Worldwide Developers Conference

Cryptography on Mac OS

Vinnie Moscaritolo

The Crypto Guy
Apple Computer, Inc.

Cryptography on Mac OS

Dave Del Torto

Pretty Good Privacy, Inc.

Overview

- PGP Background 1991–1997
  - From DOS Kitchen to “Das Desktop”
  - Public Key Crypto—How PGP works
- Securing the Mac OS
- PGP 5.0
- PGPfone
- PGPdisk
- PGPcdk
- Q&A

Background

- PGP 1.0—Phil’s Pretty Good Software
  - Kitchen table engineering
- PGP Genie Gets Out of the Bottle
  - PGP is mysteriously exported from US
- Cypherpunks
  - Crypto-activism: EFF, CPSR

Background *(cont.)*

- A whole bunch of interesting stuff happens
  - Zimmermann Legal Defense Fund, etc.
- 1992–1994—PGP 2.0
  - 1992 MacPGP appears (ugly DOS port)
  - 1995 FatMacPGP (native ugly DOS port)
- 1994–1995 PGP 3.0 Volunteer Dev Team

Background *(cont.)*

- Jan 1996—US Customs has no evidence
- Mar 1996—PGP, Incorporated
  - Founded by Phil Zimmermann + Investors
  - Purpose:
    - To restore privacy in the Information Age
  - Mission
    - To become the most trusted provider of open, transparent software products that are used everywhere by individuals and businesses to restore and maintain privacy

Background *(cont.)*

- July ’96 PGP acquires Viacrypt
  - Previous commercial PGP provider
- Oct ’96 PGP acquires Privnet
- Dec ’96 PGP 3.0 pre-alpha source published
  - PGP, Inc. publishes all crypto source
- Jan ’97 PGPmail 4.5 ships
  - 2.6.2 codebase

Securing Mac OS

Will Price

Architect/Sr. Mgr. Mail
and Fone Products

PGP, Inc.

Plugging Holes

- Virtual Memory
  - LockMemory(), UnlockMemory()
- Temporary Files—Persistent Data Storage
  - Can be recovered after being written over up to 9 times or more
  - Write to disk encrypted (or use PGPdisk!)
- Wipe up after yourself
  - Memory buffers

More Holes

- Memory Burn-in (Ion migration)
  - Yes, I’m serious
  - DRAM retains charge traces
- Passphrases in TextEdit fields
  - PowerPlant undo blocks bleed all over the place
  - Bullets reveal length info (••••••)
- File tampering
  - PGP release digitally signed executables
- Disk block shrinkage

Beware of Snake Oil

- Designing secure software is very hard
- Mose security products can be easily defeated by unfunded attackers
- PGP designs its software to protect against attackers with unlimited resources
- PGP source code is subjected to rigorous internal and external review

PGP 5.0 for Personal Privacy

- Public Beta starts Today
- No more goofy DOS port
- Rewritten from the ground up
- Primary goal: Ease of Use
  - Mac and Win32
- Backward compatible

PGP 5.0 Modules

- PGPkeys key management application
- PGPtools dropper toolbar
- PGPmenu
- E-mail Plug-ins
  - Eudora Pro/Lite
  - Claris Emailer 2.0
- Common API in CFM Shared Library

PGP 5.0 Features

- Diffie-Hellman/DSS Keys
  - Algorithm neutral
  - SHA-1 one way hashing algorithm
  - At least as secure, faster
- PGP/MIME
  - Attachments automatically encrypted
  - Automatic lookup and synchronization with keys on HTTP keyservers built-in

Demo

PGPfone 2.0

- Secure Internet/Modem telephone
- Full duplex
- Bidirectional secure file transfer in call
- Diffie-Hellman public key algorithm
  - Negotiates shared secret key unknown to man in the middle
  - Party independent, no password required
- CAST-128, TripleDES, Blowfish
- Cross-platform Mac OS/Win32
- 2.0 for Mac OS available now

Disk and CDK Products

Lloyd Chambers

Architect/Sr. Mgr. Disk and CDK Products

PGP, Inc.

PGPdisk 1.0

- Rewrite of Will Price's "CryptDisk"
- Secure volumes via "disk image"
- 128 bit encryption
  - 7 times the age of the universe to break
- Works on any local volume
- No extensions, no hardware accesses
- Works on Blue Box!

PGPdisk 1.0 Security

- 128 bit CAST in dual-CFB mode
- Protection against memory burn-in
- Protection against VM paging
- Passphrase erasure
- Each volume uses random key
- Auto-unmount of volumes

PGPdisk 1.0 Performance

- Hand-coded PowerPC and 68K assembly
- Completely asynchronous driver
- I/O fully overlaps with encryption
- Ascending sort of I/O requests
- Excellent system responsiveness
  - Minimal work done at interrupt time
- Really fast!

PGPdisk 1.0 Other Uses

- Sharing PGPdisk volumes in workgroups
- Multiple users, each with their private volume
- Multiple users, each sharing one volume with multiple passphrases, some can be read-only

PGPdisk 1.0 Misc…

- Distribute information securely, conveniently
- Secure backups
- Convenient way to create partitions

PGPdisk 1.0 Comparisons

- Volume approach inherently faster and more secure than file by file approach
- Completely transparent once mounted
- Considerably more convenient for securing lots of data
- No encrypt/decrypt security hole, no temp files needed

Demo

PGPcdk 1.0

- Cross-platform API for Mac, Win32, UNIX, others
- Encryption, Digital Signatures, Key Management, GUI services
- Easy to use, well documented, good sample code/demo app
- Binary and Source code kits
- CFM 68K and PPC

PGPcdk Encryption/Signing

- Public/Private Key
- Forward looking API
- Symmetric ciphers (CAST, TripleDES, IDEA)
- Strong crypto only
- Support for a wide variety of options

PGPcdk Key Management

- Forward looking for performance, key server support
- API largely stable, implementation will improve over time

PGPcdk UI Services

- Standard Get Passphrase Dialog
- Standard Get Recipients Dialog
- More

PGPcdk Availability

- Q3, maybe sooner
- Contact PGP for seeding
- Licensing TBD

Contact

- E-mail
  - Dave Del Torto <ddt@pgp.com>
  - Will Price <wprice@pgp.com>
  - Lloyd Chambers <lloyd@pgp.com>
  - Vinnie Moscaritolo <vinnie@apple.com>
- Web
  - http://www.pgp.com/
  - http://www.vmeng.com/mc

Q&A

Worldwide Developers Conference