

Application Security for HotSpots

Cliff Skolnick, Iron Systems, INC. &
BAWUG

Topics

- What is Application Layer Security?
- Encrypting Your E-Mail
- Using SSH as a helper

Application Layer Security

- Each application is configured to communicate securely
- Data is opaque to the network
- Not as good as network layer security
- More versatile and compatible

Application Layer Security (Cont.)

- Applications Supported
 - Any browser that supports https protocol
 - Most modern mail clients
 - Some “ssl” enhanced applications (stelnet, sftp, etc.)
 - SSH

Application Layer Security (Cont.)

- Security is good if you use care
 - Bad “localhost” in DNS
 - Hostile DNS
 - Leaking DNS names
- Man in the middle vulnerability

Encrypting E-Mail

- Built-in encrypted transport in modern email clients
- Do not confuse with encrypted messages
- Server Side
 - SMTPAUTH
 - STARTTLS

Encrypting E-Mail (Cont.)

- Client Side
 - E-Mail from client to server is encrypted
 - E-Mail between servers is NOT secure
 - Netscape Demo
 - Outlook Express Demo

Encrypting E-Mail (Cont.)

- Server Side
 - Get a certificate
 - Search the web for “sasl tls <insert_mail_server_here>”
 - Prepare for a bunch of work
 - Creating a SSL certificate
 - Install and configure stunnel or enable native ssl support

SSH as a Helper Application

- SSH is a remote login program
- A live account on the remote system will be needed
- Any TCP ports can be redirected
- Modern SSH can act as a SOCKS proxy

SSH as a Helper App. (Cont.)

SSH as a Helper App. (Cont.)

- Platforms
 - Most Unix systems
 - Windows Platform
 - Java