Keys to the Kingdom: Mac OS X Security Secrets Revealed

Session P234

Macworld Conference and Expo Boston 2005

Arek Dreyer
arek@arekdreyer.com
Dreyer Network Consultants, Inc.
Apple Certified Trainer, ACSA 10.3

What We'll Cover

- Kerberos
- SSL Certificates, self-signed and purchased
- SSH keys and tunnels

Why You Need To Know This

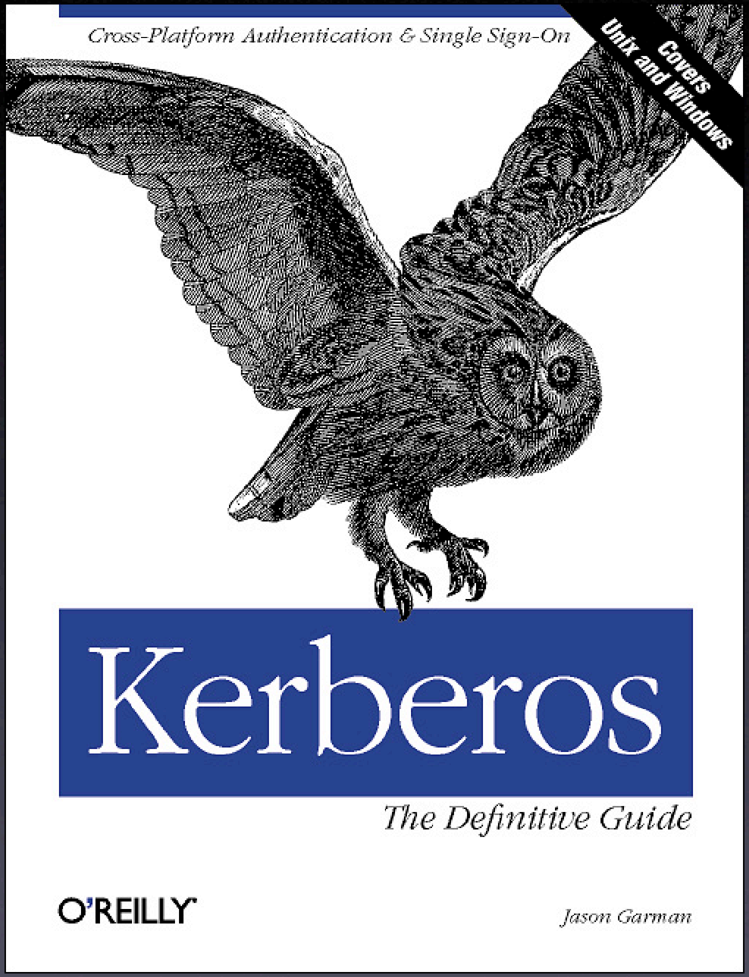
- Open Directory's Kerberos implementation is so easy it makes me weep with joy
- We often encrypt authentication, but leave the payload (data) traffic cleartext to steal
- SSH & SSL are two ways to encrypt traffic
- Tiger Server's new Certificate Manager makes requesting SSL certs quite easy.

Where this is useful

- Kerberos for enabling single sign-on
- SSL for securing network services on Mac OS X Server, such as
    - LDAP, VPN, Mail, Web, iChat Services
- SSH for securing network traffic between two hosts, when you have an account on both hosts

Kerberos for authentication

Read the first chapter of the O'Reilly Kerberos Book by Jason Garman.



Kerberos Players

- Kerberos Key Distribution Center (KDC)
- Kerberos Client (user)
- Kerberized Service (mail server)

Kerberos and Open Directory Master

- If your DNS is cool, when you make your server an ODM, Kerberos is set up
- Clients who use Directory Access to bind to your ODM get configured upon boot to participate in the Kerberos Realm
- Easy to Kerberize your Mac OS X services

Kerberos is not a silver bullet

- Kerberos ONLY takes care of authentication, is does not encrypt payload.
- Kerberos relies on the client being part of the Kerberos realm; /Library/Preferences/edu.mit.kerberos
- Kerberos requires pre-shared secrets
- Not all services are kerberized

What We'll Cover

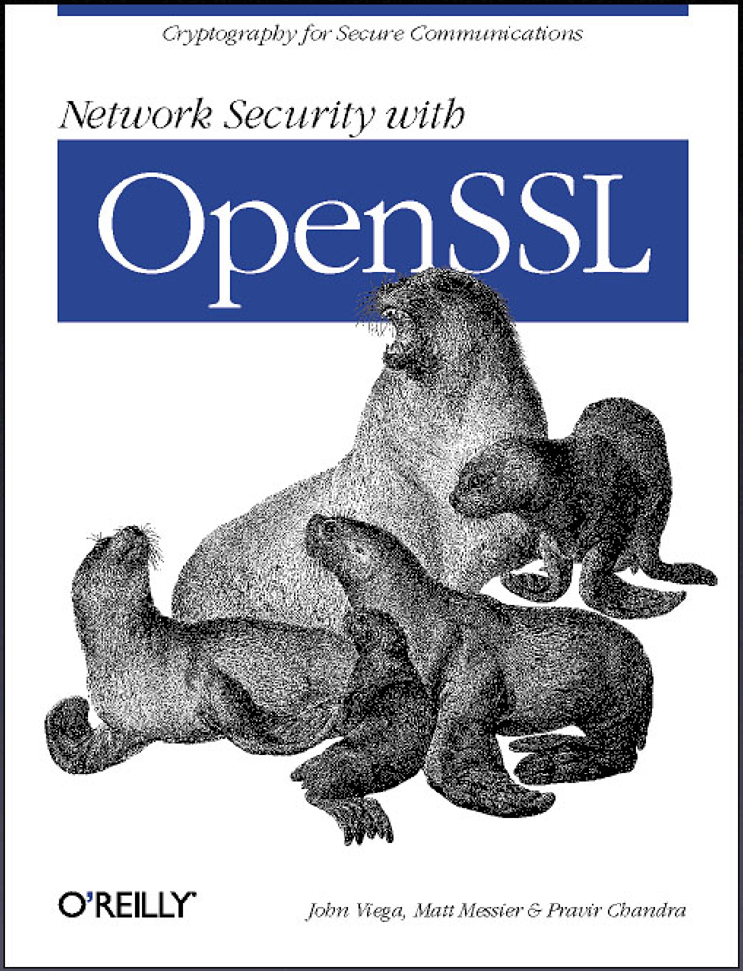
- Kerberos
- SSL Certificates, self-signed and purchased
- SSH keys and tunnels

SSL and Certificates

- Quick introduction to SSL
- Server Admin Certificate Manager
- Becoming your own Certificate Authority

OpenSSL

If you will be relying on SSL, please read the first few chapters of the O'Reilly book on OpenSSL to be aware of its strengths and weaknesses


Cryptography for Secure Communications

Network Security with

OpenSSL

O'REILLY

John Viega, Matt Messier & Pravir Chandra

Intro to SSL

- Allows client and service to encrypt data
- People are familiar with SSL over the web, https, port 443
- If service can use SSL, let’s use our SSL certificate
- Some services don’t know how to use SSL, as is the case with Kerberos

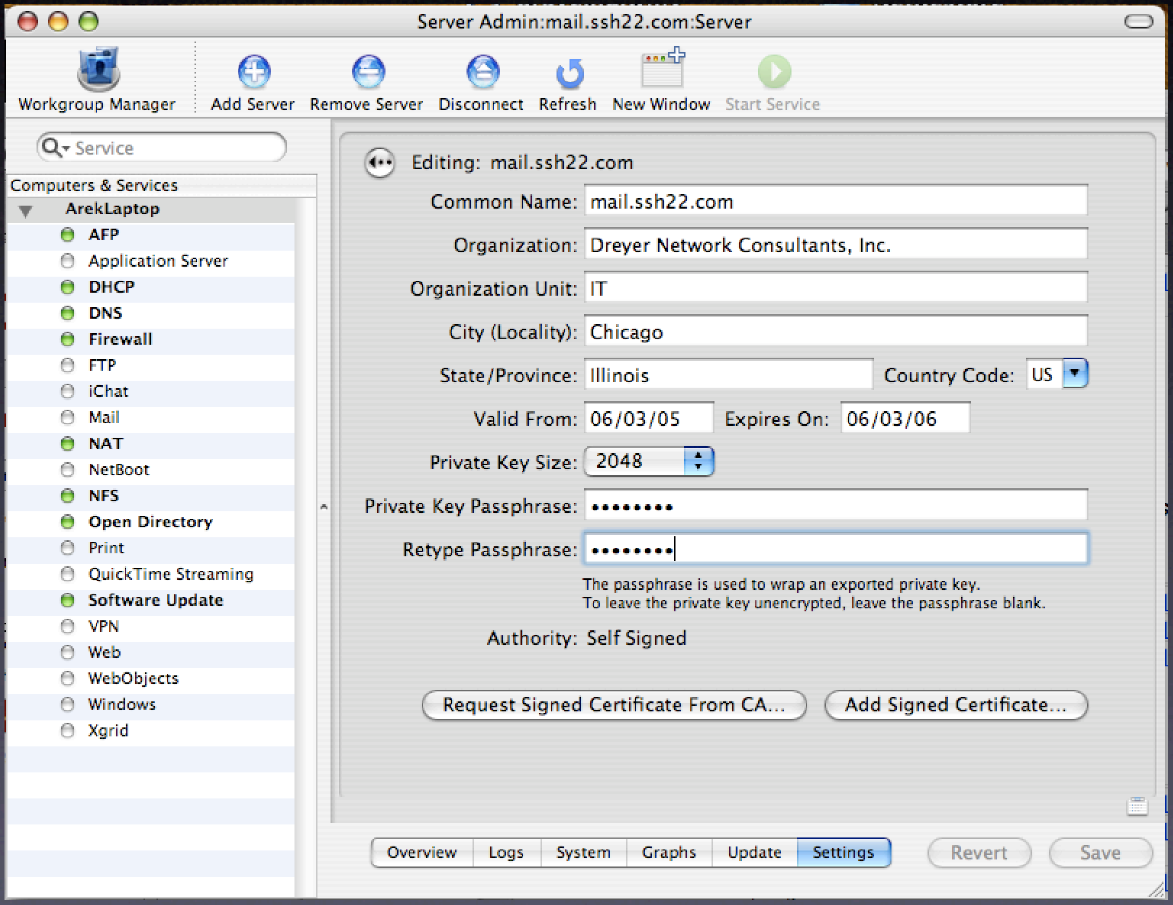
Intro to SSL: Certification Authority

- Client asks a service for its certificate
- Service’s certificate claims to be legit
- How does client trust the certificate without a pre-existing shared secret?
- Client is pre-configured to trust a set of Certification Authorities (CAs), which can sign SSL certificates

Obtaining an SSL Cert

- Generate a certificate signing request, tied to FQDN like mail.ssh22.com
- Ask a Certification Authority to sign it, and give them money
- Import the signed certificate

Server Admin Certificate Manager



Editing: mail.ssh22.com

Common Name:	mail.ssh22.com
Organization:	Dreyer Network Consultants, Inc.
Organization Unit:	IT
City (Locality):	Chicago
State/Province:	Illinois
Country Code:	US
Valid From:	06/03/05
Expires On:	06/03/06
Private Key Size:	2048
Private Key Passphrase:	••••••••
Retype Passphrase:	••••••••

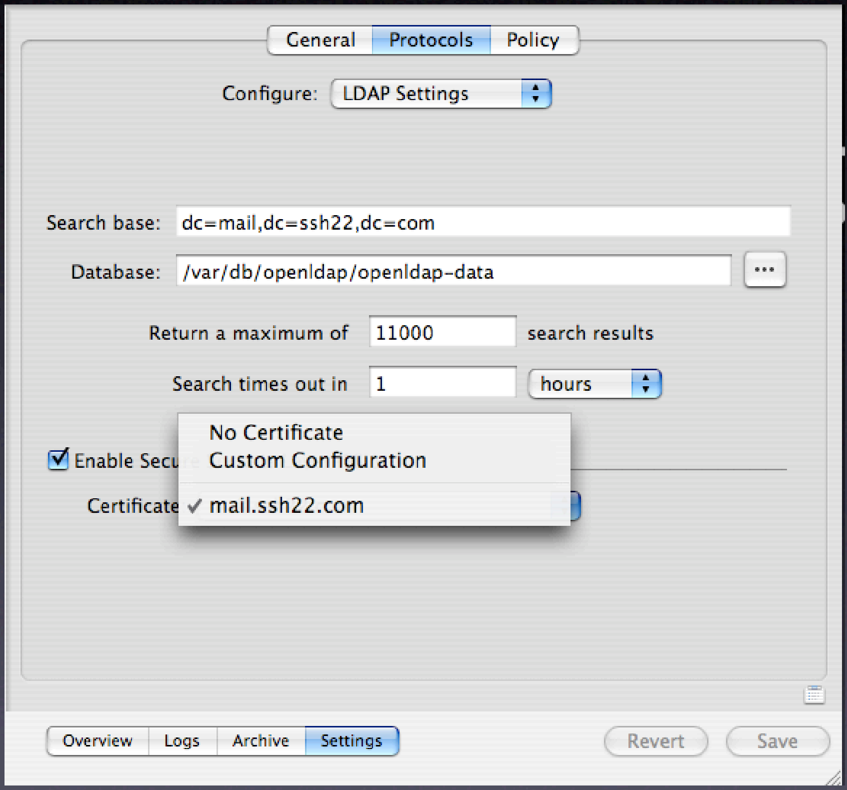
The passphrase is used to wrap an exported private key.
To leave the private key unencrypted, leave the passphrase blank.

Authority: Self Signed

Server Admin Certificate Manager

- Places files in /etc/certificates
- Certificates appear for services in SA
  - iChat, Mail, Open Directory, VPN, Web

Server Admin
Certificate Manager



Configure: LDAP Settings

Search base: dc=mail,dc=ssh22,dc=com

Database: /var/db/openldap/openldap-data

Return a maximum of 11000 search results

Search times out in 1 hours

☑ Enable Secu

Certificate ✓ mail.ssh22.com

Some SSL CAs

- www.verisign.com
- www.thawte.com
- www.qualityssl.com
- www.godaddy.com

Become your own CA

- Execute as root user in command line
- I ran into problems with the openssl command when /sw/bin was first in PATH
- Generate keys, csrs, and sign them
- Distribute your CA file to your computers
  - Everyone else will get untrusted warning

Become your own CA

- See afp548.com article on exact steps
- Create secret key file - ca.key
- Sign the key to create ca.crt
- Create server private key - server.key
- Create server signing request - server.csr
- Sign server.csr, resulting in server.crt

Become your own CA

- Distribute the ca.crt file to all clients
- `certtool  i` at the command line
- Or use Keychain Access.app

Demo SSL Certs

- GoDaddy is pretty inexpensive
- Verisign
  - Also requires you import their demo CA
- QualitySSL
  - As of 10.4.1, Server Admin generated CSRs don’t work, but CLI is fine

What We'll Cover

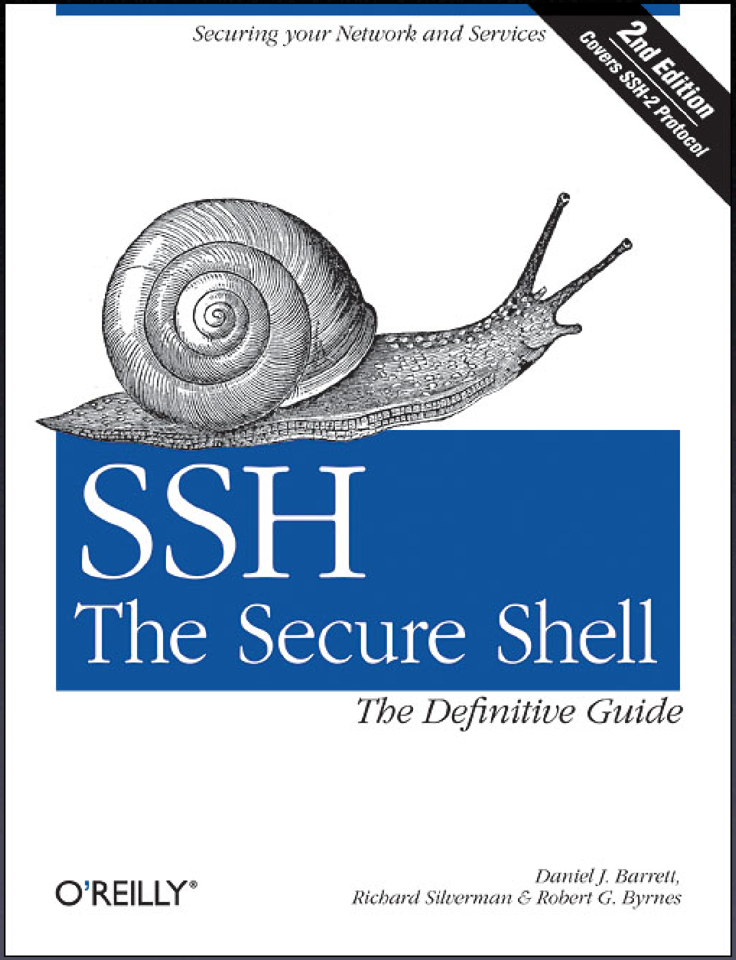
- Kerberos
- SSL Certificates, self-signed and purchased
- SSH keys and tunnels

Secure Shell - SSH

- SSH Keys
- SSH tunnelling

SSH

See the O'Reilly book on SSH.



Securing your Network and Services

2nd Edition
Covers SSH-2 Protocol

SSH
The Secure Shell

The Definitive Guide

O'REILLY®

Daniel J. Barrett,
Richard Silverman & Robert G. Byrnes

SSH keys

- You can use ssh without providing passwords
- Useful for scripting
- If anyone captures your keys, GAME OVER

SSH keys

- `ssh-keygen -t dsa`
- Distribute that key in a secure manner

-
  ```
  mv id_dsa.pub \
  ~/.ssh/authorized_keys
  ```
- ssh to a remote host - password free

SSH Tunnels

- Set up one tunnel per port
- Need ssh access on remote host
- Network sniffers will see only encrypted traffic

SSH Tunnel example

-
  ```
  ssh -L 8080:127.0.0.1:80 -f \
  -N arek@mail.ssh22.com
  ```
- -L port:host:port
  - localport, localIP, remoteport
- -f background, -N no remote command
- remote user and host

What We’ll Cover

- Kerberos
- SSL Certificates, self-signed and purchased
- SSH keys and tunnels

Synopsis

- Authentication is often encrypted, but data is often cleartext
- SSL allows client and service to communicate securely without preshared secrets, with help of trusted 3rd party (CA)
- SSH allows tunnels for secure encrypted traffic, but requires an account on both hosts

Thank You!

Mac OS X Security Secrets Revealed

Session P234

Macworld Conference and Expo Boston 2005

Arek Dreyer

arek@arekdreyer.com

Dreyer Network Consultants, Inc.

Apple Certified Trainer, ACSA 10.3