One example approach for identifier privacy

Wed, Aug 3rd, 2005
63rd IETF, Paris, France

Pekka Nikander
Joint work with Jari Arkko and Mats Näslund

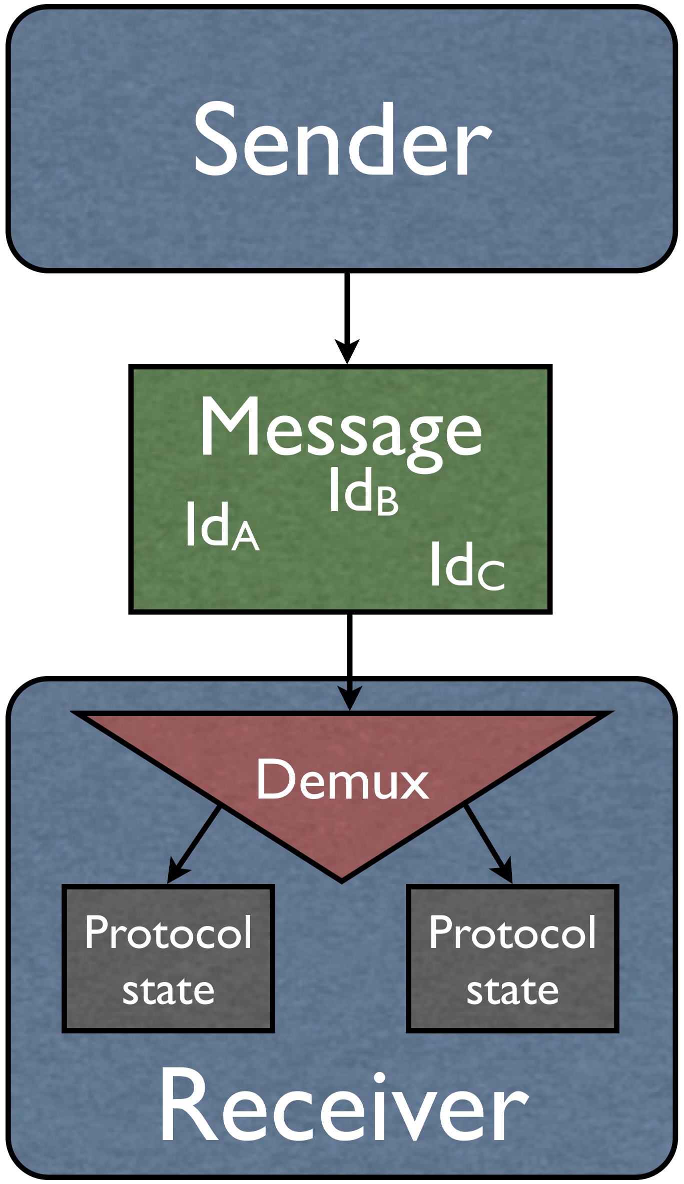
Note: No ID (paper available); may or may not be IPR

Presentation outline

- Identifiers everywhere
- Going random
    - Dealing with demultiplexing
- Mobility for free!?
- Summary

Identifiers everywhere

- Most protocols are full of fixed identifiers
  - IP addresses, IPsec SPIs, TCP/UDP ports, ...
- Needed for demultiplexing at the receiver
  - Determine the right context (state) for handling the packet
- Allow tracking of users, including mobile ones



Going random

- Replace identifiers with pseudo-random sequences
    - $ID \rightarrow \{ ID^0, ID^1, \ldots, ID^n \}, ID^i = f(K, i)$
- Create an *identically indexed* series for *each* externally visible identifier in the protocol
    - A set of IDs $\{ ID_A{}^k, ID_B{}^k, \ldots, ID_N{}^k \}$
- Also other data like *sequence numbers* should be considered as (predictable) identifiers

Timing

- All identifiers must be changed in synchrony
    - Partial info would be enough for tracking…
- Practical problem: When to go to the next set?
    - New identifiers in every packet?
        - But you can't change some identifiers easily, since they are not controlled by you
    - Whenever externally controlled identifiers, such as the IP address, change

Demultiplexing

- Fixed identifiers are used to denote the context
  - For IPsec, $< dst, SPI > \rightarrow SA$
  - For TCP, $< src, dst, sport, dport > \rightarrow TCB$
  - In general, $< ID_A, \ldots, ID_N > \rightarrow state$
- Random sequences necessitate many mappings
  - $< dst^i, SPI^i > \rightarrow SA; < dst^{i+1}, SPI^{i+1} > \rightarrow SA$
- Some identifiers may not be known beforehand
  - $< *, dst^{i+1}, sport^{i+1}, dport^{i+1} > \rightarrow TCB$

Conflicts

- Multiple parallel sessions may cause conflicts
  - $< dst_A{}^{i+1}, SPI_A{}^{i+1} > \equiv < dst_B{}^{i+1}, SPI_B{}^{i+1} >$
  - Note that the set $\{ dst* \}$ is small
- The more bits in the identifier space, the smaller the probability of conflicts
- Many conflicts will never be actualised!
  - E.g. because sequence numbers or other dynamic identifiers stop to conflict

Resolving conflicts

- Typically easy through (mis)using the protocol
- Example 1: IPsec
  - Problem: Two different SAs to pick from
  - Solution: Just try them all; see what works
    - And move to next set of identifiers
- Example 2: TCP
  - Problem: Two different TCBs to pick from
  - Solution: Move to next index send ACK in both, use the ACK to signal the peers to move to next index

Mobility for “free”!?

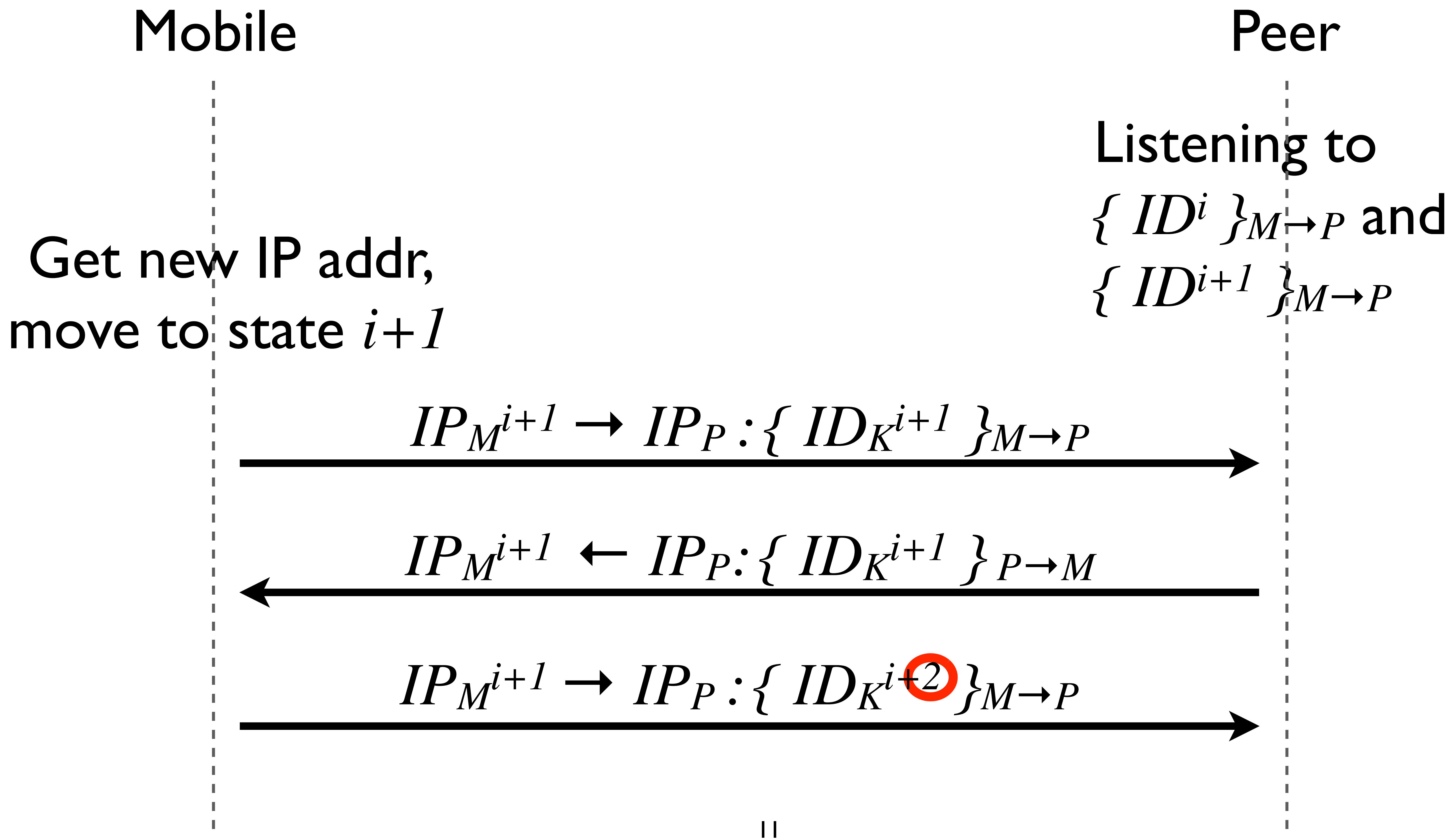
- What is network-layer mobility anyway?
- How do these two things relate?

Network-layer mobility

- Find your to-be-peer’s address
- Keep track of the peer’s address
- Recover from temporary loss of contact

- Local state keeping track of peer’s address
    - How to verify authenticity of updates?
        - Is the sender the actual peer?
        - Is the sender at the claimed new address?

Identifier sequences and mobility



Mobile

Peer

Listening to
$\{ ID^i \}_{M\rightarrow P}$ and
$\{ ID^{i+1} \}_{M\rightarrow P}$

Get new IP addr,
move to state $i+1$

$IP_M^{i+1} \rightarrow IP_P : \{ ID_K^{i+1} \}_{M\rightarrow P}$

$IP_M^{i+1} \leftarrow IP_P : \{ ID_K^{i+1} \}_{P\rightarrow M}$

$IP_M^{i+1} \rightarrow IP_P : \{ ID_K^{i+2} \}_{M\rightarrow P}$

Summary

- Simple idea: Replace static identifiers and other predictable data with sequences
- Receiver accepts data at the current and one or more next identifier sets
- Conflicts: low probability and can be managed
- Implicit origin authentication, no extra bits
    - “Zero-signalling” mobility
    - Securing all protocols, including TCP/UDP

Literature

- Farber et al: Network Security via Dynamic Process Renaming. Fourth Data Communications Symposium, Quebec City, Canada (1977, October)
- Kesdogan, et al: Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks, ESORICS 1998.
- Ylitalo et al: BLIND: A Complete Identity Protection Framework for End-points, Security Protocols, 12th International Workshop, Cambridge, April, 2004.
- Jari Arkko, et al, Enhancing Privacy with Shared Pseudo Random Sequences, Security Protocols, 13rd International Workshop, Cambridge, April, 2005