Invited Talk

Identity-Based Encryption From Algorithm to Enterprise Deployment

Guido Appenzeller
Voltage Security
Palo Alto, CA, USA
guido@voltage.com

Abstract

Identity-Based encryption is an asymmetric encryption system where identifiers such as email addresses, server names or phone numbers, can be used as public keys. Originally proposed by Adi Shamir in 1984, the first practical algorithm became available in 2001. Since then IBE has not only generated huge interest in academia, it has seen wide-scale adoption in industry, is used by hundreds of thousands of users and is in the process of being standardized by the IEEE.

In this talk we will give an overview of the state of IBE, and reflect on what led to its rapid success. Unlike many encryption protocols, IBE is a new cryptographic paradigm that can not be built from existing encryption algorithms. As a new primitive, IBE directly solves some of the existing problems with classic public key systems. Specifically it enables the use of short-lived public keys, removes the overhead of certificate management and enables keys to be centrally managed. As a result IBE systems require less state and are much more lightweight and scalable than traditional PKI systems.

In this talk we will give an overview over the IBE algorithms and standardization activities. We will describe a secure email systems based on IBE, and by examining the example of a live enterprise deployment of IBE discuss advantages and differences to traditional PKI.

Categories & Subject Descriptors: E.3 Data Encryption

General Terms: Algorithms, Management, Security.

Bio

Guido Appenzeller co-founded what is now Voltage Security while attending Stanford University in 2002 and now serves as Chief Technology Officer, overseeing the expansion of Voltage IBE technology into new application areas such as mobility, data-at-rest, VoIP and other forms of digital communication. Guido has over a decade of computer science, security, networking and e-commerce experience, is the author of over 20 peer-reviewed technical publications and was named to the MIT TR100 list of top technology leaders for 2004.

Guido was previously an Associate at Kappa IT Ventures, a European Technology Investor, worked for McKinsey and Company in their German office. Guido received a Ph.D. and an M.S. in Computer Science from Stanford University and his undergraduate degree in Physics magna cum laude from the University of Karlsruhe, Germany.

CCS'05, November 7–10, 2005, Alexandria, Virginia, USA.
ACM 1-59593-226-7/05/0011.