Foundations of Computer Security

Lecture 66: PGP

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Pretty Good Privacy

Various crypto algorithms and products provide strong encryption, but are not particularly easy to use.

Phil Zimmermann had the goal of providing strong encryption to everyone, in the form of an email encryption system that is:

- extremely strong, using state of the art cryptographic algorithms;
- easy to use and accessible to all.

PGP is "the closest you're likely to get to military-grade encryption." –Bruce Schneier, *Applied Cryptography*

Zimmermann's Motivation

Zimmermann had a strong distrust of the government, and believed strongly that everyone had an absolute right to privacy.

The government generally believes that the right to privacy is limited by the need of the government to read messages under certain circumstances. Historically, the government restricted access to strong encryption.

PGP is a "end-run" around government restrictions, and almost landed Zimmermann in jail.

Did Zimmermann Succeed?

From Wikipedia page on PGP:

> *In 2003, an incident involving seized Psion PDAs belonging to members of the Red Brigade indicated that neither the Italian police nor the FBI were able to decode PGP-encrypted files stored on them.*
>
> *A more recent incident in December 2006 (see United States v. Boucher) involving US customs agents and a seized laptop PC which allegedly contained child pornography indicates that US Government agencies find it "nearly impossible" to access PGP-encrypted files.*

PGP

Zimmermann developed PGP (Pretty Good Privacy) in the late 1980's and early 1990's. Some characteristics include:

1. Uses the best available cryptographic algorithms as building blocks.
2. Integrates these into a general-purpose algorithm that is processor-independent and easy to use.
3. Package and documentation, including source code, are freely available on-line.
4. PGP is now provided by Viacrypt in a compatible, low-cost commercial version.

Why would anyone buy this software from Viacrypt when it's available free?

Growth of PGP

PGP has grown explosively and is widely used.

1. Available free worldwide for Windows, UNIX, Macintosh, and others. The commercial version satisfies businesses needing vendor support.
2. Based on algorithms with extensive public review.

   Key Exchange: Diffie-Hellman.
   Public key encryption: RSA, DSS.
   Symmetric encryption: CAST-128, IDEA, and 3DES.
   Hash coding: SHA-1.
3. Wide applicability: standardized scheme for encryption, supports secure communication over Internet and other networks.
4. Not developed by or controlled by any government.
5. Now on track to become an Internet standard (RFC 3156).

Lessons

- PGP illustrates that strong encryption can be packaged conveniently and accessible to everyone.
- PGP is very widely used and extremely secure.

Next lecture: PGP Services