Security Futures

NETWORK-1
Software and Technology, Inc.

Bill Hancock, Ph.D., CISSP
Network-1 Software & Technology, Inc.
DFW Research Center
878 Greenview Dr.
Grand Prairie, TX 75050
(972) 606-8200
(972) 606-8220 fax
Internet: hancock@network-1.com
Web Server: http://www.network-1.com

What is being protected?

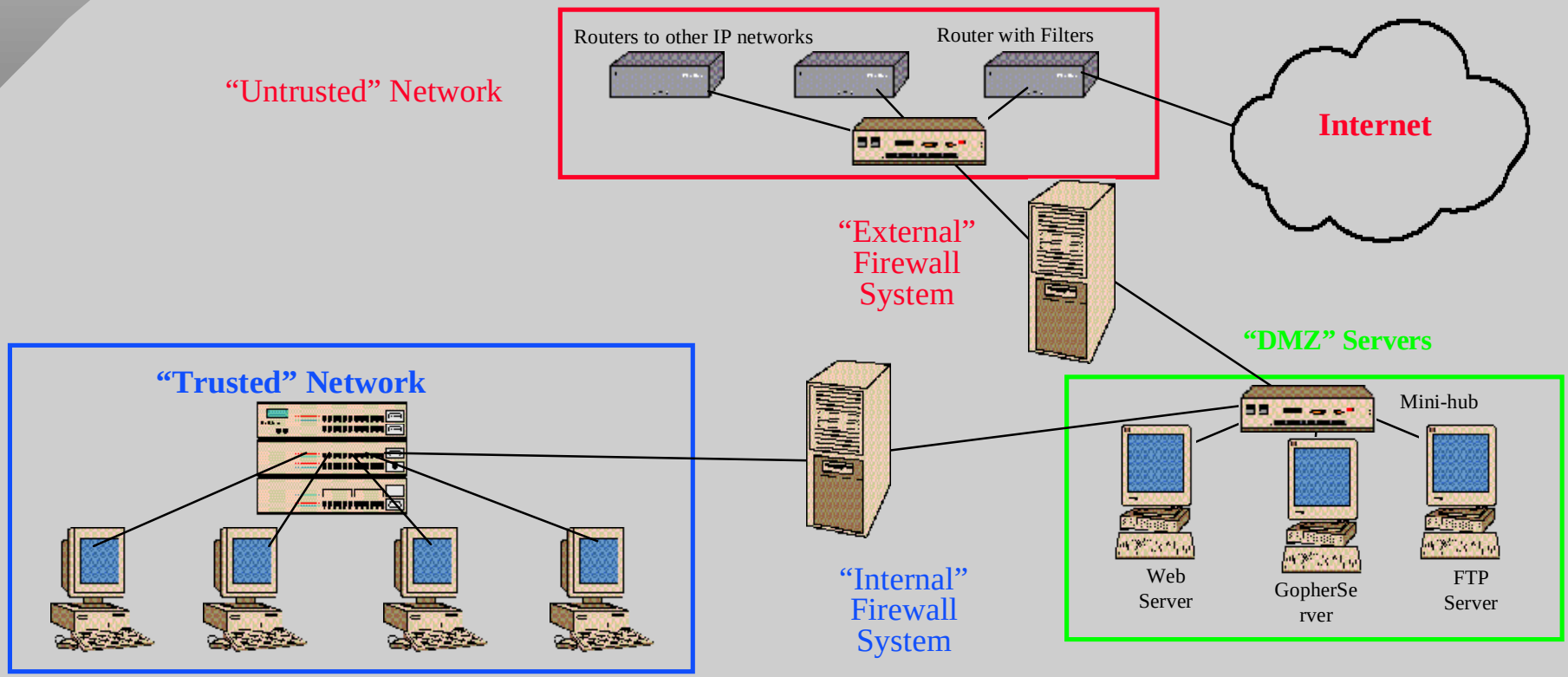
- *Your data*
  - *Secrecy - what others should not know*
  - *Integrity - what others should not change*
  - *Availability - your ability to use your own systems*
- *Your resources*
  - *Your systems and their computational capabilities*
- *Your reputation*
  - *Confidence is shaken in your organization*
  - *Your site can be used as a launching point for crime*
  - *You may be used as a distribution site for unwanted data*
  - *You may be used by impostors to cause serious problems*
  - *You may be viewed as “untrusted” by customers and peers*

Threat Assessment

- *The amount of security required for an entity is based on the security threat*
- *Current major threats include:*
  - *Internal user attacks (still the most common)*
    - *CSI and FBI 1997 (April) Stats: 55% Internal, 15% Dial-up*
  - *Network "hackers" (non-internal)*
    - *CSI and FBI 1997 (April) Stats: 30% Internet*
  - *Electronic commerce compromises*
  - *Digital "money" facilities and transfers*
  - *Residential system attacks and compromises*
  - *Personal information attacks and modifications*

Best Network Security

- *Tiered ("layered") network security architecture provides the best security facilities:*



Cryptography

- *New U.S. laws allow export of 56-bit key crypto provided "key recovery" facilities are included*
- *There are challenges to the legislation regarding encryption export and use*
- *More and more products including cryptographic elements in basic offerings*
- *Still an "element" of total security*
- *Some companies getting around export restrictions via overseas investment*

Key Escrow / Key Exchange

- *Diffie-Hellman still rules for now, but the patent expires soon and this will cause an even greater number of adoptees*
- *Certificate authorities*
  - *In the U.S., the United States Postal Service*
  - *Private corporate authority facilities*
- *Some proprietary facilities begining to pop up in general use*
- *X.509 very popular and growing quickly*

Cisco and Microsoft Tunnels

- *Merging of L2F and PPTP*
  - *L2TP almost finished*
- *Direct challenge to IETF's IPsec initiative (commercially known as S/WAN)*
- *Allows encrypted tunneling of sessions*
- *Whatever comes out is not what is in the industry at this time in any form*

S/WAN and IPsec

- *Firewall vendors are working on a new Internet firewall-to-firewall RFC called IPsec. It is also called S/WAN (Secure/Wide Area Network).*
- *Currently in hypothetical concepts*
- *Two demos of interoperability have been done to date*
- *RFCs still under development*
- *Allows use of incompatible firewalls as VPN provider systems to the Internet*

Authentication Servers

- *Improvements to Kerberos facilities*
- *Private solutions allow per-user authentication facilities and certificate facilities either via individual or software*
- *More trend towards individualized “token” device utilization*
- *Improvements to RADIUS and TACACS+ for use with automated systems and devices on a network environment*

Smart Cards

- *Three major banks in the U.S. are integrating "smart cards" into their credit facilities and also promoting their use for individualized security identification*
- *Concerns over destruction of privacy of transactions and demographic information of individual activities*
- *Concerns on general data formatting and management of "smart card" items*

Biometrics for Authentication

- *Human "input" devices (retinal scan, fingerprint, facial thermography, etc.)*
- *Implants (mandibular, cranial, arm, etc.)*
- *Cellular analysis facilities*
- *Voiceprint*
- *Others...*

Router Security Improvements

- *Currently, any router for any protocol can easily be attacked with what is called a “table update” attack (routing tables corrupted by what looks like a legitimate routing update from an unauthorized “updater” of information)*
- *New routing algorithms will require authentication of routing update as an option in the exchange*
- *This is part of the IPv6 initiative*

Protocol Security Improvement

- *IPv6 has a security layer before the transport protocol which allows some security features*
- *Need classification on a packet-by-packet basis for B-level compliance*
- *Encryption at the protocol level is still needed, but is very far off (if at all)*
- *IP security initiative are worthless for all other protocols in use in company networks that are NOT IP-related*

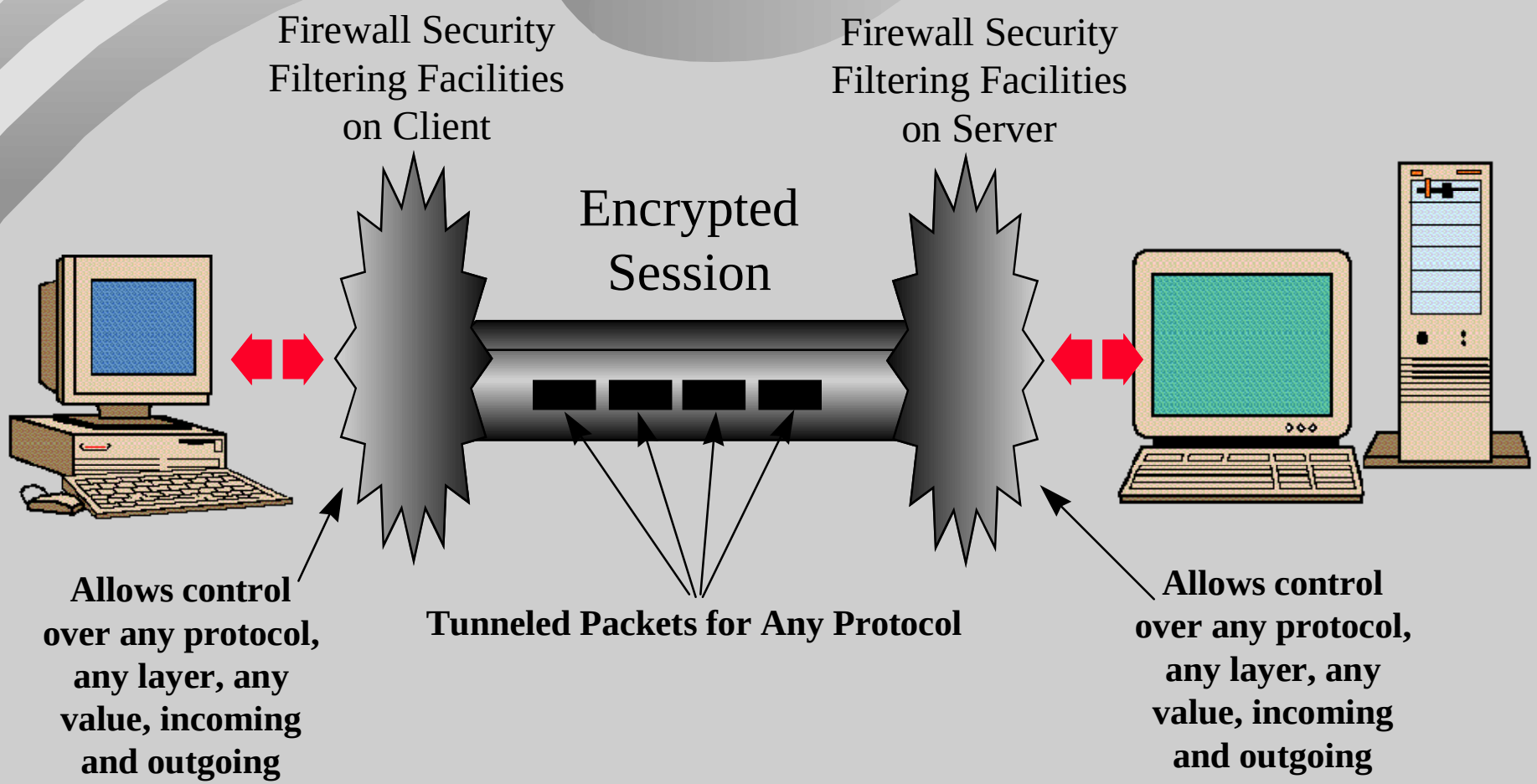
New Firewall Facilities

- *Embedded virus detection for “object” scans (stream still far off)*
- *Certificate authority integration*
- *Support of new and different application protocols (StreamWorks, Videomaster, Realaudio, database streams, etc...)*
- *IPsec integration (slowly and intentionally)*
- *NCSA certification facilities (V2.0 underway)*
- *OS vendor proxy facilities (Catapult project)*

Firewall Certification Update

- *NCSA does not currently test proxy firewalls as rigorously as stateful firewalls*
- *New test suite may invalidate many proxy firewalls and lose their certification*
- *Additional functionality needs to be tested as the threat to network compromise change with time*

New Firewall Concepts: A Firewall on Every System



New Firewall Types

- *Traditional firewalls:*
  - *Packet filtering*
  - *Application filtering*
  - *Proxy*
  - *Stateful*
- *New types: all-inclusive firewalls*
  - *packet, application, proxy and stateful in one product offering*
- *Available now for NT, soon for W95/W97 clients and standalone systems*

New Firewall Management Concepts

- *Client firewall facilities on a workstation*
- *Server firewall facilities on a server*
- *Standalone firewall facilities between networks*
- *Administrative firewall facilities to control multiple firewall installations (could be thousands in the near future)*
- *Use of Virtual Reality facilities for mass-network management of security*

Firewall Management Models

- *One-to-one*
  - *One manager to one firewall at a time*
- *One-to-many*
  - *One manager to many firewalls at a time*
- *Many-to-one*
  - *More than one manager to the same firewall*
- *Many-to-many*
  - *Many designated managers to groups of firewalls and also synchronized updates between groups of firewalls and manager stations*

"Personal" Firewalls

- *Package added to workstation, laptop, etc.*
- *Provides total security end-to-end*
- *Critical for new residential network enviroments (cable MODEMs)*
- *Must be multi-protocol to be useful with existing intranet facilities*
- *Will be the "norm" for telecommuting*
- *Causes security perimeter at an organization to be extended to a "public" LAN environment (especially on CATV)*
- *Is happening NOW!*

ANSI X9 (Banking) Efforts

- **Financial Industry Security Standards (ANSI X9)**

  - **X9.9: Existing wholesale DES MAC standard**
  - **X9.19: Existing retail DES MAC standard**
  - **X9.23: Existing wholesale encryption standard**
  - **X9.17: Existing, recently updated wholesale DES key management standard**
  - **X9.24: Existing retail DES key management standard**
  - **X9.30-1: NIST DSS**
  - **X9.30-2: NIST SHA**
  - **X9.30-3: Certificate management for DSA (much new material beyond X.509)**
  - **X9.31-1: RSA signature (aligned with ISO 9796)**
  - **X9.31-2: Hash algorithms for RSA (i.e. MD2, MD5, SHA, MDC-2)**
  - **X9.31-3: Certificate management for RSA (99% same as X9.30-3)**
  - **X9.41: Security Services Management**
  - **X9.42: Diffie-Hellman key agreement (and variant for store and forward use)**
  - **X9.44: Key transport using RSA**
  - **X9.45: Authorization certificates**
  - **X9.xx: Certificate extensions (also being progressed in ISO)**

Security Certification

- *Certified Information System Security Professional (CISSP) now in year four*
- *Effort to combine with Certified Computer Professional of ICCP*
- *Enhancement to Certified Network Expert testing for security facilities*
- *More effort by traditional security organizations to emphasize technical security as well as management issues*

Legal Resources

- *Netlaw by Lance Rose (Osborne-McGraw Hill)*
- *Law on the Net by James Evans (Nolo Press)*
- *gopher://una.hh.lib.umich.edu:70/00/netdir stacks/citizens:bachpfaff*
- *http://www.portal.com/~cyberlaw/cylw_home.html*
- *http://www.eff.org*
- *http://thomas.loc.gov*
- *Search engine: http://altavista.digital.com*

Web & Other Resources

- http://www.yahoo.com *(search for crypto)*
- NIST publications
- RSA web server (www.rsa.com)
- EFF web server (www.eff.org)
- Various cryptographic research BBS and web sites
- Books (e.g. Applied Cryptography)
- Hacker Chronicles II CD-ROM product
- 2600, Phrack, etc., underground publications
- ANSI and IEEE standards
- Security organizations (CSI, NCSA, ISACA, $(ISC)^2$, etc...)

Summary

- *There are a LOT of hackers on the Internet and other networks - like your own!*
- *Protection is a multi-level defense, not just one layer of protection*
- *Internal breaches are much more common*
- *Intra-nets need security as much as Internet access and the problems are more intense*
- *Experts abound - be careful and require credentials from your security professional*
- *Use the Internet as a tool for gathering information on security as well as other items*

Questions?

NETWORK-1
Software and Technology, Inc.

Bill Hancock, Ph.D., CISSP
Network-1 Software & Technology, Inc.
DFW Research Center
878 Greenview Dr.
Grand Prairie, TX 75050
(972) 606-8200
(972) 606-8220 fax
Internet: hancock@network-1.com
Web Server: http://www.network-1.com