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

Internet Architecture and Security

Quirin Scheitle

Motivation & Research Goals

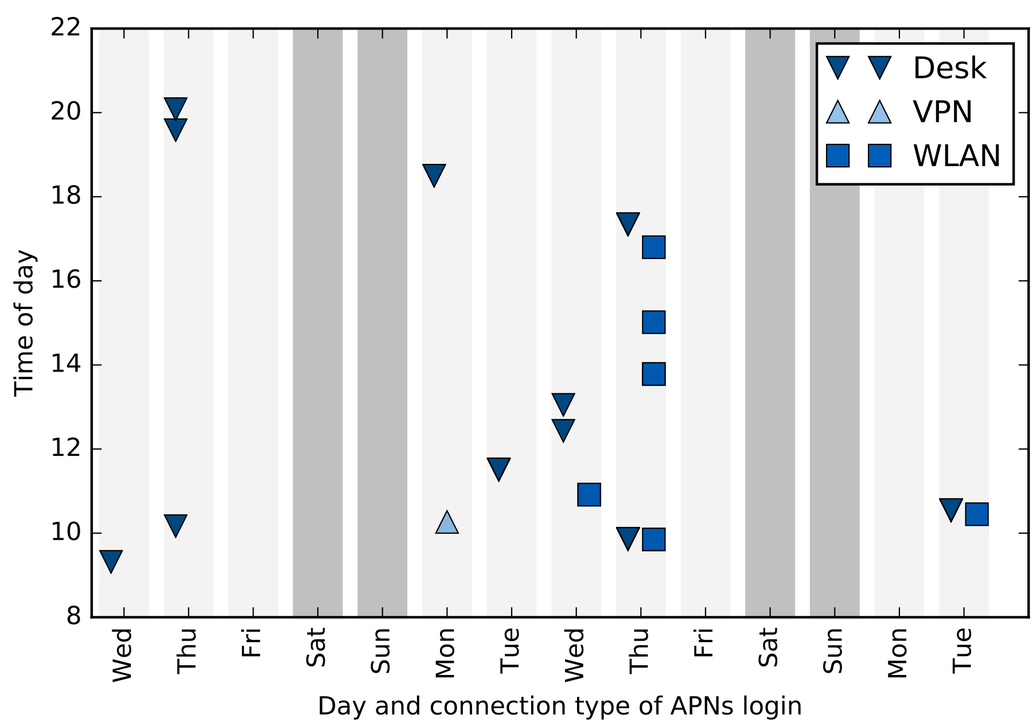
- Hypothesis: Internet Architecture may influence the security posture of services
- Goal: Find and throughly map those interactions between security and architecture
- Methodology: Large-scale active and passive Internet measurements

Specific Topics

- Foundations
  - Router Geolocation [4] **TMA'17**
  - v6-v4 Sibling Mapping [3] **TMA'17**
  - IPv6 Internet Scanning [2] (TMA'16)
  - Reproducibility [6] (Reproducibility'17)
- Applications
  - Mobile Messengers [5] (PAM'16)
  - Apple Push Notification Services [7] **TMA'17**

Apple Push Notification Services [7]

- Apple Push Notification Service (APNs) uses TLS Client Certificate Authentication (CCA) for device login
- TLS1.2-CCA does not encrypt client certificates!
- APNs is "always-on" on all iOS, macOS, watchOS, tvOS, and iTunes on Windows devices
- This combination of an always-on service with mobile devices provides unique device tracking capabilities
- We conduct a Proof-of-Concept tracking of consenting users and quantify the problem at Internet-Scale
- We find that eavesdropping access to 10 large networks will provide tracking capabilities for >80% of devices
- Responsible disclosure to Apple, high-priority fix



Mobile Messaging Locality [5]

- Mobile Messaging Services such as WhatsApp quickly gain market share from SMS or E-Mail
- Services are neither standardized nor thoroughly researched (impeded by change frequency)
- Our Hypothesis: Central server architecture heavily directs traffic out of region
- Complex testbed with control framework "MATADoR" to run 4 Apps (WhatsApp, Threema, WeChat, TextSecure/Signal) from 28 countries
- Results confirm hypothesis and call for discussion

Reproducibility [6]

- Repeatability, Replicability, Reproducibility
- Challenges: Authors, Artifacts, Details
- Proposed Solution: Evolving Ecosystem

Building Block	Initial	Evolved	Mature
Reproducibility Challenge	✓	✓	✓
Author Incentives	✘	✓	✓
Reproducibility Review	✘	✓	✓
Metrics & Badging	✘	✘	✓
Journal Fast-Track	✘	✘	✓

[1] O. Gasser, Q. Scheitle, C. Denis, N. Schricker, and G. Carle. Security Implications of Publicly Reachable Building Automation Systems. In *Traffic Measurements for Cybersecurity*, 2017.
[2] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist. In *TMA'16*.
[3] Q. Scheitle, O. Gasser, M. Rouhi, and G. Carle. Large-Scale Classification of IPv6-IPv4 Siblings with Variable Clock Skew. In *TMA'17*.
[4] Q. Scheitle, O. Gasser, P. Sattler, and G. Carle. HLOC: Hints-Based Geolocation Leveraging Multiple Measurement Frameworks. In *TMA'17*.
[5] Q. Scheitle, M. Wachs, J. Zirngibl, and G. Carle. Analyzing Locality of Mobile Messaging Traffic Using the MATAdOR Framework. In *PAM'16*.
[6] Q. Scheitle, M. Wählisch, O. Gasser, T. C. Schmidt, and G. Carle. Towards an Ecosystem for Reproducible Research in Computer Networking. In *SIGCOMM Reproducibility Workshop*, 2017.
[7] M. Wachs, Q. Scheitle, and G. Carle. Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication. In *TMA'17*.

Quirin Scheitle

scheitle@net.in.tum.de