Project Proposal for an Intrusion Tolerant Threshold Cryptographic (ITTC) System

Kamran Riaz Khan,
Department of Telecom Engineering,
National University of Computer and Emerging Sciences,
Islamabad,
Pakistan.
krkhan@inspirated.com

15 February, 2010

Abstract

An ITTC system works on principles of distributive secret sharing. Instead of sharing a secret key among several parties which would be reconstructed upon requirement, threshold cryptography relies on sharing of cryptographic functions so that the secret key is never constructed in one place. This project aims to incorporate threshold cryptographic functionalities in two of the most important cryptographic services: web servers and certificate authorities.

1 Introduction

Any implementation of a public-key cryptographic system depends critically upon two factors concerning the private key:

- `Reliability` - Loss of private key renders the whole system unusable for all transactions and applications involving that particular key.
- `Confidentiality` - Similarly, any successful attempt of compromising the private key undermines the whole system.

Threshold cryptography attempts to address these concerns by distributing the signing process among multiple parties. Such an implementation addresses both of the aforementioned issues. For example, we can use a (k, n) threshold scheme with $n = 2k - 1$ to confront these concerns (1):

- `Reliability` - The system continues working even when $[\frac{n}{2}] = k - 1$ of n components are defective.
- `Confidentiality` - An adversary cannot compromise the system even if a security breach exposes $[\frac{n}{2}] = k - 1$ of the remaining k components.

Shamir has described a simple (k, n) threshold scheme in his 1979 paper which relies on polynomial interpolation in a 2-dimensional plane (1). However, the technique is useful only for threshold cryptography based on single-secret sharing. De Santis, Desmedt, Frankel and Yung have presented an efficient threshold function sharing protocol for RSA (2). Wu, Malkin and Boneh have described and implemented an intrusion tolerant system with working prototypical applications (3).

2 Deliverables

2.1 Shared Server Daemon

Unix daemon which provide threshold cryptographic capabilities to its clients. The processes would be controllable from a remote administration server as well as local configuration tools.

2.2 Interface Library

A shared library for utilizing the ITTC daemon functionalities. The library will be preloaded to override polymorphic functions for RSA signing.

2.3 OpenSSL and lighttpd Modifications

OpenSSL source code will be modified in order to use the interface library for shared certificate generation. Similarly, lighttpd web server's source code will be modified for revamping the HTTPS infrastructure.

3 References

[1] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, pp. 612–613, Nov. 1979.

[2] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung, "How to share a function securely," in *Proceedings of the twenty-sixth annual ACM Symposium on the Theory of Computing: Montréal, Québec, Canada, May 23–25, 1994* (ACM, ed.), (New York, NY 10036, USA), pp. 522–533, ACM Press, 1994. ACM order no. 508930.

[3] T. Wu, M. Malkin, and D. Boneh, "Building intrusion tolerant applications," in *Proceedings of the 8th conference on USENIX Security Symposium*, (Berkeley, CA, USA), pp. 7–7, USENIX Association, 1999.