System and Data Security - A CS Systems Prelim

PROPOSAL

Andy Sayler
University of Colorado Boulder, Colorado
andy.sayler@colorado.edu

1. PROPOSAL

I propose that my CS System PhD Prelim exam focus on system and data security. My exam will build on the background work completed in my Master's Thesis [10], further extending my analysis of the current state of the art and hypothesizing on future extensions to this state. This prelim will be overseen by Prof. Dirk Grunwald, with the help of committee members Prof. Eric Keller and Prof. John Black.

This exam will approach the topic of system and data security from four core areas: cryptography, access control, file systems, and management. System and data security is an inherently large topic: narrowing the focus to these core topics will help to keep the exam size manageable. In particular, this exam seeks answers to the question: "How can we secure our systems and data in a robust, comprehensive, and easy-to-use manner?". This question in examined from a historical perspective as well as the perspective of a modern user with modern use cases.

This exam will focus on the work presented in ten papers representative of the prior art. On the topic of cryptography, I will present the basics or modern cryptographic systems [3], extensions to these systems to accommodate the diversification of trust [11], and the manner in which these core concepts can be leverage in access control applications [1]. On the topic of access control, I will present the basics of modern access control models [9], the ways in which these models can incorporate cryptography to avoid the need for a trusted compute base [1], and the manner in which various access control schemes have been applied to modern file systems [6]. On the topic of file systems, I will present an effort to support file system distribution with minimal trust [5], an overview of the security mechanism employed by a range of modern file system [4], and the manners in which modern file system implement access control [6]. Finally, on the topic of management, I will present an early effort to standardize the basic system security primitives [8], techniques for making security more robust and simpler for the end user to leverage [2], and modern efforts to unify security primitives across multiple administrative domains [7]. These ten papers are by no means the complete body of prior art, but they do elucidate the core concepts relevant to the question at the core of this exam.

CU CS Systems Prelim, Spring 2014.

University of Colorado, Boulder
03/2014.

2. REFERENCES

[1] Bethencourt, J., Sahai, A., and Waters, B. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy, 2007* (May 2007), IEEE, pp. 321–334.

[2] Cox, R., Grosse, E., Pike, R., Presotto, D., and Quinlan, S. Security in Plan 9. In *USENIX Security* (2002), pp. 3–16.

[3] Diffie, W., and Hellman, M. E. New directions in cryptography. *IEEE Transactions on Information Theory 22*, 6 (Nov. 1976), 644–654.

[4] Kher, V., and Kim, Y. Securing distributed storage: challenges, techniques, and systems. In *Proceedings of the 2005 ACM workshop on Storage security and survivability* (New York, New York, USA, 2005), ACM Press, p. 9.

[5] Mazières, D., Kaminsky, M., Kaashoek, M. F., and Witchel, E. Separating key management from file system security. *ACM SIGOPS Operating Systems Review 33*, 5 (Dec. 1999), 124–139.

[6] Miltchev, S., Smith, J. M., Prevelakis, V., Keromytis, A., and Ioannidis, S. Decentralized access control in distributed file systems. *ACM Computing Surveys 40*, 3 (Aug. 2008), 1–30.

[7] Morgan, R. L. B., Cantor, S., Carmody, S., Hoehn, W., and Klingenstein, K. Federated Security: The Shibboleth Approach. *Educause Quarterly 27*, 4 (2004), 12–17.

[8] Samar, V. Unified login with pluggable authentication modules (PAM). In *Proceedings of the 3rd ACM Conference on Computer and Communications Security* (New York, New York, USA, 1996), ACM Press, pp. 1–10.

[9] Sandhu, R. S., Coynek, E. J., Feinstein, H. L., and Youman, C. E. Role-Based Access Control Models. *IEEE Computer 29*, 2 (1996), 38–47.

[10] Sayler, A. Custos: A Flexibly Secure Key-Value Storage Platform. Master's thesis, University of Colorado Boulder, December 2013.

[11] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (Nov. 1979), 612–613.