5G Security: Forward Thinking

David Francis  European CSO

Huawei Technologies
5G Security: Forward Thinking

• Security Challenges Ahead of 5G
  • Traditional Security Practice
  • New Business Models
  • IT-Driven Network Architecture
  • Heterogeneous Access
  • Privacy Protection

• 5G Security Goals
  • E2E Security for Vertical Industries
  • Secure Infrastructure

• 5G Security Perspectives
  • New Trust Model and Identity Management
  • Service-oriented Security
  • Security Assessment
  • Low-Delay Mobility Security
  • User Privacy Protection

• Summary
Traditional Security Practice

- Common security features
  - Identity management: USIM
  - Authentication: Mutual authentication
  - Data encryption: hop-by-hop
Security Challenges Ahead of 5G -- 5G New Business Models

5G Service Oriented

(100Billions New Devices@2025)
New Applications, New Business Models, and even New Industries

Mobile Internet
(4 Billions@2020)
Mobile Internet replaced PC Internet

Voice Smartphone

3G 4G
Security Challenges Ahead of 5G -- IT-Driven Network Architecture

- **SDN**
  - Manage the isolation for control nodes and forwarding nodes
  - Keep the SDN flow table securely and correctly enforced

- **NFV**
  - virtual NEs isolation and security management
  - Network slice isolation
  - Each virtual network slice requires differentiated security capabilities

Industry Defined Network Slicing

- **End-to-End Security Protection**

X Gbps

SDN/NFV

One Infrastructure, Multiple Network Slices
Security Challenges Ahead of 5G -- Heterogeneous Access

• 5G network is heterogeneous, security design need to consider various access technologies and different types of operators
  • **Access technologies:** 5G/LTE/3G/2G/Wi-Fi
  • **Operators:** MNO, MVNO, Local operators
Security Challenges Ahead of 5G -- Privacy Protection

- New sensitive services to deploy
- More privacy information to transport

- Service sensing for differentiated QOS
- Location sensing for LBS
- User sensing for AAA and better QOE

Public 5G network

Users

Attacker

- Collect user data
- Mine privacy information

Eavesdrop & Hack

Services
Future challenges and opportunities

- Big Data
- Cloud – do we have enough?
- Smart Home
- Car-2-Car Communications
- Industry 4.0
- SCM Security
- Smart devices
- 3G / 4G / 4.5G / 5G
- Internet of Things / IoT
- Mobile access to Cloud and DC
- Smart Cities / Energy / ..
- Compliance + Technologies
- Security operation centers / cyber defense centers

No security – No future!

Collected and selected from multiple sources like conference agendas, online webcast offerings, customer Q&A sessions.

Risk Metrics to influence business decisions

ISO27000 topics
- Data Security

Work Community @ GSMA, ISF, ..

Security policy and compliance management
- No security – No future!
5G Security: Forward Thinking

• Security Challenges Ahead of 5G
  • Traditional Security Practice
  • New Business Models
  • IT-Driven Network Architecture
  • Heterogeneous Access
  • Privacy Protection

• 5G Security Goals
  • E2E Security for Vertical Industries
  • Secure Infrastructure

• 5G Security Perspectives
  • New Trust Model and Identity Management
  • Service-oriented Security
  • Security Assessment
  • Low-Delay Mobility Security
  • User Privacy Protection

• Summary
5G Security Goals-- E2E Security for Vertical Industries

- Differentiated
  - E2E security design caters to different vertical industries
- Flexibility
  - Flexible and high efficient E2E security deployment and adaptation.
- Privacy protection
  - Massive personal privacy data, including device identifiers, user IDs, and user preference.
- Security as service
  - 5G will continue to extend the user trust by opening up security capabilities as a service to individual users and vertical industries.

HUAWEI TECHNOLOGIES CO., LTD.
5G Security Goals – Secure Infrastructure

- Secure Infrastructure
  - Diversified system level protection of IT-aware infrastructure
  - Identity management
  - Data Protection

Physical Infrastructure
5G Security: Forward Thinking

- Security Challenges Ahead of 5G
  - Traditional Security Practice
  - New Business Models
  - IT-Driven Network Architecture
  - Heterogeneous Access
  - Privacy Protection
- 5G Security Goals
  - E2E Security for Vertical Industries
  - Secure Infrastructure
- 5G Security Perspectives
  - New Trust Model and Identity Management
  - Service-oriented Security
  - Security Assessment
  - Low-Delay Mobility Security
  - User Privacy Protection
- Summary
5G Security Perspectives -- New Trust Model and Identity Management

- **Authentication**
  - Two parties → multi-parties:
    - user, network, and service providers will be actively involved in the authentication.
  - Flexible access and services authentication
    - authentication by carriers alone, by service alone, or by both of them.

- **Identity management**
  - Combination of device and service identity
  - From device-based to user-based management
5G Security Perspectives—Service-oriented Security

- Build E2E security
  - Differentiated security for different services
  - Flexible security architecture to support security attributes for different network slices
  - A Uniformed security management framework for multi-vendor environment

- Open Up Security Capabilities, and provide security as a Service
- Isolate Virtual Network Slices
Security Assessment on 5G system:
- Assessment on interfaces
  - Interoperable for different vendors
- Assessment on network function unit
  - Private keys storage
  - Encryption/integration protection operation
  - password length and its complexity, etc
- Automatic verification
  - Certificate granted after success assessment

Security Assessment on 5G system:
- Interface assessment
- Unit tested by Security Assessment standard
- Certified unit
5G Security Perspectives -- Low-Delay Mobility Security

- **Mission Critical Connectivity**
  - Autonomous driving
  - Industrial automation and process control
  - Remote control
    - Manufacturing
    - Medicine
    - Maintenance
  - Traffic intensity monitoring

- **Security Requirements**
  - Low Delay
  - Ultra-High Reliable
  - Ultra-High Availability

- **Security Targets**
  - Build an efficient, lightweight, and compatible mobility security management mechanism
  - High Reliability while providing QoS guarantee with a delay not more than 1 millisecond
Security Perspectives -- Privacy Protection

- Big data techniques make privacy breach easier.
  - Attacker may collect user information from multiple channels.
  - Sensitive user information can be mined from seemingly harmless user information.
- The 5G network needs to manage the use of privacy information.
  - Define sensing rule clearly
  - Stipulate the use, storage and deletion of user information
- The 5G network needs to provide a more rigorous privacy protection scheme.
  - Protect user information in heterogeneous access networks
  - Protect user information in network functional entities from different vendors

Public 5G network
- Sensing user/service information for AAA and better service

- Attacker
- Collect data
- Mine privacy information from collected user data

Users
Summary

• Security and privacy protection need to be part of the system design at the beginning
  • Cannot be properly built as an add-on
  • Security and privacy community need to start active dialog with 5G stakeholders

• High level agreement can be obtained at the current stage
  • Including service layers in the security and privacy protection solutions.
  • Extend the hop-by-hop security to end-to-end security

• Security as services provides additional competitive strength to operators
  • Security is not a burden
  • Security provides competitive strength in 5G

• It’s time for security community and other stake holders of 5G to work together and come out a robust and proper security solution for 5G.
Thank you