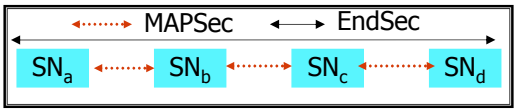
EndSec: An End-to-End Message Security Protocol for Mobile Telecommunication Networks

Kameswari Kotapati, Peng Liu, Thomas F. LaPorta
kotapati@cse.psu.edu, pliu@ist.psu.edu, tlp@cse.psu.edu

Security Problem: Cleartext Wireline Signaling Messages

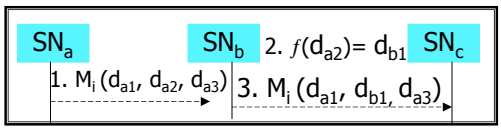
- Security Solution to Cleartext Wireline Signaling Messages : MAPSec
- MAPSec is Insufficient :
  - Only protects MAP Signaling messages and only on link
  - MAP messages are exposed in intermediate service nodes
  - All other signaling message protocols are unprotected on link and intermediate service nodes
- EndSec (End-to-End Security) proposed to protect all signaling message protocols on link and intermediate service node



EndSec Design Goals:

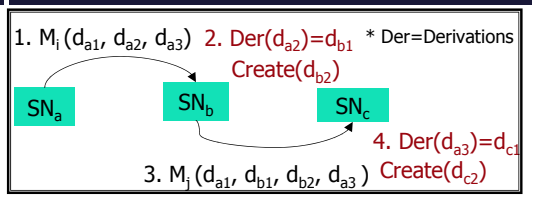
- Provide end-to-end security for all types of wireline signaling message protocols
- Detect and repair corruption
- Identify the service nodes causing corruption

Data Item Model



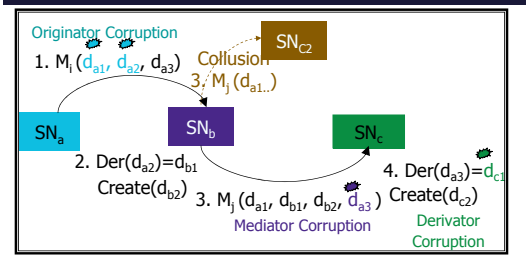
- Data Items valid for length of signal flow
- Data items have different destination service nodes
- Some data items have multiple destination service nodes
- They may be used to derive other data items (also called derivation operations)

Network Model



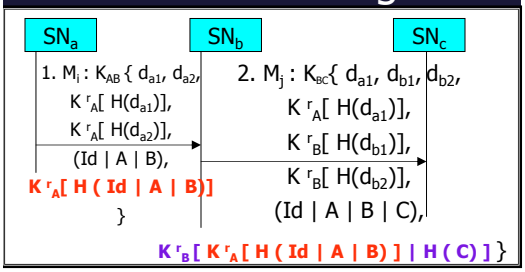
- Originator: Service node that creates data items unaided. A is the originator of data items d_{a1}, d_{a2}, d_{a3}
- Derivator: Service node that derives data items using data items created by others. B is the derivator of data item d_{b1}
- Mediator: Service node that simply pass on data items. B and C are mediators of data item d_{a1}

Attack Model



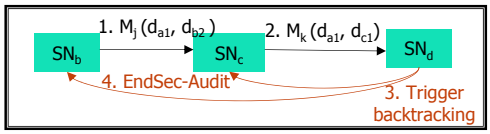
- Consider System Acceptable Incorrect Value Corruption
- Corruption by:
  - Originator, Mediator, Derivator
- Collusion based mis-routing
- Node Impersonation

EndSec Message



- Originators or Derivators encrypt data items using asymmetric keys
- Data Item encryption: authenticity, integrity and trace corruption source
- Record the PATH (Nested Path) taken by the signal flow
- PATH detects collusion based mis-routing and node impersonation attacks
- Perform EndSec Corruption check

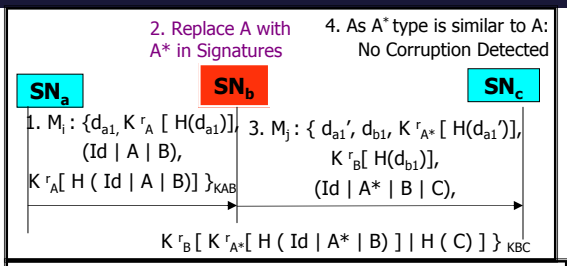
EndSec Corruption Check

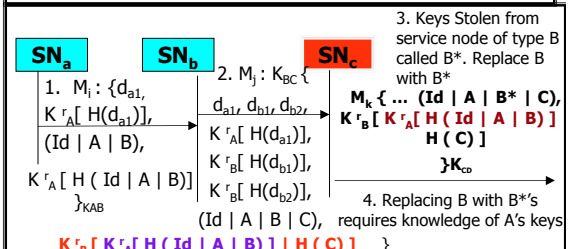


Detects corruption in received message using 5 phases:

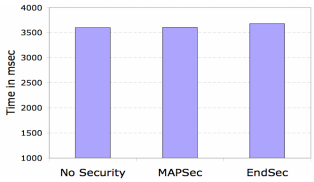
1. Signature Verify Phase: Detect corruption on Link
2. Originator and derivator check phase : Detect mediator corruption : Checking the service node type & position of originators and derivators.
3. Path check phase - Detect node impersonation, collusion based mis-routing by checking the PATH
   - Path service node type sequence ⇒ collusion misrouting
   - Discarding data items not signed by service nodes in PATH
4. Auto-audit phase - Detect originator and derivator corruption by automatic backtracking
5. Offline audit phase - Detect originator and derivator corruption by backtracking triggered manually

Nested Path & Node Impersonation



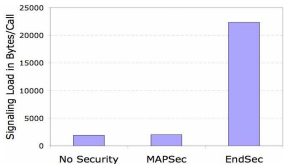


Time Delay Analysis



- MAPSec similar to "No Security"
- MAPSec is applied to MAP messages only
- EndSec applied to all the messages
- EndSec takes an extra 70 msec
- Extra time to sign and verify
- EndSec scales well with time

Signaling Load Analysis



- MAPSec similar to "No Security"
- EndSec much higher due to PATH and data signatures
- Public key signatures are rounded to nearest multiple of public key size
- For 128 byte RSA, its multiple of 128 bytes
- PATH size at nth node is 128*n
- Alternative use cross network signaling

Remarks

- EndSec is the first comprehensive solution for wireline network signaling messages.
- It is generic and can be applied to all types of messages.
- Uniqueness is the EndSec check based on the specifications.
- In the future, EndSec can be extended:
  - Devise better schemes to detect originator and derivator corruption.
  - Apply to other mobile networks

Sponsored by NSRC