Network Protocols

Jack Wilburn

Protocols
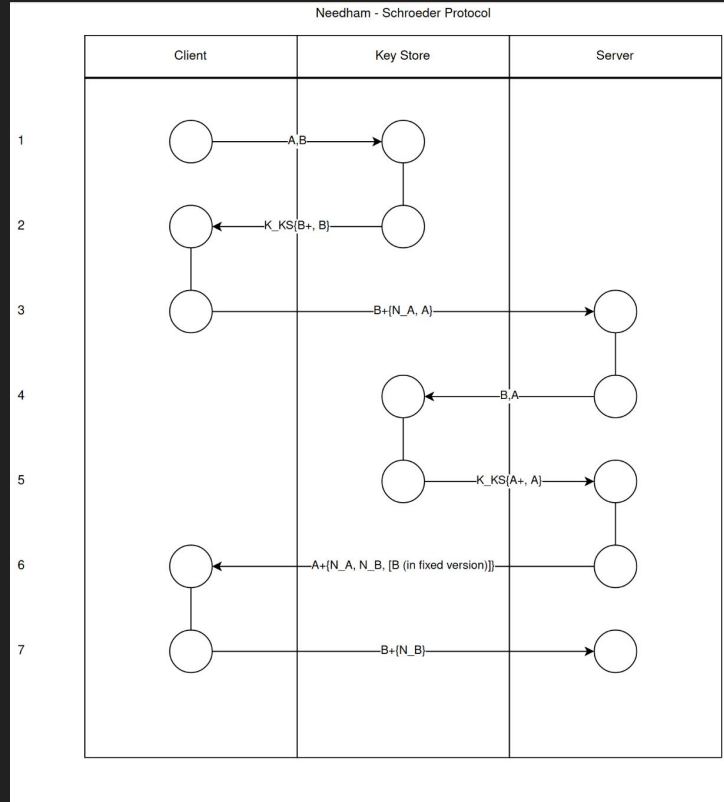
- Needham-Schroeder

- OpenID 2.0

Given models

- Content Centric Networking (CCN)

I modeled

Needham-Schroeder
Murphi + Promela

Needham-Schroeder

Needham - Schroeder Protocol

Client	Key Store	Server

1 A, B

2 K_KS{B+, B}

3 B+{N_A, A}

4 B, A

5 K_KS{A+, A}

6 A+{N_A, N_B, [B (in fixed version)]}

7 B+{N_B}
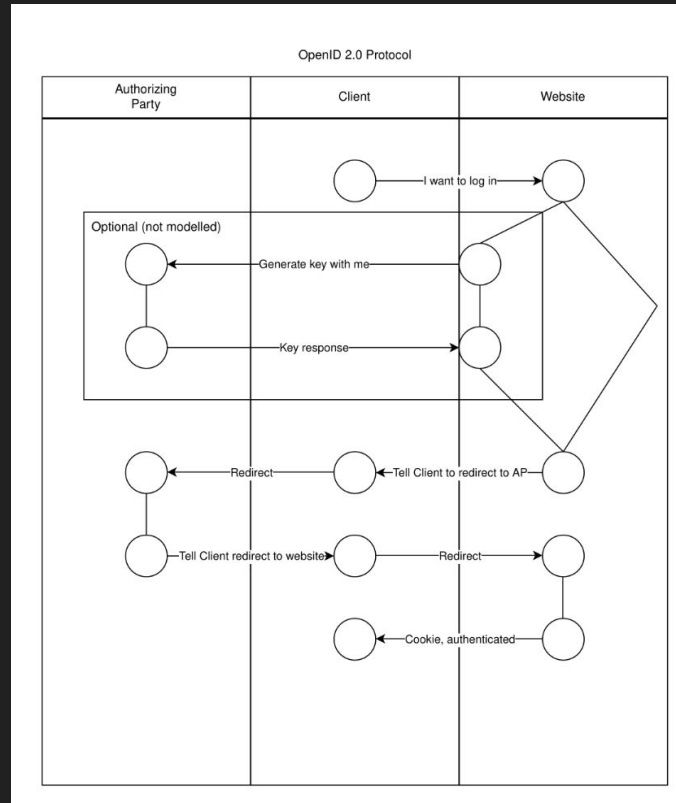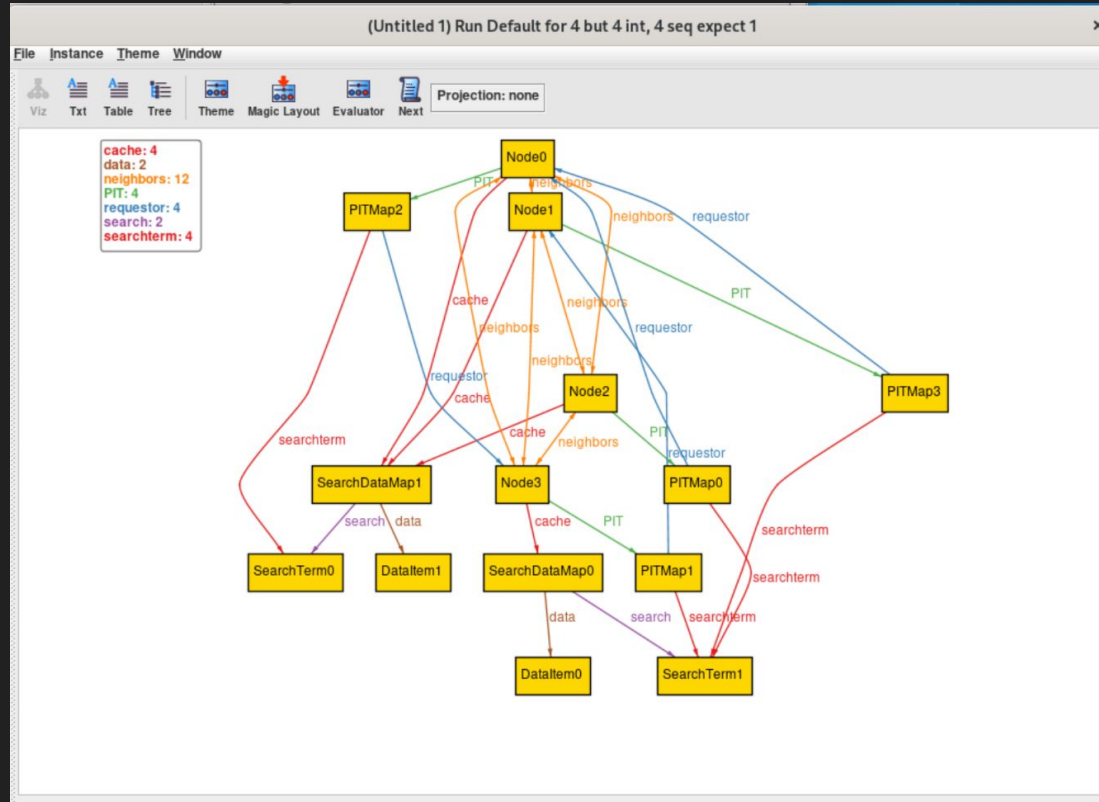
OpenID 2.0
Murphi

OpenID 2.0

Content Centric Networking Alloy

Content Centric Networking (CCN)

- IP - Request an address and path
- CCN - Request data

- Routing - Cache on intermediary nodes
- Aggregate requests - for multiple clients send 1 request for data and duplicate response packet

- DDOS resiliency

Content Centric Networking (CCN)

References

- [1] Van Jacobson et al. "Networking Named Content". In: Commun. ACM 55.1 (Jan. 2012), pp. 117–124. issn: 0001-0782. doi: 10.1145/2063176.2063204. url: https://doi.org/10.1145/2063176.2063204.
- [2] Shivaram Lingamneni and Ben Newman. SecLab: CS259 (Winter 2007-08) Student projects. url: https://seclab.stanford.edu/pcl/cs259/projects.htm.
- [3] Gavin Lowe. "An attack on the Needham-Schroeder public-key authentication protocol". In: Information Processing Letters 56.3 (1995), pp. 131–133. issn: 0020-0190. doi:https://doi.org/10.1016/0020 - 0190(95)00144 - 2. url: https :// www.sciencedirect. com/science/ article/ pii/0020019095001442.
- [4] Catherine Meadows. "Analyzing the Needham-Schroeder Public-Key Protocol: A Comparison of Two Approaches". In: Proceedings of the 4th European Symposium on Research in Computer Security: Computer Security. ESORICS '96. Berlin, Heidelberg: Springer-Verlag, 1996, pp. 351–364. isbn: 3540617701.
- [5] Ulrich Stern. Needham-Schroeder Protocol in Murphi. url: https://seclab.stanford.edu/pcl/mc/murphi_models/