servers, voice mail systems, etc. in which the code may be more difficult to change due to its heritage or due to feature interactions. This can potentially lead to "make-do" implementations of SSO that are more vulnerable to attack. As an example, it was mentioned earlier in the identity mapping discussion that within a UC solution, a given user may have multiple IDs including a numeric ID to be entered from the telephone. The numeric ID is typically associated with a numeric password or personal identification number for ease of entry on the telephone as well. When soft clients that run on PCs or tablets are developed, they may continue to use a numeric ID and password for ease of interfacing with the telephony call server. If the soft client is integrated into the UC SSO scheme and becomes the point from which the user initiates SSO, there is a question of how much additional access to other applications should be allowed.

IX. SUMMARY AND CONCLUSIONS

In this paper, we have discussed several approaches to providing SSO for multiple UC applications based on different protocols. SSO to SIP and HTTP-based applications and SSO for IMAP, SMTP and LDAP were examined as specific examples. A number of environmental considerations were also explored, such as user provisioning / identity mapping, federation with other identity providers deployed or used by enterprises, and unifying network and application level access.

It is observed that providing centralized password management, making the result of application authentication dialogs known to identity providers, and sharing authentication state among several applications running on an endpoint are the key work items in bringing SSO to non-HTTP protocols.

It was also highlighted that SSO can become a single point of attack if not properly secured, and UC SSO is potentially even more vulnerable due to the involvement of multiple protocols, communication devices and sometimes legacy telecommunications products. Focus on maintaining strong security is essential for credible UC SSO implementations.

Given the importance of SSO in providing a unified user experience (the “U” in “UC”), it is perhaps surprising that this topic has not received much research attention so far. The authors think that SSO for UC is an area that deserves more work, particularly in blending protocol-level design approaches with practical usage considerations and constraints in UC deployments to provide highly usable and secure SSO support for a variety of UC scenarios.

ACKNOWLEDGMENT

Ping Lin, Sunil Menon and Shailesh Patel would like to thank Ravi Palaparthi, Director of System Management and Monitoring, and our colleagues David Ahrens, Steve Warren, and Witold Kaczmarek at Avaya Inc. for discussing and working together on topics related to this paper.

REFERENCES

[1] OpenAM 10 Administration Guide, Lysaker, Norway: Forgerock AS, http://openam.forgerock.org/doc/admin-guide/index.html, 2011-2012

[2] Sun OpenSSO Enterprise 8.0 Technical Overview, Santa Clara, CA: Sun Microsystems Inc., 2008

[3] Security Assertion Markup Language (SAML) V2.0 Technical Overview, OASIS Community Draft 02, Mar. 2008

[4] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, Mar. 2005

[5] RADIUS Extension for Digest Authentication, IETF RFC 5090, Feb. 2008

[6] HTTP Authentication: Basic and Digest Access Authentication, IETF RFC 2617, June 1999

[7] P. Nie, J. Tapi, S. Tarkoma, J. Heikkinen, “Flexible Single Sign-On for SIP: Bridging the Identity Chasm”, Proc. IEEE International Conference on Communications, 2009

[8] Simple Authentication and Security Layer (SASL), IETF RFC 4422, June 2006

[9] “The Kerberos Network Authentication Service (V5)”, IETF RFC 1510, Sept. 2003

[10] “A SASL and GSS-API Mechanism for SAML”, IETF draft, http://tools.ietf.org/html/draft-ietf-kitten-sasl-saml-09.txt, Feb. 2012

[11] Wang, R., Chen, S., Wang, X.: Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided SecurityStudy of Commercially Deployed Single-Sign-On Web Services, Proc. IEEE Symposium on Security and Privacy, May 2012

[12] Juraj Somorovsky, Andreas Mayer, Jörg Schwenk, Marco Kampmann, Meiko Jensen, "On Breaking SAML: Be Whoever You Want to Be", Proc. 21st USENIX Security Symposium, Aug. 2012.

