ERICSSON

S3z010127

3GPP SIP Security Requirements for IETF

Jari Arkko

Ericsson

Nice, France

13th-14th September 2001

Background

1. 3GPP has been developing new SIP solutions
2. IETF SIPPING WG requests for requirements before solutions can be discussed
   - Centralised requirements gathering from multiple organisations in order to co-ordinate development and control complexity
3. Only one version of SIP protocol is needed in order to guarantee interoperability and flexible development

How to proceed?

Two organizations must be able to work on the same thing

Let IETF in to the process sooner

Convince the IETF on the need for standard solutions even for our problems

How to proceed?

"Take requirements written in 3GPP specifications, de-3GPP-fied, IETF-ied, and write them down."

ERICSSON

Work in progress: 3GPP requirements on SIP

- CN1 has initiated an internet draft trying to capture the 3GPP SIP requirements
- IETF prefers all requirements in just one document
  - draft shall also include security requirements
  - (may include pointers to possible solutions if there is agreement that such solutions exists)
- Authors from CN1 including several organizations (Ericsson, Vodafone, Nokia, Siemens, Alcatel, AWS and Motorola)
- New co-authors are welcome!

ERICSSON

SIP Security

- Ericsson has defined preliminary security requirements to the document in order to accelerate the process
- Preliminary work is based on documents
  - 23.228 IP Multimedia (IM) Subsystem - Stage 2
  - 33.203 Access Security for IP-Based Services
  - 33.210 Network Domain Security
  - I-D: SIP security requirements from 3G wireless networks (draft-kroeselberg-sip-3g-security-req-00.txt)
- SA3 comments and contributions required!

IETF-ied Presentation

- Security Model
- Access Domain Security
  - Authentication
  - Scalability and Efficiency
    - Bandwidth and Roundtrips
    - Computation
    - Delegation of Security Tasks
  - Secure negotiation of mechanisms
  - Message protection
- Network Domain Security

Security Model

- MUST provide independent security from the underlying network
- MUST be possible to access the IMS services securely from other accesses
- Each operator acts as its own domain of trust, and shares a long-term security association with its subscribers
- Roaming agreements between operators
- A hop-by-hop model MUST be used to protect actual SIP signaling
- MUST allow separate access domain and network domain solutions

Access Domain Security (1/4)

- Authentication methods
  - MUST use strong, mutual authentication method
  - MUST provide legacy authentication methods
  - MUST support secure storage of long-term authentication keys

Access Domain Security (2/4)

- Scalability and Efficiency
  - bandwidth and roundtrips
    - SHOULD NOT unnecessarily increase the bandwidth needs
    - MUST minimize the number of necessary extra roundtrips
  - computation
    - MUST be possible to provide security without PKI
  - delegation of security tasks
    - MUST be possible to perform an initial authentication, followed by subsequent protected signaling that uses only session keys

Access Domain Security (3/4)

- Secure negotiation of mechanisms
  - MUST be possible to choose among several security services, and select parameters they might need
  - MUST be possible to protect the service and parameter negotiation against attackers

Access Domain Security (4/4)

- Message protection
  - MUST be able to communicate using integrity and replay protection
  - MUST be based on initial authentication
  - MUST be possible using symmetric cryptographic keys
  - MUST be possible to handle also error conditions in a satisfactory manner

Network Domain Security

- MUST provide
  - authentication
  - key agreement
  - integrity
  - replay protection
  - confidentiality
- security associations MUST be independent of the number of network elements

Time plan

- Preferred deadline for SA3 comments and contributions on security requirements during next week
- Submission to SIPPING WG beginning of October
- New security solutions will be developed in IETF SIP Security team and SA3
  - Contribution on both forums needed from the participating companies
- Goal: new SIP security solutions available around April 2002 (two IETF meetings)

Conclusion

- We need access security for Release 5
- We do not want to end-up with two SIP protocols
- N1 has taken the first rapid move to solve the problem
- SA3 contribution required
- In order to continue this path, SA3 support required