CAM

Author(s): Greg O'Shea and Michael Roe April 2001
Submitted by Michael Roe January 10, 2003
Last modified November 28, 2002

Summary: A protocol used by mobile computers to inform their peers when their network address has changed.

Protocol specification (in common syntax)

```
M,C :    principal
Tm :     timestamp
PK,SK :  principal -> key (keypair)
HoA :    principal -> address
CoA :    principal -> address
i :      salt

1.    M  ->  C  :    CoA(M), HoA(C), HoA(M), PK(M), i, Tm,
                     {H(CoA(M), HoA(C), HoA(M), Tm)}SK(M)
      HostPart(HoA(M)) = H(PK(M), i)
```

Description of the protocol rules

Each mobile node (M) generates a key pair PK(M), SK(M). M then generates a home address HoA(M) by concatenating the routing prefix of its home network with a hash of PK(M) and a salt i. HoA(M) serves two purposes. It is used by the correspondent C as an identifier for M, and it is a routable network address that can be used to contact a home agent that will forward messages on to M. The places where M can be attached to the network are also given identifiers; CoA(M) is the identifier of M's current network attachment point. CoA(M) varies over time. M knows (by means outside the protocol) when CoA(M) changes.

M has a set of correspondents that it wishes to communicate with. The set of M's correspondents varies over time.

M runs the protocol with C when any of these events happens:

- CoA(M) changes and C is one of M's correspondents
- M adds C to its set of correspondents
- C is one of M's correspondents, and time delta1T (as measured by M's local clock) has elapsed since M last ran the protocol with C

Each correspondent C maintains a table mapping home addresses HoA(M) to care-of addresses CoA(M). This is a partial table — there can be home addresses HoA(M) that do not have an entry in the table.

When C receives message 1, it will check that the timestamp Tm is within delta2T of the current time (as measured by C's local clock); that the home address satisfies the relation HostPart(HoA(M)) = H(PK(M), i); and that the signature can be verified with PK(M). If all of these checks pass, C adds the pair to (HoA(M),CoA(M)) to its table, replacing the previous entry for HoA(M) if one exists.

If C has not accepted a valid message containing HoA(M) within the last Delta3T seconds, then it will remove the entry for HoA(M) from its table.

The local clocks of M and C are assumed to be loosely synchronised. That is, there exists a Delta4T such that the times measured by C and M's clocks are within Delta4T of each other. Clocks are assumed to be monotonically increasing.

Requirements

There is a time interval DeltaT such that if CoA(M) has not changed within the last DeltaT seconds, and both C and M are following the protocol, then either C's table does not contain an entry for HoA(M) or C's table contains (HoA(M), CoA(M)).

References

This protocol was described by O'Shea and Roe in Computer Communications Review [OR01]. A concrete realisation of this protocol is given in the first version of the Internet draft draft-roe-mobileip-updateauth-00.txt ([RAOA02]); later versions of this document describe a different protocol that meets additional requirements. The idea of constructing IPv6 addresses from the hash of a public key was proposed by Christian Huitema [Hui98], Jeff Schiller and others.

Related protocols have been proposed by Bradner, Mankin and Schiller [BMS02], Montenegro and Castelluccia [MC02] and Nikander [Nik01, NYW03].

Remark

Authentication of the principal M is not a goal of this protocol. Although C cannot necessarily distinguish a run of the protocol with M from a run of the

protocol with a different principal, this is not an attack.

If authentication of `M` is desired, the protocol can be used in conjunction with an additional protocol that authenticates `M`.

Runs of the protocol in which `M` tries to run the protocol with `C`, but `C` does not create a table entry (e.g. because an attacker prevents the message from reaching `C`) are also not attacks. It is an assumption of the protocol that the absence of a table entry for `HoA(M)` is "fail safe" and does not correspond to an insecure state. The table entry is used for an optimisation only; if it is not present, `C` has an alternative method of proceeding without it.

Citations

[BMS02] Scott Bradner, Allison Mankin, and Jeffrey I. Schiller. A framework for purpose built keys (PBK). Internet draft, November 2002.

[Hui98] Christian Huitema. *IPv6 The New Internet Protocol*. Prentice Hall PTR, 1998.

[MC02] G. Montenegro and C. Castelluccia. Statistically Unique and Cryptographically Verifiable (SUCV) identifiers and addresses. In *Network and Distributed Systems Security Symposium*. Internet Society, February 2002.

[Nik01] Pekka Nikander. Denial-of-service, address ownership, and early authentication in the IPv6 world. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Security Protocols*, number 2467 in Lecture Notes in Computer Science. Springer, 2001.

[NYW03] Pekka Nikander, Yukka Ylitalo, and Jorma Wall. Integrating security, mobility and multi-homing in a HIP way. In *Network and Distributed Systems Security Symposium*, 2003.

[OR01] Greg O'Shea and Michael Roe. Child-proof authentication for MIPv6 (CAM). *Computer Communications Review*, April 2001.

[RAOA02] M. Roe, T. Aura, G. O'Shea, and J. Arkko. Authentication of mobile IPv6 binding updates and acknowledgments. Internet draft, February 2002.