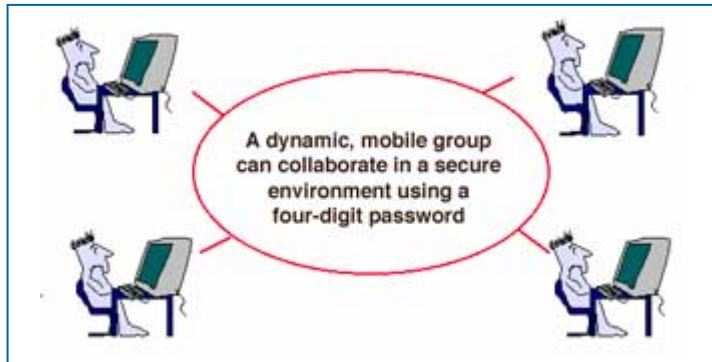


Cryptography for Secure Dynamic Group Communications

APPLICATIONS OF TECHNOLOGY:



Robust cryptography for virtual collaborative environments including:

- mobile user groups such as emergency rescue, military operations, and police teams
- mesh networking such as PAN and WLAN networks
- peer-to-peer and Grid computing

ADVANTAGES:

- Enables secure, efficient communication within a group without a centralized security infrastructure
- Able to manage a dynamic membership
- Needs a password of only four digits in length
- Could be made to work with a variety of wireless products
- Provably secure against dictionary attacks

ABSTRACT:

Olivier Chevassut from Berkeley Laboratory, David Pointcheval, and Emmanuel Bresson have invented a method that enables secure, group-oriented communication without a centralized security infrastructure. The technology is easily deployable, flexible, provably secure against dictionary attacks, and can be developed for use in wireless communication devices like Wi-Fi products.

Unlike Public-Key Infrastructure (PKI)-based technology, the Berkeley Lab cryptography provides for the deployment of secure collaborative groups anywhere and at any time. The Berkeley Lab technology allows group members to meet once and then immediately start exchanging

cryptographically protected messages without having to rely on fixed and centralized servers. Group members can join and leave the group at will.

The main advantage of the Berkeley Lab method is that it does not require users to carry hardware devices embedding their long-symmetric keys or to import these cryptographic keys into potentially insecure computers. The method was designed to be used with short passwords that are easily memorized.

Using the Berkeley Lab cryptographic system, a virtual group is created when the peer collaborators establish a secure communication session among themselves by computing a master key via a group key-exchange bootstrapped from a four digit password. The master key is then used as a means to encrypt sensitive messages between collaborators.

STATUS: Patent pending; available for licensing or collaborative research

FOR MORE INFORMATION SEE: [Bresson, E., Chevassut, O., Pointcheval, D., "Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks," *Advances in Cryptography – Proceedings of ASIACRYPT 2002*, 497-514.](#)

REFERENCE NUMBER: IB-1973

CONTACT:

Pam Seidenman
Technology Transfer Department
E.O. Lawrence Berkeley National Laboratory
MS 90-1070
Berkeley, CA 94720
(510) 486-6467
FAX: (510) 486-6457
TTD@lbl.gov