Tutorial: File System Internals
Presenter: Ahmed Amer (University of Pittsburgh)

The filesystem is probably the most prevalent and unobtrusive abstraction in computer systems but, going beyond the familiar interface that allows so many uses, we will delve into the internals of filesystem implementations. The interface to the filesystem can be used to interact with anything from persistent storage to running processes or physical devices, and for this tutorial we will be focused on the filesystem's role as a means to store and access data. For this tutorial we will cover the internals of a varied range of example systems, running the gamut from basic filesystems that do little more than provide a means to access named files, to more complex systems. Our goal will be to understand the tradeoffs and decisions behind different optimizations and architecures. We will cover typical filesystems such as FFS, ext3, NTFS, HFS+, and NTFS, but we will also discuss the design choices and decisions behind a number of distributed and cluster filesystems, concluding with a discussion of recent research in filesystems.

Tutorial: Cryptographic Methods for Protecting Storage Systems
Presenter: Christian Cachin (IBM Zurich Research Lab)

Storage systems have undergone a tremendous evolution over the last years. Today, storage space is typically provided by complex networked systems, in which clients communicate with storage servers over a network. In the near future, networked storage systems will extend beyond the server room, and their security will become a prime concern. Most data storage systems will soon rely on cryptographic protection methods as a key technology.

Protecting “data at rest” in storage systems poses new challenges compared to protecting “data in flight”, which has been the focus of communication security for some time and is well understood today. One notable difference between these two problems is that a communication channel typically uses a streaming interface with FIFO characteristic, whereas a storage system must provide random access to small portions of the stored data. New techniques are needed for providing security in this context, in particular for protecting the integrity of stored data efficiently and for key management.

Methods for cryptographic storage protection have been investigated for some time already, and some have been available in practice, like hard-disk and whole file-system encryption. Concerns about the involved overhead has so far prevented their pervasive use in distributed storage systems. But privacy regulations that have recently been introduced mandate encryption for certain environments; this explains why the industry is actively working on strong cryptographic protection methods for data storage systems.

OUTLINE

* Design options for security
  - Data in flight & data at rest
* Security at the Block Layer
  - Tweakable encryption modes
  - Integrity protection using tweakable encryption
* Security at the Object Layer
  - Capabilities in Object Store
* Security at the Filesystem Layer
  - Designs for key management
  - Encryption using lazy revocation and key updating
  - Integrity protection using hash trees
* Example systems

The focus will be on recently developed methods for encryption, integrity protection, and access control that use strong cryptography.

BIOGRAPHY

Christian Cachin graduated with a diploma in Computer Science from ETH Zurich (1993) and obtained his Ph.D. in Computer Science from ETH Zurich in 1997. From 1997 to 1998 he was postdoctoral researcher at the MIT Laboratory for Computer Science, with Prof. Ron Rivest, one of the inventors of public-key

cryptography. He has been a Research Staff Member at IBM Zurich Research Lab since 1998, where he was involved in a number of projects in security and distributed systems.

He has authored many publications in the areas of cryptology and distributed systems, holds several patents on secure protocols and cryptographic algorithms, and has been a frequent member of program committees of technical conferences. He is a Director of the International Association for Cryptologic Research (IACR). Together with Jan Camenisch he was program chair and organized Eurocrypt 2004. His current Research interests are cryptography, network security, fault tolerance and distributed systems.