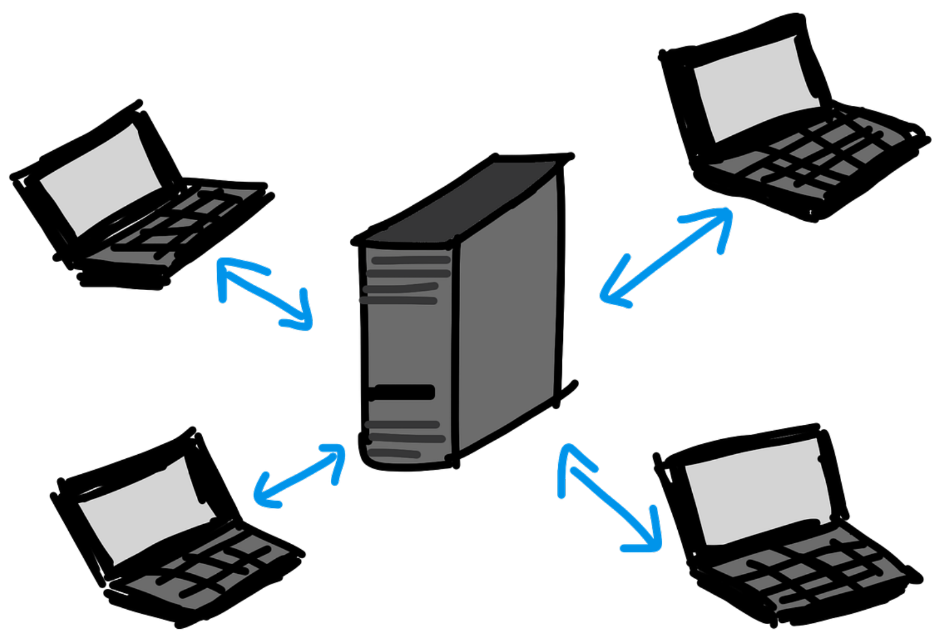
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Evaluating Network Security Using Internet-wide Measurements

Oliver Gasser

Internet-wide Measurements

- Useful tool
- Various measurement techniques
- Focus on **empirical security** measurements



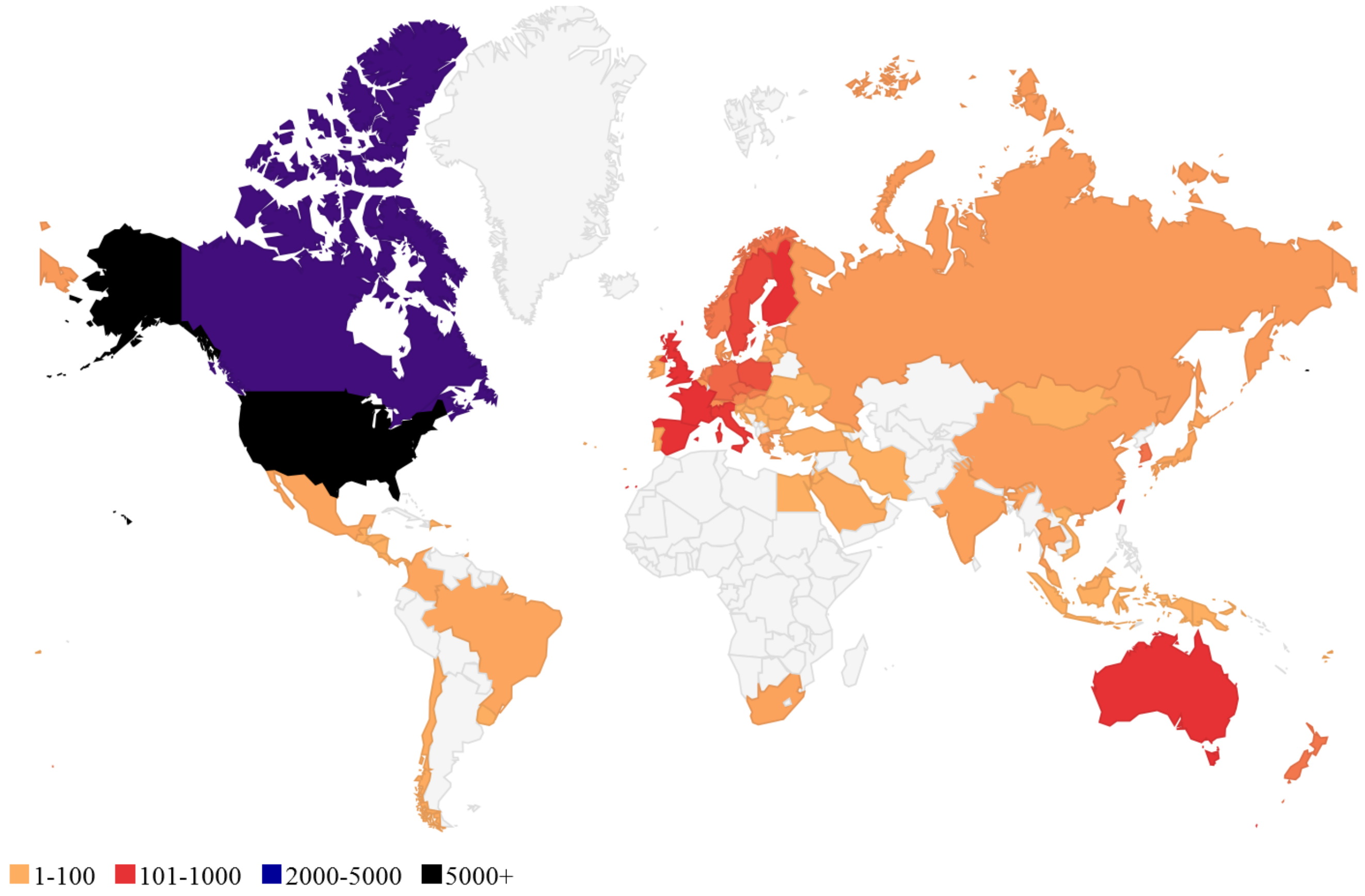
Network Security

- More and more devices are connected to the Internet
- Devices mostly not designed with security in mind

- Use **Internet-wide measurements** to evaluate security

Building Automation Systems

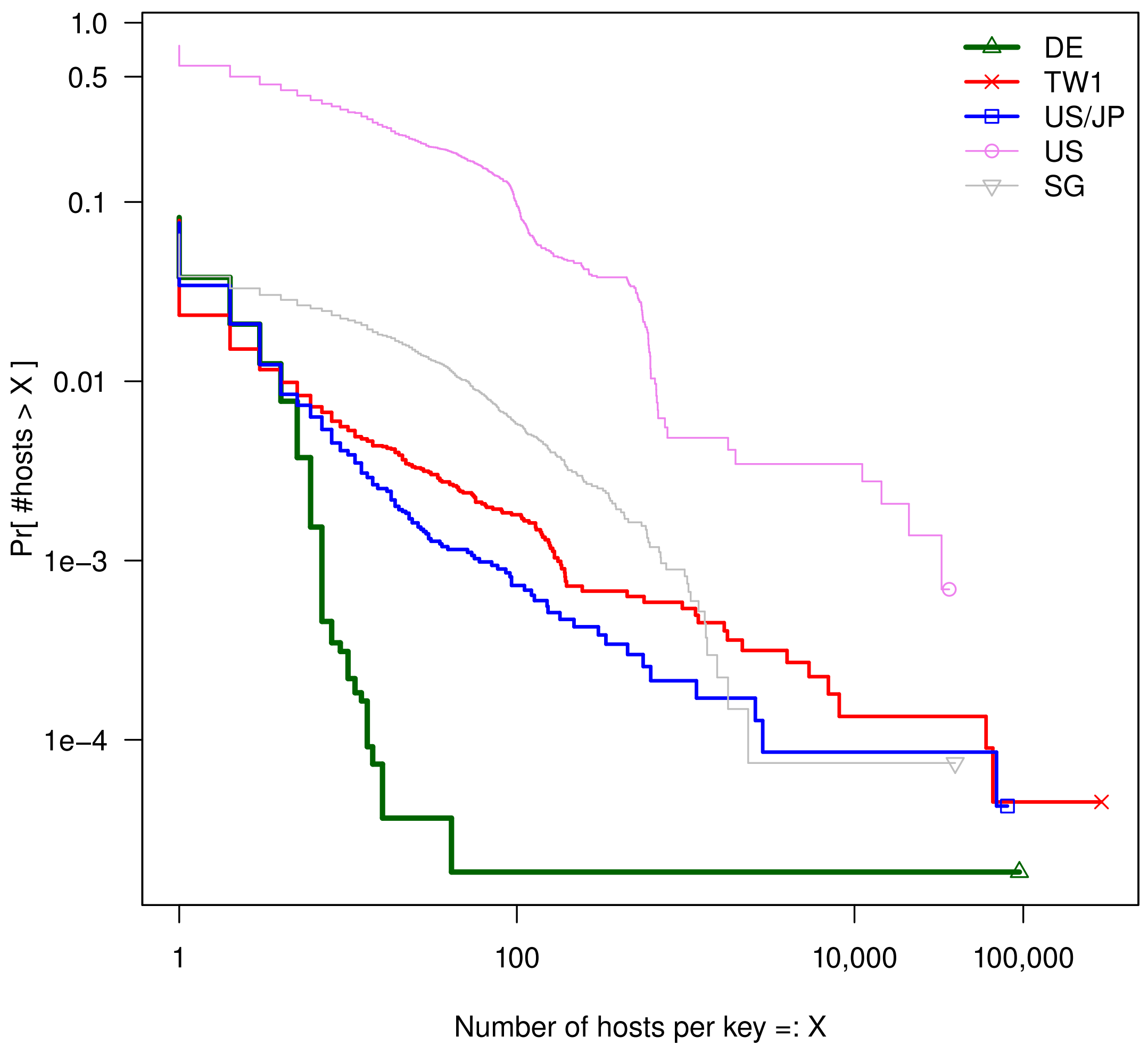
- BACnet: Security and safety critical protocol
- More than 16 k publicly accessible BACnet devices



- Most are vulnerable to **amplification attacks** [2]
- Amplification factor similar to Open DNS resolver (≈50x)

SSH Servers

- SSH: Mostly used for server administration → security critical protocol
- More than 15 M SSH servers [1]
- Many **duplicate keys** → Man-in-the-Middle attacks



Infrastructural Measurements

- Detecting IPv6-IPv4 siblings [4]: **Paper at TMA'17**
- Geolocating routers [5]: **Paper at TMA'17**
- Generating a hitlist for IPv6 [3]
- Detecting routing anomalies [6]

Future Work

- Assessing success of vulnerability notification campaigns
- Extending IPv6 hitlist with additional sources
- Making measurement data publicly available in append-only logs

[1] O. Gasser, R. Holz, and G. Carle. A deeper understanding of SSH: results from Internet-wide scans. In *NOMS*, Krakow, Poland, May 2014.
[2] O. Gasser, Q. Scheitle, C. Denis, N. Schricker, and G. Carle. Security Implications of Publicly Reachable Building Automation Systems. In *WTMC*, San Jose, CA, USA, May 2017.
[3] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist. In *TMA*, Louvain-la-Neuve, Belgium, Apr. 2016.
[4] Q. Scheitle, O. Gasser, M. Rouhi, and G. Carle. Large-Scale Classification of IPv6-IPv4 Siblings with Variable Clock Skew. In *TMA*, Dublin, Ireland, June 2017.
[5] Q. Scheitle, O. Gasser, P. Sattler, and G. Carle. HLOC: Hints-Based Geolocation Leveraging Multiple Measurement Frameworks. In *TMA*, Dublin, Ireland, June 2017.
[6] J. Schlamp, R. Holz, O. Gasser, A. Korsten, Q. Jacquemart, G. Carle, and E. W. Biersack. Investigating the Nature of Routing Anomalies: Closing in on Subprefix Hijacking Attacks. In *TMA*, Barcelona, Spain, Apr. 2015.