A Network Security FAQ

(Frequently Agonizing Quandries)

1

What is this talk about?

- YOU ARE NOT ALONE
  - Many network admins seem to feel they are the only people with these problems
  - Recognizing general problem trends helps focus on issues
- Most network security problems *(IMHO)* have very little to do with network security
  - Policy problems
  - Conflicting goals
- Why?

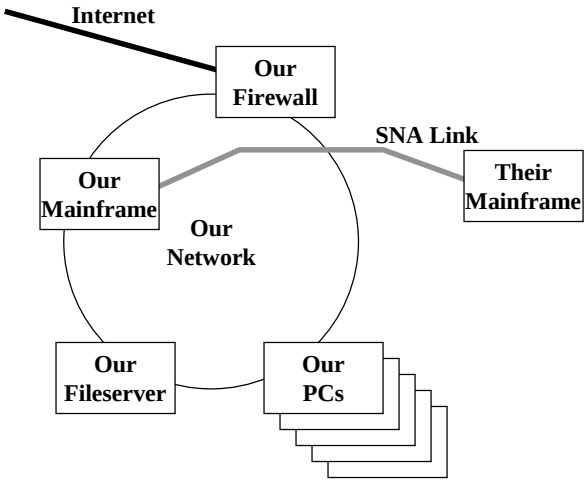
2

Who's on First

- Many sites have no idea what their network looks like
  - The octopus effect
  - How many competitors are actually on the same LAN?
- Many network admins have no idea who/what is on their network
  - The midnight vampire-clamper strikes again!

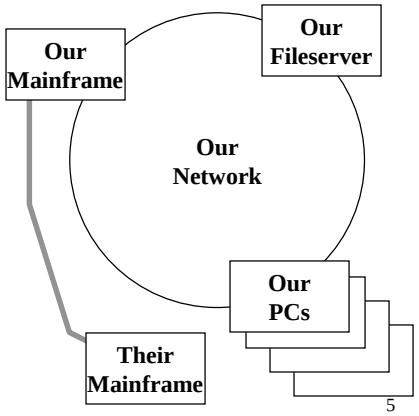
3

A Network Map



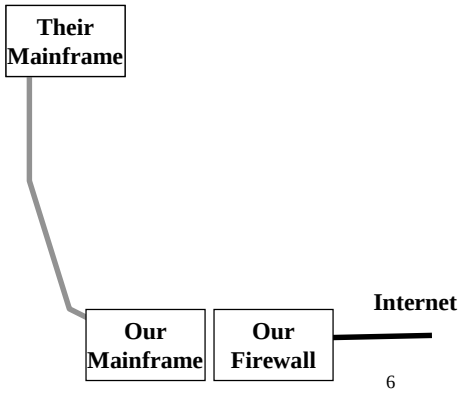
4

A Network Map



5

A Network Map



6

A Network Map

- Presumably organizational policy should address who needs to OK interconnections
- In practice it usually “just happens”
- Network admins who ask these questions are *not popular*

7

Mission Critical Services

- Sometimes a mission critical service requires throwing security away
- How can this *be?!?!?!*
  - If it’s mission critical, shouldn’t it be secure?
- Damage control is best defense
  - I.e., *you* the sysadmin must cover thy assets
  - Disaster or incident response preparations may let you keep your job
  - But you’ll still be unpopular, especially if you say “*I told you so.”*

8

Lack of Policy

- Networks exist to get work done
- Therefore most networks are run from the perspective of "*get the job done*"
- Security is therefore an impediment
- Either no security policy exists or it's based on how the mainframe does things which has nothing to do with a modern WAN

9

Lack of Management

- Where does the buck stop?

10

Conflicting Policy Goals

- Organizations that have multiple, distributed customers almost always have weak security on network
- Organizations that have independent departmental budgets almost always have weak security on network
- "Make the customer happy"
  - Well - the customer wants *both* to be secure and to have nothing get in his way
  - Which comes first?

11

Remote Management

- As LANs/WANs get more complex management no longer manual
- Management tools seldom incorporate security
- I'd like to SNMP manage the router on the *outside* of my firewall
- How do you securely remote manage security critical assets over an untrusted network?
  - Hint: there is a business opportunity here

12

Consistency

- Different owners of problems produces inconsistent answers
- Network/UNIX admin “owns” the IP network
- Telecom “owns” the modem pool

Do they have consistent and compatible ideas of the security policy/goals?

13

Privacy / Legality

- Consult your lawyer (eeeew! yuck!)
- Impact of computing is so new that it is a legal land mine
- Produces violently varying answers ranging from
  - Government-esque 3-page long “ACCEPTABLE USE” banners on the FTP daemon prompt (for crying out loud!)
  - Simple acceptable use policies
  - No policies whatsoever

14

Where can you go for help?

- Follow chain of command?
- Ask a lawyer? (eeeew! yuck!)
- Make it up as you go along?
- Ask USENET?

15

Conclusion

- The nasty problems in network security are at the meta-level
- Deciding the goals and policy goals is the hard part
- Get management buy-in
- Educate management
- The rest is a simple implementation detail

16