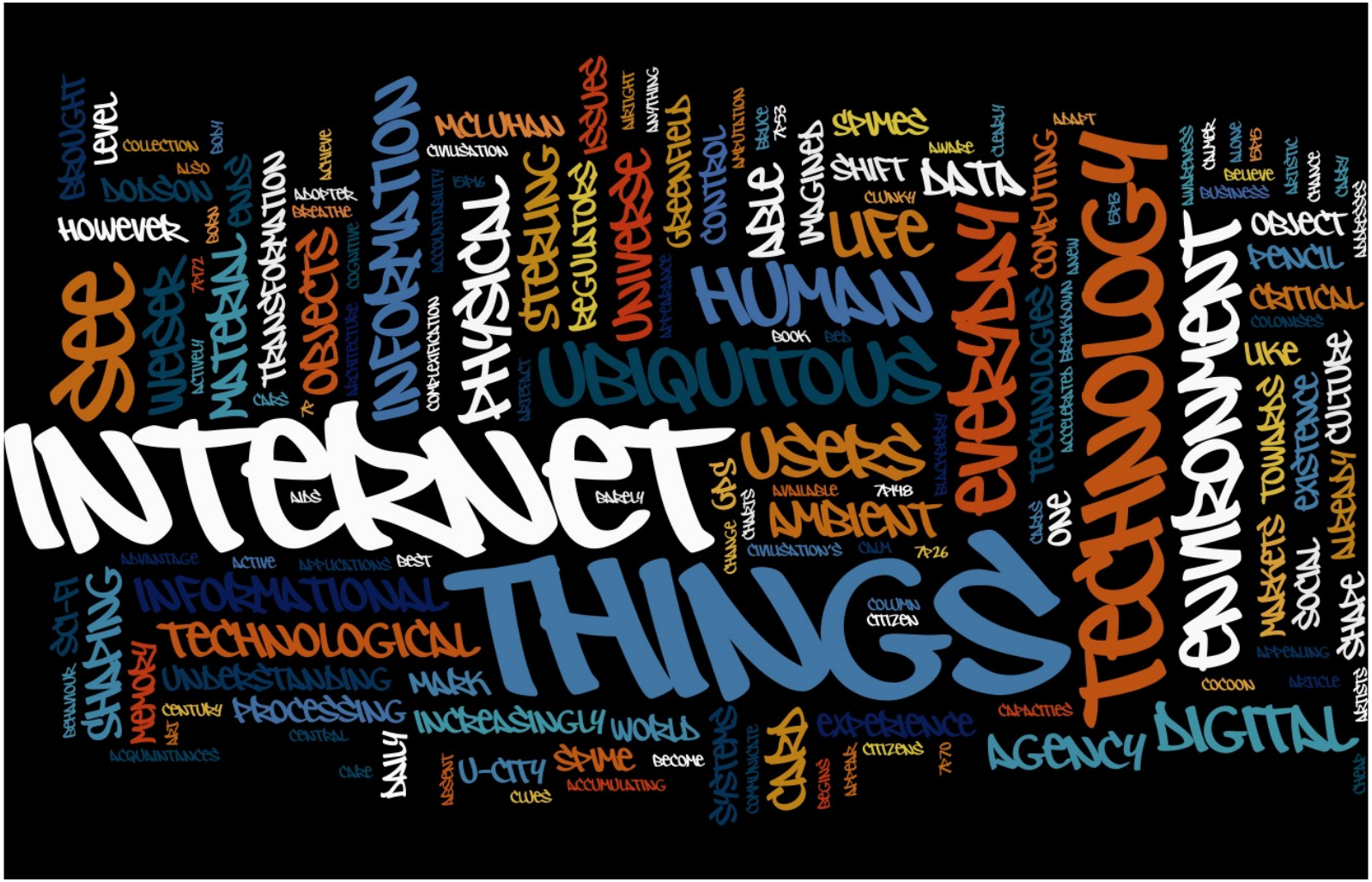
“privacy”, “security”

http://thumbs.dreamstime.com/z/internet-things-word-cloud-words-which-related-to-concept-iot-refers-to-uniquely-38616417.jpg

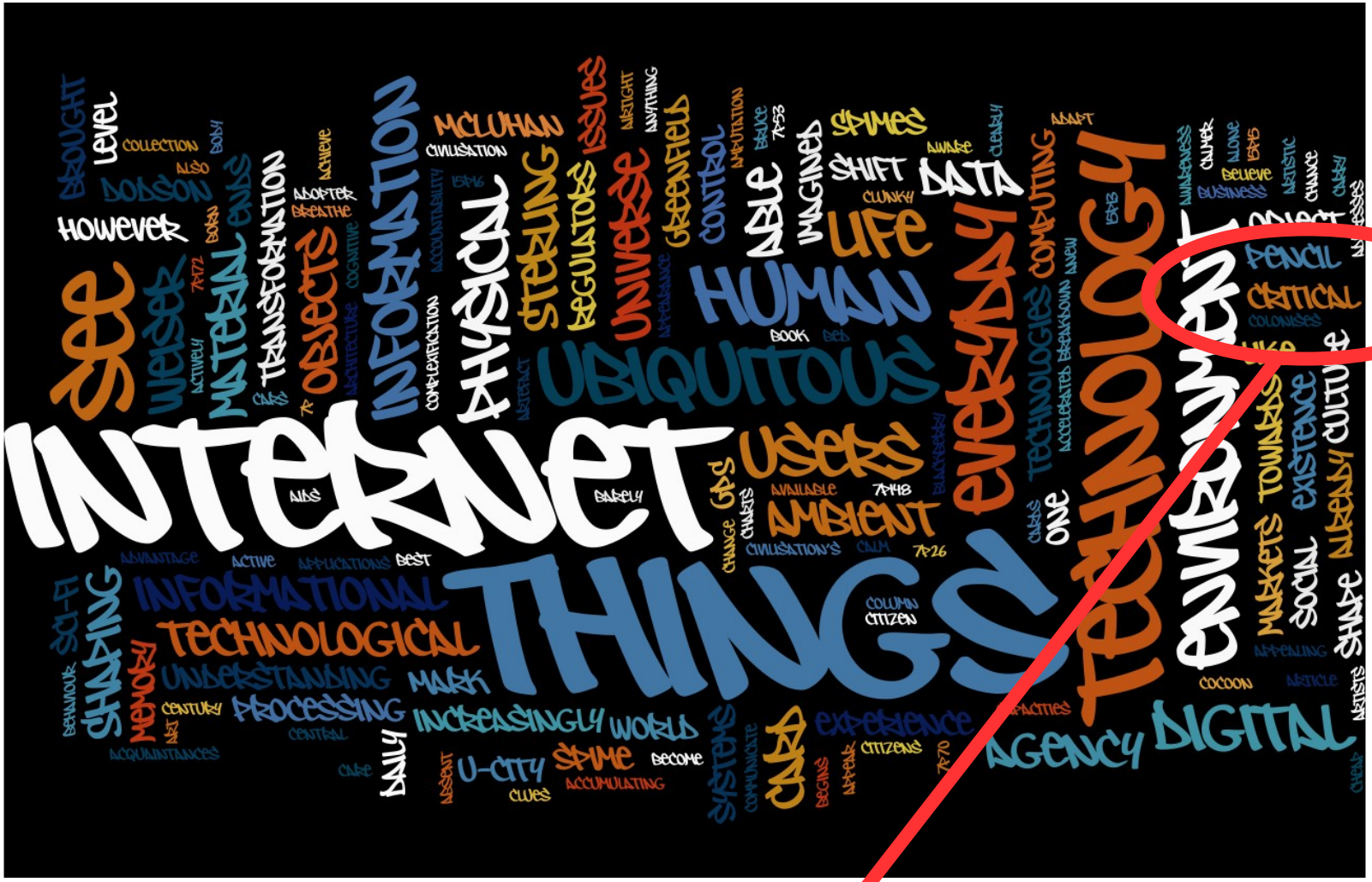
http://thumbs.dreamstime.com/z/internet-things-word-cloud-words-which-related-to-concept-iot-refers-to-uniquely-38616417.jpg

“secure”, “safe”, “resilient”

http://thumbs.dreamstime.com/z/internet-things-word-cloud-words-which-related-to-concept-iot-refers-to-uniquely-38616417.jpg



http://theinternetofthings.files.wordpress.com/2008/12/tagcloud3.jpg



“Critical” … security critical or critical for success?

http://theinternetofthings.files.wordpress.com/2008/12/tagcloud3.jpg

IoT & Security ?

Security And The Internet Of Things

“What is troubling, is the possibility that security is not taken into account with these carious implementations.”

(Forbes)

http://www.forbes.com/sites/davelewis/2014/09/16/security-and-the-internet-of-things/

IoT & IPv6 ?

Finally, IPv6's killer app:
The Internet of Things

"IPv6, with its glorious address space, is just what's needed to connect all those billions of things"

(ZDNet)

http://www.zdnet.com/finally-ipv6s-killer-app-the-internet-of-things-7000027644/

IPv6 Address Space

- IPv4: 2^32

  ~ 4 billion addresses (de: Milliarden ;)

  e.g.: **8.8.8.8**

- IPv6: 2^128

  ~ *100 addresses for every atom on surface of the earth*

  e.g.: **2001:4860:4860::8888**

  2001:4860:4860:0000:0000:0000:0000:8888

IPv6

2001:4860:4860:0000:0000:0000:0000:8888

- **Provider + Customer = Prefix**
- **Interface-Identifier**
- Possible to have one globally unique address for every”**thing**” and forever
  - Privacy?
- Privacy extensions
  - Change Interface-Identifier, but prefix?

IPv6 Address Space

- Scan of **all IPv4** Internet addresses form a single machine on one port using *zmap*:

  ~ 45 min (gigabit Ethernet)

- The same scan of **one IPv6 subnet** (2^64)

  ~ 300 000+ years

IPv6

- Don't blindly trust *“security through obscurity”* IPv6!
  - DNS and other sources to find out
  - Sniffing
  - Manually entered addresses => memorable
  - Frequent addresses (EUI-Format)
  - Heuristics

  [research]

[1] Johanna Ullrich and Katharina Krombholz and Heidelinde Hobel and Adrian Dabrowski and Edgar R. Weippl, "IPv6 Security: Attacks and Countermeasures in a Nutshell," in 8th USENIX Workshop on Offensive Technologies (WOOT), 2014

Example BAS

- Building Automation Systems (**BAS**)
- Back then: HVAC
- Now: **intelligent buildings**
- security and safety
  - alarm systems
  - access control systems
  - …
- connected to

  IP based networks

http://www.myenergymonster.com/wp-content/uploads/2014/04/Home-automation.jpg

Example BAS

- Raised attack surface
- Still legacy systems / protocols
- Requires good understanding of:
  - attack scenarios
  - hardening mechanisms

[research]

Source: http://laughingsquid.com/wp-content/uploads/tetris1_img6080.jpg

[1] Judmayer A., Krammer L., Kastner W., "On the security of security extensions for IP-based KNX networks", 10th IEEE Workshop on Factory Communication Systems (WFCS), 2014

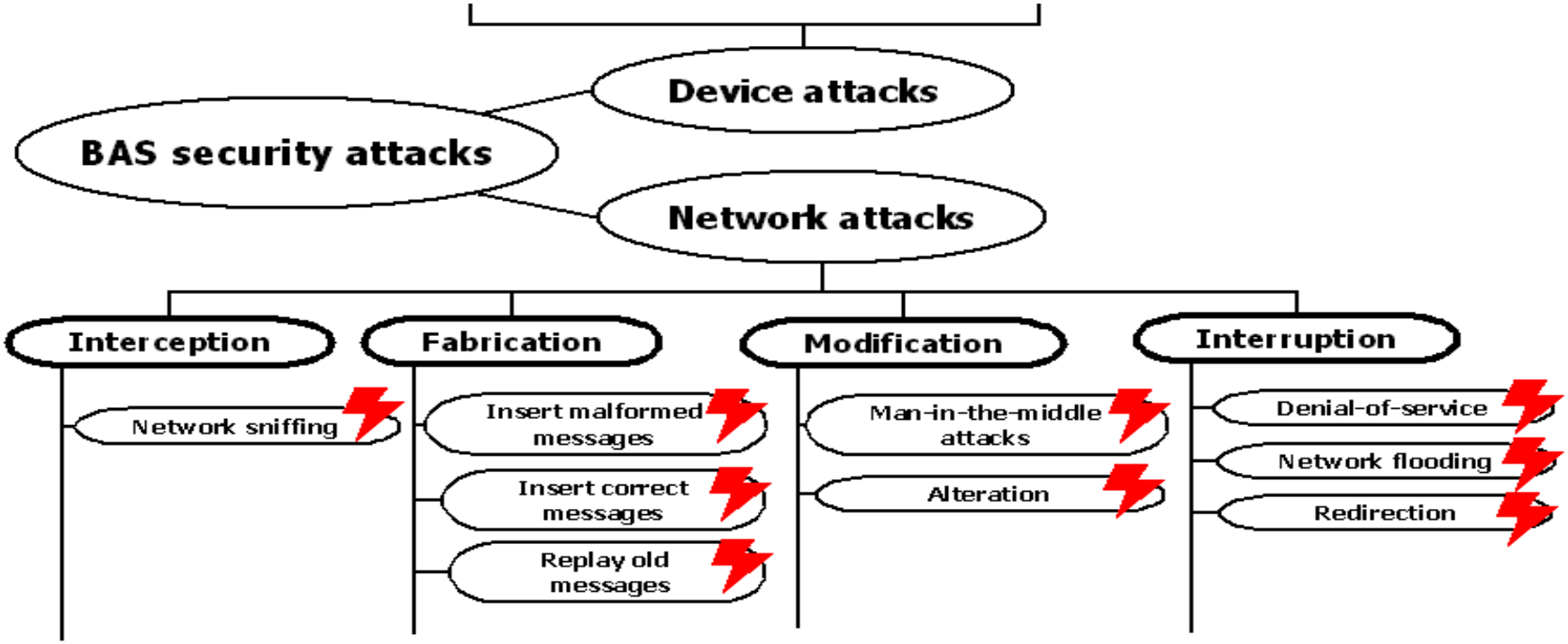
Security challenges in BAS IoT

- Resource constrained environment
  - CPU / RAM / power / clock
  - Impact of strong cryptography on performance
- Internet connectivity considered as a feature – not especially area of expertise
  - Classical vulnerabilities
- Effective patch deployment
- ...

Example KNX

- A standard for home and building automation
- **K**o**N**ne**X** Association
  - publish KNX Systems specification
  - Develop the Management Software
- Ensuring the **interoperability** between *products*, *applications* and *systems*

Attacks on classical KNX



Source: W. Granzer et al. "Security in Building automation Systems", IEEE vol. 57. NO. 11.NOV.2010

OWASP IoT Security Top 10

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

OWASP IoT Security Top 10

1. Insecure Web Interface
2. **Insufficient Authentication/Authorization**
3. **Insecure Network Services**
4. **Lack of Transport Encryption**
5. *Privacy Concerns*
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. **Insufficient Security Configurability**
9. **Insecure Software**/Firmware
10. Poor Physical Security

- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

IoT – what to do?

- Consider security **during design** and implementation
  - Careful feature selection
  - Keep it simple
  - Update plan
- IT Security Research and Testing
  - Protocols, attack techniques, test techniques, technologies, hardware, privacy ...

What we do **not** want in the IoT

Hackers Reveal Nasty New Car Attack (Forbes)

- Disable or slam breaks
- Steer the wheel
- Tighten seat belt
- ...

http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

- I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, I. Seskar, Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study , USENIX 2010

- S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX 2011

- C. Miller, C. Valasek, Adventures in Automotive Networks and Control Units, Defcon 2013

- K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental Security Analysis of a Modern Automobile IEEE Symposium on Security and Privacy 2010

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Thank you

SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
ajudmayer@sba-research.org

secure
sba-research.org

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfi
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien