Electronic Notes in Theoretical Computer Science 83 (2004)
URL: http://www.elsevier.nl/locate/entcs/volume83.html 2 pages

# Designing a Group Protocol Specification Language

Jonathan Millen and Grit Denker

*SRI International*
*333 Ravenswood Ave*
*Menlo Park, CA 94025 USA*
{millen,denker}@csl.sri.com

Formal methods such as model checking can be applied to gain design assurance in the security of cryptographic group management protocols, just as they have been used to analyze unicast security protocols between two parties. MuCAPSL (Multicast Common Authentication Protocol Specification Language) is a high-level application-oriented language. It can be translated into an intermediate form (MuCIL) with rewrite-rule semantics [DM02], which is close to the the input representation needed by many analysis tools. MuCAPSL is a formal specification language and not an implementation language, so it can be relatively abstract.

MuCAPSL is based on an earlier language CAPSL for unicast protocols, which in turn attempted to follow the textbook "Alice-Bob" message list style of protocol presentation, with strong typing and security goal declarations [DM00]. As with CAPSL, the MuCAPSL translator checks for implementability of protocol steps, which is a challenge when the processing of received messages is specified implicitly and somewhat ambiguously in a symbolic pattern-matching style [MD03]. MuCAPSL differs from CAPSL by requiring an encoding of persistent state information associated with group members across multiple tasks, and by necessarily moving from the shared message-list style to a role-process style [MD02]. The web site [WWW] has supporting documents.

## References

[1] G. Denker and J. Millen. CAPSL integrated protocol environment. In *DARPA Information Survivability Conference (DISCEX 2000)*, pages 207–221. IEEE Computer Society, 2000.

[2] G. Denker and J. Millen. Modeling group communication protocols using multiset term rewriting. In *4th International Workshop on Rewriting Logic and its Applications*, volume ENTCS 71. Elsevier, 2002.

[3] J. Millen and G. Denker. CAPSL and MuCAPSL. *Journal of Telecommunications and Information Technology*, (4):16–27, 2002.

[4] J. Millen and G. Denker. MuCAPSL. In *DISCEX III, DARPA Information Survivability Conference and Exposition*, pages 238–249. IEEE Computer Society, 2003.

[5] `www.csl.sri.com/users/millen/capsl`.