3GPP SA3 - 5G SECURITY

Major changes in 5G security architecture and procedures | Sander de Kievit
SA3 is the working group tasked with security and privacy within the scope of 3GPP.

Study started at #83 with TR 33.899
- Overall topics identified
- Priorities set

Specification work started at #86-BIS
- New spec: TS 33.501
- First approved version (15.0.0) available soon
- Result of ‘phase-1’ work
MAJOR CHANGES IN 5G – AUTHENTICATION

- **Design Goals:**
  - Unified authentication framework for both 3GPP and non-3GPP access
  - Improved control by home network

- **Design Questions:**
  - How to deal with potentially different transport of NAS and EAP?
  - How to add home control to EPS AKA?
  - Authentication algorithm under control of 3GPP SA3?

- **Final design decisions:**
  - Both EAP AKA’ and newly developed 5G AKA supported
  - Continued compatibility with Rel-8 USIM
MAJOR CHANGES IN 5G – AUTHENTICATION

HOME CONTROL IN 5G AKA

- Based on EPS AKA
  - New authentication confirmation
  - New RES* and H(X)RES*

- Calculation of RES*:
  - KDF(CK, IK, SN name, RAND, RES*)
  - Calculated in ARPF and UE

- Calculation of HRES*:
  - HASH(RAND, RES*)
  - Calculated in SEAF and AUSF
  - Used for authentication by the SEAF
MAJOR CHANGES IN 5G – SUBSCRIBER PRIVACY

- **Design Goal:**
  - Defeating the IMSI catcher

- **Design Challenges:**
  - Scalable solution under control of operator
  - Comply with regulations
MAJOR CHANGES IN 5G – SUBSCRIBER PRIVACY

Solution:
- SUPI encrypted with home network public key on initial attach (SUCI)
- Complete authentication
- Then, send SUPI from HPLMN to VPLMN
- Finally, confirm SUPI by binding into a key

Further details:
- Encryption can done on UE or USIM
- Two algorithms standardized on UE side
- Algorithms on the USIM can be controlled by operators
MAJOR CHANGES IN 5G – KEY HIERARCHY

- Key hierarchy extended to also include:
  - $K_{AUSF}$ at home network
  - $K_{SEAF}$ at serving network

- Reasons for $K_{AUSF}$:
  - Fast reauthentication
  - Protecting home to UE traffic, e.g. steering of roaming under discussion

- Reasons for $K_{SEAF}$:
  - Separate security anchor from mobility anchor
  - Pre-empts AMF at insecure locations

Network side

- Home Network
  - $K_{AUSF}$

- Serving Network
  - $K_{SEAF}$
  - $K_{AMF}$
  - $K_{N3IWF}$
  - $K_{gNB, NH}$
  - $K_{RRCint}$
  - $K_{RRCenc}$
  - $K_{UPint}$
  - $K_{UPenc}$
  - $K_{NASint}$
  - $K_{NASenc}$

UE side

- 5G AKA
- EAP
  - AKA'
- $CK'$, $IK'$
MAJOR CHANGES IN 5G – INTERCONNECT SEC.

Design Goal:
Protecting messages exchanged between operators via the IPX network

Design Challenge:
Deal with the complex services of IPX providers:
- Rerouting of messages
- Mediation of messages
- Roaming hubs
- Providing PLMN to PLMN security
- Being compliant with JSON and HTTP2 standards
MAJOR CHANGES IN 5G – INTERFACE SEC.

Current status:
- ‘Agreed’ solution

Solution details:
- Introduction of SEPP at PLMN border
- Complete rewriting of messages before sending to IPX
- End-to-end integrity protection
- Some elements end-to-end confidentiality protected
- IPX changes recorded using JSON patch

WORK IN PROGRESS

NF

SEPP

IPX1

Rewrite message

IPX2

SEPP

Apply patches
Rewrite message

NF
WHAT’S NEXT?

› Who can predict the future?
› What is going on / agreed?
   › Security of slice management interfaces
   › Security assurance of 5G NF
   › Authentication and key agreement services for 5G
      › Also known as GBA and BEST for 5G
   › Cellular IoT / massive MTC security in 5G
      › Bringing LTE IoT optimizations and more to 5G
   › Fixed Mobile Convergence
   › …
SUMMARY

- Specifications to be approved soon
- Major changes since 4G:
  - Unified authentication framework for both 3GPP and non-3GPP access
  - Extended key hierarchy for later security services
  - Improved subscriber identity confidentiality
  - Security of the interconnect network between operators
    - Work in progress…
- This is only the beginning. Phase-2 will add more!
THANK YOU FOR YOUR ATTENTION

Take a look: TIME.TNO.NL