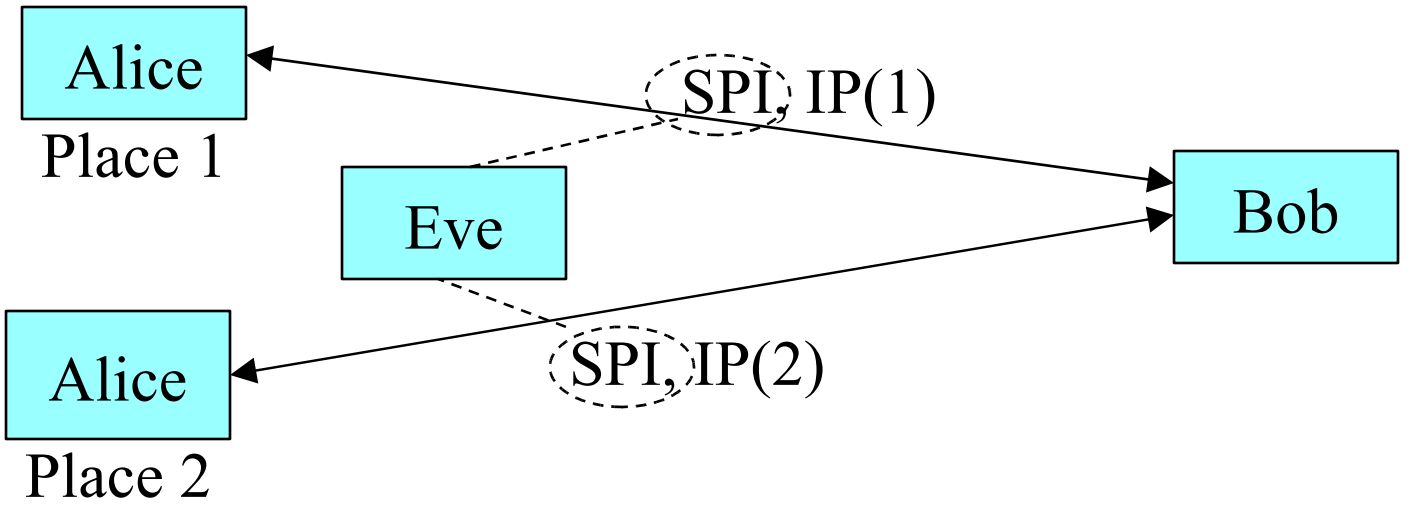
Enhancing Privacy with Shared Pseudo Random Sequences

A presentation of the paper
(http://www.tml.tkk.fi/~pnr/publications/cam2005-pre.pdf)
written by Jari Arkko, Pekka Nikander, and Mats Näslund

Jani Suomalainen
Helsinki University of Technology
Research Seminar on Datacommunications Software
28th September 2005

The Problem

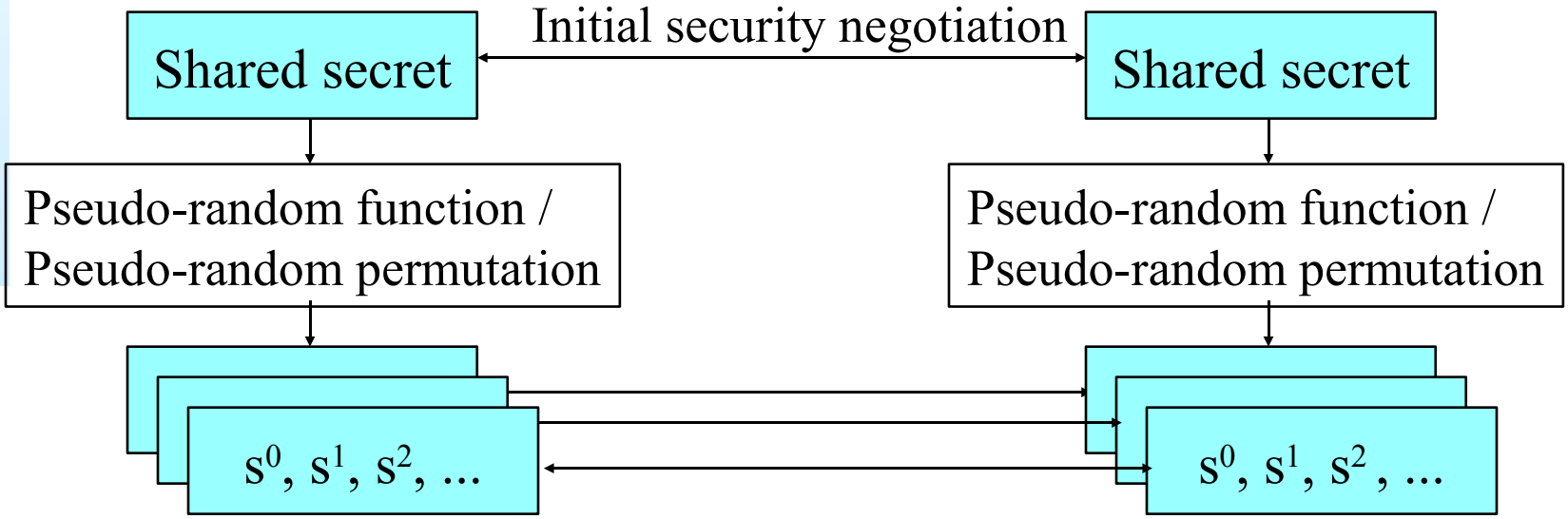
- *An attacker may collect privacy critical information by using identifiers, which link old and new values of other identifiers*
- *E.g. Alice moves and her IP address changes. However, IPSec SPI value remains and Eve can use it to find Alice's new IP address (and location)*



The Solution

- *Every identifiers must be changed at the same time to remove linkability*
- *The paper proposes a method for getting new identifiers*
- *The idea is to replace identifiers with pseudo random values, which are derived from a shared secret*
- *Advantage of the method is the efficiency in a sense of computational and routing cost*
  - *No signalling required to fetch new identifiers*
  - *No heavy computing due to public key / hash chain calculation*

Creating Shared Pseudo Random Sequences



- *All parties derive random sequences using a shared secret and random number generation method*
- *One sequence set provides identifiers, which are used at the same time*
- *Different sequence sets cannot be linked to each others*

Using Shared Pseudo Random Sequences

- *In communication:*
  - *The receiver expects identifiers belonging to the current or future sets*
  - *Consequently, the sender can start using a new random sequence set at anytime*
- *Idea of Shared Pseudo Random Sequences may be applied to protect other parameters like public key traces, hash chains and Mobile IP home addresses*

Problems Identified in the Paper

- *The deployment may require some changes:*
  - *Mechanisms for agreeing on using the method*
  - *Local changes to protocol implementations*
- *The problem of linkability must be considered separately for different protocols*
  - *Therefore, IETF interest group (BOF) has proposed some work (www.ietf.org/ietf/05aug/alien.txt)*
- *It is possible that identifier belonging to different nodes may collide (same sequence is used by different hosts)*
  - *Collision cost depends on the protocol*
- *State preserving network access control solutions, firewalls, NATs may have a problem with frequently changing nodes*

An Attack Against the Proposed Method

- *All identifiers cannot be changed: Bob's (receiver's) address will remain and may compromise the privacy*
- *For instance, Eve sees that Bob is first communicating with Alice and then with someone else*
  - *Eve can guess that this someone is Alice (but cannot be sure since this someone could also be Carol, who just logged in at the same time when Alice initiated identifier change, or Dave, who initiated identifier change at the same time as Alice)*
- *To handle the problem, Bob should have several simultaneous communications. Perhaps, Bob should also initiate use of new sequences with other peers at the same time when Alice initiates a change*

Summary & Conclusions

- *The paper proposed a method for achieving privacy against third-party eavesdroppers by changing all identifying information at the same time in an efficient manner*
- *The method can be applied to e.g. cases where a mobile user, who wants to protect location information, is accessing a server, which has several clients*

Thank You!

- *Questions...*
- *Comments...*
- *Discussion...*