Journal of Computer Security 4 (1996) 265
IOS Press

Editors' preface

Of the three papers in this issue, two address leading-edge topics in network security, and one provides a new insight into a classical model of the propagation of access rights.

"The Ω key management service", by Reiter et al., shows how public-key cryptography, key escrow, and fault-tolerance technologies can be integrated into a single flexible, safe, and reliable system that supports the needs of a large organization. It protects private keys, both its own certificate-signing key and escrowed keys, by dividing them among multiple servers. The system has been put to use already as a certification authority for Web servers within AT&T.

In "Securing ATM networks", Shaw-Cheng Chuang analyzes the problem of placing security mechanisms in the Asynchronous Transfer Mode (ATM) network environment to achieve both data confidentiality and data integrity. Based on the analysis, a key agile cryptographic device, called the *CryptoNode*, is proposed. The paper describes the implementation of the device and the lessons learned from this implementation effort.

In "Conspiracy and information flow in the Take-Grant Protection Model", Matt Bishop explores the information transfer aspects in the Take-Grant Protection Model, a simple model of propagation of access rights in which safety is decidable in linear time. This paper develops a notion of "conspirators" in the context of information flow and gives precise bounds on the number of conspirators required for information to be shared or stolen.

Sushil Jajodia and Jonathan Millen