The Internet Firewall Toolkit

Experiences and Lessons Learned

Frederick M. Avolio avolio@tis.com
Marcus J. Ranum mjr@tis.com

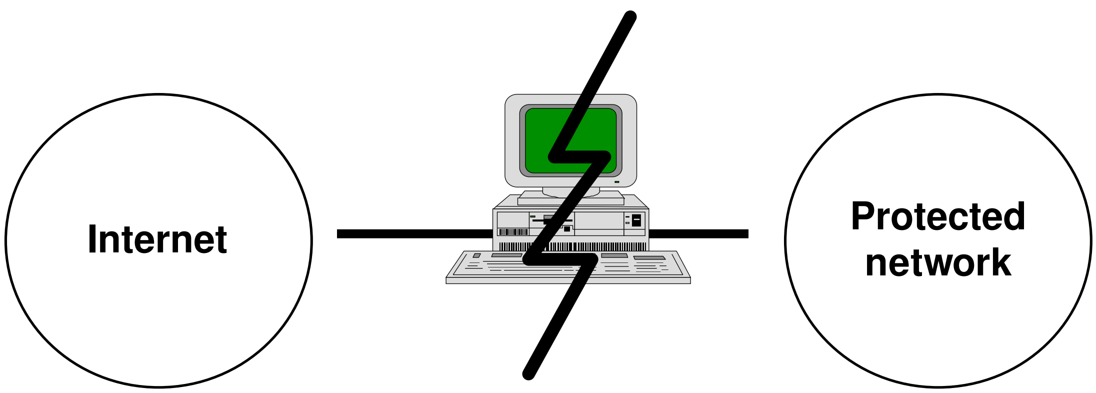
Trusted Information Systems, Inc.

Goals

- Extensible tools
- Policy free
- Freely available
- Minimalist implementation
- Comprehensible security paradigm
- Highly portable

Security Design

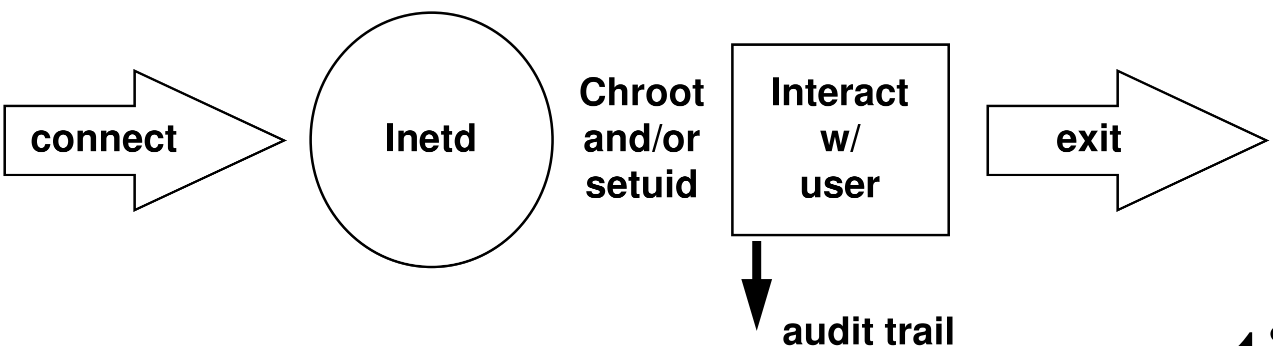
- Clear security dependencies / assumptions
- Intended for “proxy” model of firewalls



All Traffic Must Pass Through Applications On Bastion Host

Security Design (cont)

- Software invoked by inetd
- Proxies are minimalist protocol forwarders
- Proxies don’t start subprocesses
- Proxies may run under chroot
- Proxies don’t permit access to bastion host
- Proxies may require authentication



Toolkit Components

- TELNET proxy (*tn-gw*)
- Rlogin proxy (*rlogin-gw*)
- FTP proxy (*ftp-gw*)
  - Can selectively block or log operations
- “TCP wrapper” (*netacl*)
- SMTP wrapper (*smap/smapd*)
  - Collects and queues SMTP mail
  - Can scan for “dangerous addresses”
- Authentication server (*authsrv*)
  - Supports different forms of authentication system
  - Used by interactive proxies

Installed Base

- Over 1,500 sites have FTP'd source
- 300 active members in mailing list
- Many sites using toolkit or components
  - Not everyone who is using it has told us
- Commercial, government and private users

Outstanding Issues

- Data-driven attacks
- New protocols and protocols w/o user authentication
- Desire to "do everything" securely
- System specific holes
- Support
  - Inexperienced systems/network admins may install it incorrectly
- User resentment

Practical Experience

- Base software robust and portable
- Exposure of source code improves quality
- Clearly articulated security design beneficial
- “Policy free” approach means software has been deployed quite creatively by end users

tis

Future Work

- Add new proxies
- Formal security assessment of toolkit design and implementation
- Resist temptation of “creeping features”
- Bug and portability fixes

Availability

- **Sources and documentation:**
  ftp.tis.com: pub/firewalls/toolkit
- **Overview documentation via WWW:**
  http://www.tis.com
- **Users' mailing list:**
  ftwk-users-request@tis.com