From Reliable to Secure Distributed Programming

PRESENTER

Christian Cachin IBM Research -Zurich, Switzerland http://www.zurich.ibm.com/~cca/

ABSTRACT

Over the course of the last decade, the field of reliable distributed systems has been extended to include security against malicious actions by non-cooperating processes. This important topic is nowadays known as "Byzantine fault-tolerance."

The tutorial addresses fundamental programming abstractions in distributed environments, including the notions of broadcast, shared storage, and consensus. It is well-known how to implement them in systems subject to uncertainty and (benign) failures. The main part of the tutorial shows how to realize these concepts in environments subject to Byzantine faults, based on recent research results. The presentation will demonstrate how several algorithms for tolerating Byzantine faults arise naturally from the evolution of algorithms that tolerate benign faults.

In particular, it focuses on reliable broadcast, shared memory, and consensus.

STRUCTURE

1. Models and assumptions

2. Reliable broadcast -Definition in the crash-failure model -Issues with the definition in the Byzantine model -Byzantine consistent broadcast -Byzantine reliable broadcast

3. Shared memory -Model of registers with Byzantine failures -Byzantine masking quorum -Authenticated-Data byzantine quorum

4. Consensus -Common model for leader-driven consensus -Consensus with crash failures (Paxos-consensus, Lamport) -Byzantine consensus (PBFT-consensus, Castro-Liskov)

5. Conclusion

PREREQUISITES

The audience should be familiar with basic notions of protocols for building reliable distributed systems that are exposed to crash failures. No particular knowledge in security is required.

SUPPORTING MATERIAL

This tutorial is based on the recently published book "Introduction to Reliable and Secure Distributed Programming", by Cachin, Guerraoui, and Rodrigues. It represents the second edition of the successful book "Introduction to Reliable Distributed Programming" by Guerraoui and Rodrigues. Website with supporting material available at http://www.distributedprogramming.net/

ABOUT THE PRESENTER

Christian Cachin graduated with a Ph.D. in Computer Science from ETH Zurich in 1997. He was a postdoctoral researcher at the MIT Laboratory for Computer Science from 1997-1998. Since 1998 he has been a Research Staff Member at IBM Research -Zurich, involved with research projects in the fields of cryptology and distributed systems. In 2009 he was a visiting researcher at the Ecole Polytechnique Federale de Lausanne (EPFL).

Christian Cachin's research focuses on cryptology and distributed systems. He has authored many peer-reviewed publications in these fields, holds several patents on secure protocols, and has been a frequent member of program committees of technical conferences, of which he chaired several. He is an ACM Distinguished Scientist (2009) and received IBM Outstanding Technical Achievement Awards. He currently serves as an editor for several international journals in the area of information security and is an author of the book "Introduction to Reliable and Secure Distributed Programming." Since 1998 he has been a member of the board of directors of the International Association for Cryptologic Research (IACR), currently as Vice President, and lead the organization of the Eurocrypt 2004 conference.

His current research interests are the security of storage systems, secure protocols for distributed systems, and cryptography. He contributed to the OASIS Key Management Interoperability Protocol (KMIP) standard and is currently concerned with security in cloud computing.