INF

FACULTY OF
COMPUTER SCIENCE

Secure Networks for IoT Devices

David Hausheer (OVGU Magdeburg), Adrian Perrig (ETH Zürich)

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Institut IKS
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Internet of Things (IoT)

- Network of smart objects, to collect and analyze data

Smart Home

home automation: lighting, heating, security, etc.

Assistance

people with disabilities, elderly care

Healthcare

remote health monitoring, emergency notification

Transportation

inter / intra vehicular communication, Smart Cities

Manufacturing

supply chain management, digital control, Smart Grid

- Characteristics: Small-scale devices, sensors, low cost, low energy usage

- Bain predicts IoT market to grow to about $520B in 2021 ($235B in 2017)

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Institut IKS
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Security of Internet of Things

- **Security** is the biggest concern in adopting IoT technology (especially IoT adoption in enterprises)

- **Threats:**
  - Potential failures and attacks hinder adoption in critical infrastructures with high availability requirements (e.g. transportation or Grid infrastructures)

  - IoT devices often use weak authentication which may facilitate unauthorized access (e.g. smart home, healthcare devices)

  - Use of unencrypted communication may leak privacy-sensitive data (e.g. healthcare)

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Institut IKS
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

SCION: Next-generation Internet Architecture

- Secure by design, most attacks are fundamentally impossible
- Path-aware networking: sender knows packet's path
  - Enables geo-fencing
- Highly available communication
- Multi-path communication
  - Caution: use is highly addictive!
- BGP-free Internet communication
- Better scalability than current Internet
- Improved network operation
  - Higher network utilization
  - Advanced traffic engineering

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Institut IKS
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

SCION Mechanisms to Satisfy IoT Requirements

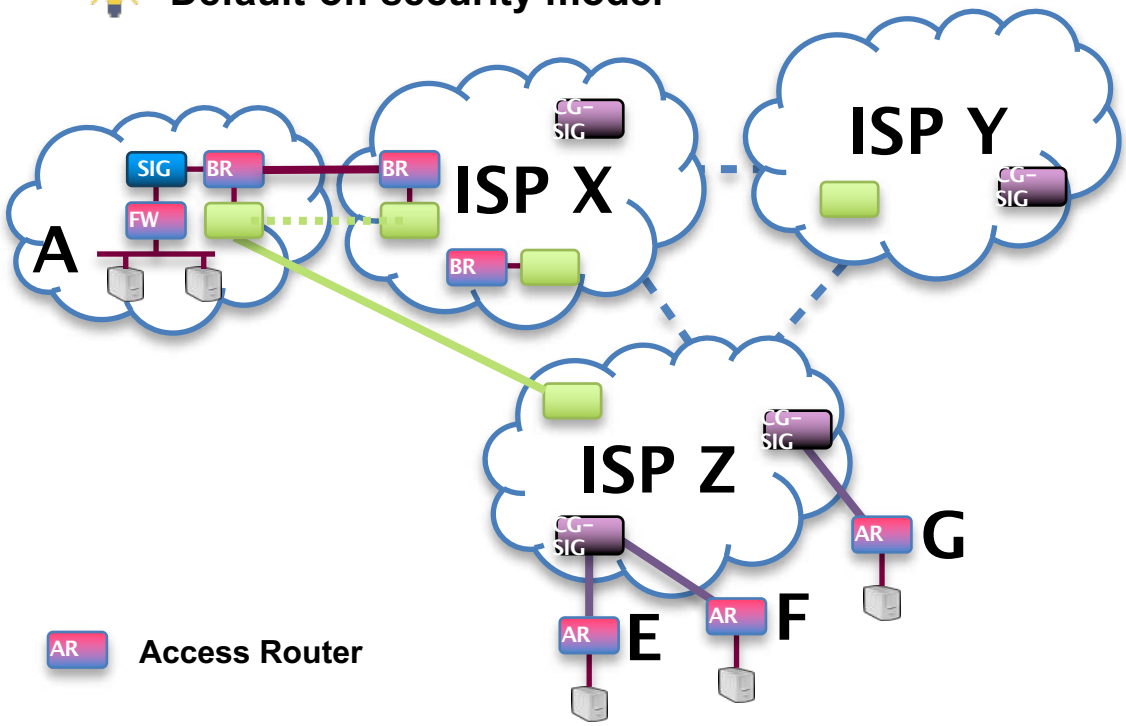
Key Management	Enable E2E encryption and authentication	DRKey
Controlled / restricted remote access	Prevent exploitation of device vulnerabilities	Hidden path (EPIC)
Guaranteed access for command-and-control	Packet delivery Traffic filtering at high data rates	Multipath in multi-homed environments EQ for guaranteed low-bw packet delivery Lightning Filter for high-speed filtering
Privacy	Complicate traffic analysis	Multipath communication can complicate traffic analysis
Compliance	Geofencing to avoid traffic leakage	Geofencing to avoid traffic leakage

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Institut IKS
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Use Case: Secure Networks for IoT Devices

- Use Hidden Paths
- Default-off security model



Deployment Scenario

- Site A is the monitoring site for IoT devices
- IoT Devices E, F, G are at ISP Z
  - Connected to SCION via CG-SIGs
  - Path Segments to the CG-SIGs are hidden and only given to site A

Benefits

- ✓ Secure network access
  - Only site A can access E, F, G
- ✓ High availability for the IoT network by using CG-SIG

SCION

Thank you for your attention!
Questions?

david.hausheer@gmail.com

Networks and Distributed Systems Lab (NetSys)

SCION

Online Resources

- https://www.scion-architecture.net
  - Book, papers, videos, tutorials
- https://www.scionlab.org
  - SCIONLab testbed infrastructure
- https://github.com/scionproto/scion
  - Source code
- https://www.anapaya.net
  - SCION commercialization

SCION