TECHNOLOGY

Efficient Key Exchange for Symmetric Cryptosystems

OVERVIEW

Background
The efficient replacement of secret keys is a central problem of key management in symmetric cryptosystems. These systems are used to secure communications and electronic transactions between businesses, banks, and other entities where secure communications are required. In using such systems, messages between senders and receivers are encoded and decoded with identical digital keys. But each time an encrypted message is exchanged, part of a key is revealed. The keys must be replaced on occasion to minimize the risk of a key being compromised by an outside agent. However, generating new keys can use a significant amount of computing resources. Different strategies exist to manage the keys but involve explicit communication between sender and receiver, the presence and cooperation of trusted third parties, and large storage requirements.

Researchers at the University of Maryland, in cooperation with the Army Research Laboratory, have developed a method of efficiently updating and exchanging secret keys that exploits the randomness of Markov models in selecting a new key. This new method eliminates the need for third-party key management or public key infrastructure, explicit communication of keys between sender and receiver, and large amounts of storage space. The system has perfect forward secrecy and is resistant to known key attack methods and interception by third parties. A patent application is pending.

Advantages
• No explicit communication between sender and receiver means the keys are not exposed to potential interception during update
• No need for third-party key repositories means even greater system security
• Low system resource requirement to update keys leads to greater system efficiency

Applications
• Symmetric key cryptosystems
• Frequency hopped communications such as multicarrier authentication
• Other applications where one or more variables change pseudo-randomly

Stage of Development: The algorithm has been designed and perfect forward secrecy has been proven. Work is continuing.

Lead Inventors: Prof. John Baras, Dr. Paul Yu, Dr. Brian Sadler

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Patent(s) pending

LICENSE STATUS

Available for exclusive or non-exclusive license

CATEGORIES

- Information Technology

EXTERNAL RESOURCES

- US Patent 8,848,904

IS-2008-112