Security in 5G – Conclusions and outlook

Stefan Schröder, Telekom Security
Bengt Sahlin, Ericsson
<table>
<thead>
<tr>
<th></th>
<th>Agenda Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>SBA security status in SA3</td>
</tr>
<tr>
<td>02</td>
<td>Signalling session conclusion</td>
</tr>
<tr>
<td>03</td>
<td>5G Phase-1 conclusion</td>
</tr>
<tr>
<td>04</td>
<td>5G Phase-2 outlook</td>
</tr>
<tr>
<td>05</td>
<td>Close of 5G Event - Lunch</td>
</tr>
</tbody>
</table>
SA3 Security goals for SBA

Simplified summary

1. Authentication, authorisation, antispoofing, traffic protection

Apply goal #1 during registration, discovery, communication

3. Establish edge proxy in 5G architecture

4. Authorisation at edge, NRF, and NF

5. Hop-by-hop plus end-to-end security for IPX

6. Security guidelines for new protocol stack
Registration and discovery of services

NSSF: Network Slice Selection Function
UDM: Unified Data Management
AUSF: Authentication Server Function
PCF: Policy Control function
AMF: Access and Mobility Management Function
SMF: Session Management Function
UPF: User plane Function
(R)AN: (Radio) Access Network
UE: User Equipment.
DN: Data network, e.g. operator services, Internet access or 3rd party services.
AF: Application Function
DSF: Data Storage network function.
NEF: Network Exposure Function
NRF: NF Repository Function

SBA: Service Based Architecture
SBI: Service Based Interface
Authorisation of NF service access
Framework based on OAuth 2.0

- Authorisation of ...
  - Registration and Discovery: by NRF
  - Service Access: by OAuth 2.0
- JSON Web Token (JWT, RFC 7519) for access
- NF Service Producer checks access token
- Same principle for roaming and non-roaming
- Described in TS 33.501 clause 13.3 and 13.4 (some details still missing)
Inter-operator signalling (API calls)
SEPP2SEPP security considering IPX intermediaries

SA3 work in progress, agreements as of week 21/2018

- Application-Layer Security on N32 with
  - End-to-end security setup between hSEPP and vSEPP
  - End-to-end integrity between HPLMN and VPLMN
  - End-to-end encryption of sensitive message contents (e.g. subscribers’ sess
  - Authenticated message modifications by trusted IPX intermediaries

- Security building blocks for N32
  - Server-side and client-side certificates
  - TLS
  - JOSE, JWE, JWS – JSON Object Signing and Encryption (RFC 7515 and 7)
  - JSON patch (RFC 6902)

- Exception to continue work on Rel-15 SBA security until September 2018
E2e signalling Message flow over N32

security principles, simplified
Let’s take the OpportunitY!

there is one chance for fundamental change every ten years

- Implement lessons learnt, right from the start
- Less fraud potential, if secure interconnection standardized as mandatory
- More detailed authorization concept
- Less complexity, due to common protocols
- Less protocol issues, due to wide use and exposure
- Best practices and experiences to draw from
- More convenient creation of test cases (OpenAPI)
Conclusions 5G Phase 1 security

what you’ll get

- Extensible authentication framework
- Support for different authentication methods and credentials for private networks
- Improved subscriber identity confidentiality
- Slicing
- Signalling security
- Not everything will be or needs to be standardized in 3GPP:
  - Policies like FW rules are up to the operator
  - Secure client credential store is up to vendor implementations
Topics for 5G Phase 2 security

Future work until mid of 2019

- Bug fixes for Phase 1 / Rel-15 :)
- Security for new service requirements and features, e.g. user centric identifiers and authentication (LUCIA)
- Security enhancements for small data and massive IoT
  - Evolution of Cellular IoT for 5G
  - Authentication and key management for applications in 5G IoT (similar to GBA?)
- Fixed-mobile convergence
  - Revisit user plane security termination points in architecture
- Security for single radio voice continuity from 5G to UTRAN
- Broadcast/multicast security
Topics for 5G Phase 2 security (continued)

Future work until mid of 2019

- Signalling security enhancements (eSBA)
  - Protection Policy between SEPPs
  - Filtering malicious messages
  - Security for 3rd party APIs
- Slicing enhancements
  - Slice management by 3rd parties
  - Slice isolation
- Security Assurance Specifications (SCAS) for 5G products
  - SCAS for network functions with SBI in general?
  - SCAS for SEPP?
Thank you!
Backup
Security Goal #1 for Release 15

Message origin authentication

“Who is the real sender?”

Message protection (integrity / confidentiality)

“Was the message modified/read?”

Cross-layer anti-spoofing enforcement

“Do identities used on different protocol layers all belong to the same sender?”

Message content authorization

“Is the consumer legitimizized to request or be subscribed to a specific service?”

Standardize all of these aspects in 5G
Cross-layer spoofing
Recurring problem due to simplicity (naivety?)

- Do upper layers confirm what lower layers are suggesting (and vice versa)?
- Ensure authentication/verification for several protocols
- Conflicting redundant IEs?
- Run multiple necessary checks w/o ruining performance
- Preferably no authentication at the NF itself
  - Improve authentication mechanism w/o NF impact
  - Shift possible brute-force attacks away from NF
Security Goal #2 for 3GPP Release 15

Goal #1 is relevant for all procedures during registration, discovery, and communication between NF Service Consumer and Producer.
A 5G signalling edge proxy is required to protect traffic crossing a security domain boundary, and thus needs to be included in the architecture.

Security Goal #3 for 3GPP Release 15

**SEPP**: Security Edge Protection Proxy
Authorization should consider the network edge, the NRF, and each NF.

Sender allowed to issue requests to “our” NF?

Sender allowed to discover a certain NF?

Sender allowed to request a certain service?

Sender allowed to send this specific request?

Edge Proxy

NRF

NF

NRF: Network Repository Function
Security Goal #5 for 3GPP Release 15

5G core network signalling needs to support hop-by-hop security for message transport, and end-to-end security for sensitive parts of messages.
Security Goal #6 for 3GPP Release 15

Define specific security requirements of the new signalling protocol stack, at least for JSON, and consider implementation recommendations.