OpenSSH & GnuPG:
Secure Communications with Open Tools

David Tomaschik
Atlanta Linux Fest
September 20, 2008

OpenSSH

Atlanta Linux Fest

- Encrypted 'Remote Terminal'
- Authentication via: PAM, Public Key
- 'Tunneling' other data
  - Route around firewalls
  - Encrypt cleartext data streams
  - Any TCP connection can generally be tunneled
- Packages: openssh (-server, -client)
- Useful: seahorse

OpenSSH

Atlanta Linux Fest

- Demo
  - Basic SSH Connection
  - Remote command invocation
  - Public Key Generation
  - Basic Tunnel
  - SOCKS-Style Tunnel
  - Specifying options in .ssh/config
  - Key Management with Seahorse

GnuPG

- Public Key Cryptography
  - Encryption
  - Signing
- Signing
  - E-Mail
  - Software Sources
  - Debian Packages, RPMs, etc.
- Package: gnupg or gpg
- Optional: seahorse or kgpg; enigmail

GnuPG

Atlanta Linux Fest

- Demo
  - CLI Key Generation
  - Seahorse Key Management
  - Enigmail Setup
  - CLI Signing
  - Verification
  - FireGPG

Advanced SSH

Atlanta Linux Fest

- ControlMaster Sockets
  - Multiple terminals, one connection
  - Only authenticate once
  - Fast: rsync, etc.
- SSH piping
  - Tar to move directories across network
- keychain/ssh-agent
- X11 Forwarding

Questions

Atlanta Linux Fest