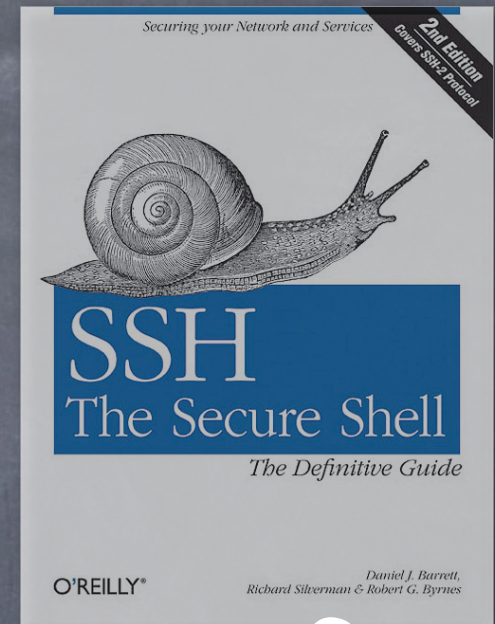


SSH (with a brief history of COMSEC)

Brad Ackerman
brad@facefault.org
CALUG



In the Beginning

- In the beginning, there was rsh
- Nobody was looking... were they?

1988: Points of Departure

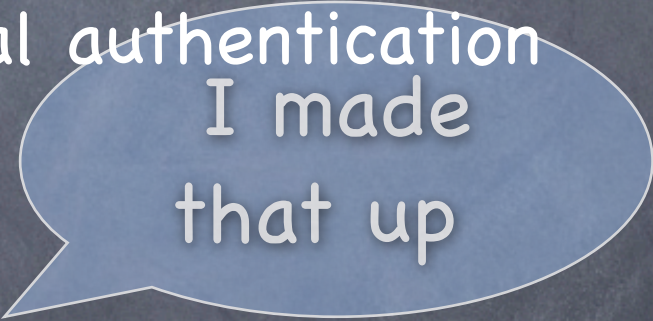
- Kerberos
 - Security over an untrusted network
 - Authentication and encryption — all is well...
 - but complex



1995:

Midnight on the Firing Line

- Secure Shell (SSH)
- Encryption and mutual authentication
- Tunnels anything
- Makes Julienne fries
- Current protocol: SSHv2 (1996)



I made
that up

All Alone in the Night

- Basic usage – drop-in replacement for rsh; username and password authentication
- You can authenticate with your password, but is that really secure?
 - Rumpelstilzkin attack
 - Timing attack on follow-on authentication



Shadow Dancing

- Public keys for authentication
- Software-stored or Common Access Card
- Your voice is your passport

(pending suitable PAM module)

Falling Toward Apotheosis

- Integrates with your organization's PKI, but that's beyond the scope of this presentation.
- To generate key: `ssh-keygen -t dsa`
- Copy public component to `~/.ssh/authorized-keys` on destination machines

Signs and Portents

- Now you authenticate... no password required
- Set up an agent!
- `ssh-agent`; `ssh-add` your keypair
- `ssh -A` will allow credential passing

Moments of Transition

- For the win, disable password authentication to kill Rumpelstiltzkin
- Here there be live demo.

And the Sky Full of Stars

- `ssh -X` — forwards X11 sessions
- `ssh -L 590x:remhost:590x`
 - forwards VNC localhost:x to remhost:x