

most commonly used algorithm today for integrity based on Merkle trees, including defense against replay attacks. Through our evaluation on some typical files from a Linux distribution and the NFS traces collected at Harvard University by Ellard et al., we demonstrate that each algorithm is best suited for a particular class of file-system workloads.

Lazy revocation in cryptographic file systems

Summer 2005

We consider the problem of efficient key management and user revocation in cryptographic file systems that allow shared access to files. We formalize the notion of key-updating schemes for lazy revocation, an abstraction to manage cryptographic keys in file systems with lazy revocation. The cryptographic keys generated by key-updating schemes can be used with either a symmetric encryption algorithm to encrypt files for confidentiality or with a message-authentication code to authenticate files for integrity protection. We give a security definition for key-updating schemes, several constructions and composition methods that combine two secure key-updating schemes into a new a secure scheme that permits a larger number of user revocations. We demonstrate through our evaluation that the novel binary tree construction proposed performs several orders of magnitude better than the existing key management schemes.

Consistency of encrypted files

Fall 2004 - Spring 2006

The consistency of the encrypted file objects in a cryptographic file system relies on the consistency of the two components used to implement them: the file storage protocol and the key distribution protocol. We formally define consistency for encrypted file objects in a generic way: for any consistency conditions for the key and file objects belonging to two generic classes of consistency conditions, we define a corresponding consistency condition for encrypted file objects. We provide in our main result necessary and sufficient conditions for the consistency of the key distribution and file storage protocols under which the encrypted storage is consistent. Our framework allows the composition of existing key distribution and file storage protocols to build consistent encrypted file objects and simplifies complex proofs for showing the consistency of encrypted storage.

Securing a remote terminal application with a trusted device

Summer 2003

We have designed and implemented a secure remote terminal application, in which users storing their credentials on a trusted device (e.g., PDA) can delegate their credentials temporarily to an untrusted terminal for accessing remotely their home computing environment, without disclosing any long-term secrets. In our implementation, the overhead in network traffic created by introducing the PDA as a trusted party is moderate.

Automatic generation of two-party cryptographic protocols

June 2002 - Fall 2003

We have designed and implemented a compiler that automatically generates two-party protocols, starting from a cryptographic function specification. To our knowledge, this is the first automatic tool for generating two-party cryptographic protocols. The protocols generated are provably secure. Several applications of the compiler include, but are not limited to, signature schemes, encryption schemes and oblivious transfer protocols. We have implemented the compiler that generates two-party signature schemes in Java.

PUBLICATIONS Conference papers

Alina Oprea, and Michael K. Reiter. On consistency of encrypting files. In Proc. of the 20th International Symposium on Distributed Computing (DISC 2006).

Michael Backes, Christian Cachin, and Alina Oprea. Secure key-updating for lazy revocation. In Proc. of the 11th European Symposium On Research In Computer Security (ESORICS 2006).

Michael Backes, Christian Cachin, and Alina Oprea. Lazy revocation in cryptographic file systems. In Proc. 3rd Intl. IEEE Security in Storage Workshp (SISW 2005).

Alina Oprea, Michael K. Reiter, and Ke Yang. Space-Efficient Block Storage Integrity. In Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS 2005). Received **Best Paper Award**.

Alina Oprea, Dirk Balfanz, Glenn Durfee, and Diana K. Smetters. Securing a Remote Terminal Application with a Mobile Trusted Device. In Proceedings of the Annual Computer Security Applications Conference (ACSAC 2004).

Lea Kissner, Alina Oprea, Michael K. Reiter, Dawn Song, and Ke Yang. Private Keyword-Based Push and Pull with Applications to Anonymous Communication. In Proceedings of the 2nd Conference of Applied Cryptography and Network Security (ACNS 2004).

Philip MacKenzie, Alina Oprea, and Michael K. Reiter. Automatic Generation of Two-Party Computations. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003).

Technical reports

Alina Oprea, and Michael K. Reiter. Integrity Checking in Cryptographic File Systems with Constant Trusted Storage. Technical Report CMU-CS-06-167, Carnegie Mellon University, November 2006.

Alina Oprea, and Michael K. Reiter. On consistency of encrypting files. Technical Report CMU-CS-06-113, Carnegie Mellon University, March 2006.

Michael Backes, Christian Cachin, and Alina Oprea. Secure key-updating for lazy revocation. Research Report RZ 3627, IBM Research, August 2005.

Michael Backes, Christian Cachin, and Alina Oprea. Lazy revocation in cryptographic file systems. Research Report RZ 3628, IBM Research, August 2005.

PROFESSIONAL SERVICE Reviewer for IEEE Transactions on Dependable and Secure Computing, ACSAC 2005, DISC 2005, INDOCRYPT 2005, ISPEC 2005, NDSS 2006, IEEE Symposium on Security and Privacy 2006, NDSS 2007.

EXPERIENCE **Carnegie Mellon University** Fall 2001 - present

- Research assistant performing research in applied cryptography and storage security.
- Designed new integrity algorithms for cryptographic file systems and implemented them in the EncFS cryptographic file system. Compared their performance with the widely used Merkle tree algorithm using a file trace from a typical Linux distribution and the NFS traces collected at Harvard university.
- Designed new integrity algorithms for block-level encrypted storage systems and evaluated them on a one-month trace collected from one desktop machine.
- Defined formally consistency of encrypted files and gave necessary and sufficient conditions for its realization.
- Designed and implemented a compiler that automatically generates two-party signature schemes given a signature specification.

IBM Zurich Research Laboratory, Switzerland Summer 2005

- Developed new key management algorithms for cryptographic file systems using lazy revocation.

Carnegie Mellon University Spring 2005

- Teaching Assistant for the freshman-level “Great Theoretical Ideas in Computer Science” course.

Palo Alto Research Center, Palo Alto, CA

Summer 2003

- Designed a secure remote terminal application using a mobile trusted device, as part of the Whisper project.

Carnegie Mellon University

Fall 2002

- Teaching Assistant for the graduate-level “Security and Cryptography” course.

Breezecom (now Alvarion), Bucharest, Romania

September 2000 - June 2001

- Software Engineer.
- Part of the team that designed, implemented and tested the remote management software for the BreezeACCESS and BreezeNET wireless access products.

LANGUAGES

Romanian - native

English - advanced (reading, writing, speaking)

Italian - fair (reading, writing, speaking)