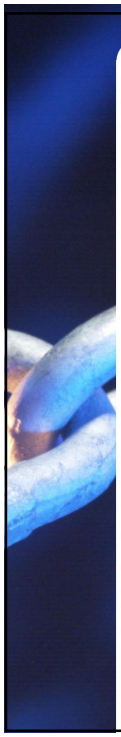



# Security in Global IP Networks

Tatu Ylönen <ylo@ssh.com>
SSH Communications Security Corp
http://www.ssh.com





## What are global IP networks?

- The Internet
  - The “consumer internet”
  - Global uncontrolled network of operators “everyone”
  - Automated routing protocols sort out chaos
- Large corporate networks
  - Many global corporations have global internal networks connected to the Internet only at certain places
- Internal operator (ISP) networks
  - Multi-tier: global, regional, local, resale carriers
  - Multi-service, with service level guarantees
- Future telecommunications networks
  - Long-distance IP telephony and other “closed” networks
- Closed networks
  - Military, corporate, or government networks

# Centrally managed networks

- Large corporations, large operators, and military & government usually control their own networks
- Such networks still typically contain links (or even backbone routing) outsourced from third parties
- Link security cannot be assured except by encryption controlled by the network owner (links under independent control or too expensive to protect physically)
- Implementations
  - Leased lines
  - Leased pipes (bandwidth)
  - Frame relay or MPLS routing-based VPN
  - Encryption-based VPN
- Security by end-to-end or link-by-link encryption
- Perimeter firewalls typically limit access






# Distributed multi-player networks

- The open internet
- Networks of many Internet service providers who buy backbone capacity from someone
- Traffic passes through multiple uncontrolled parties
- Open network includes also hostile participants
- Only end-to-end (or firewall-to-firewall) encryption is feasible
- Firewalls used to limit access to connected private networks
- Access typically paid as a fixed monthly charge, as part of the phone bill (for access), or sometimes as a fixed charge plus volume-based charges
- Typical cost to user is low; no real concern of how much one can afford to use the network
- Data transmission is low-margin business with many competitors
- Few quality-of-service guarantees; best-effort routing

# High-cost networks ("telecommunications style")

- Access billed at a high per-minute or per-byte rate
- Examples: GSM Data, GPRS networks, 3G networks; hotspot solutions for e.g. airports with GSM authentication
- Access cost per hour can exceed typical monthly charge in other models
  - Consequently, cost is major limiting factor on use
- Existence facilitated only by monopolies/oligopolies:
  - Government monopoly
  - Control over limited resource, e.g. radio bandwidth
  - Vertical control of terminals, access, transmission, and applications
  - Lock-up in proprietary technology infrastructure
- Existence threatened by more aggressive, more open competitors
- This kind of business model needed to justify 3G auction prices
- Authentication, access control and billing are key in this model






# Who would attack a network?

- Governments, with well-trained special troops
  - Information warfare, economical/semi-military pressure
  - Intelligence gathering, espionage, "crime fighting"
- Corporations (by proxy, of course)
  - Disturbing competition, stealing trade secrets (plans & technology)
- Organized criminals, high-tech criminals
  - Extortion, fraud
  - Stock trading fraud using stolen information
  - Hiding tracks, secret communication, hiding money
  - Fake banking & trading transactions
- Hackers & teenagers
  - Getting status & ego trips; frustration
- Terrorists & anarchists
  - Disturbing normal operations of the society

# Possible points of attack

- Backbone routing infrastructure
- Name servers
- Accounting, billing, access control servers
- Application servers, databases, file servers, backups
- Web servers
- Workstations, servers
- Software repositories, versioning systems




SSH® - Making the Internet Secure™

# Attack methods

- Password sniffing & other forms of credential stealing
- Using existing attack scripts & tools
- Exploiting known vulnerabilities and implementation flaws
- Exploiting design flaws (software gets run and transmitted unexpectedly due to bad design; most viruses are based on this)
- Trojans (software that user is tricked to execute)
- Active network attacks and protocol design flaws
- Exploiting misconfiguration
- Chaining compromised machines to hide tracks

http://www.ipsec.com
http://www.ssh.com
Copyright © 2000 SSH Communications Security Ltd.

# Security measures

- No plain text passwords
- Cryptographic authentication
  - Smartcard / token (PKI)
  - One-time passwords & timed passwords
  - Challenge-response with cryptographic hash functions
- “Private” networks
- Encryption & message integrity (VPNs, IPSEC)
- Firewalls to protect against implementation problems






# Plain text passwords still used

- Router configuration
- Routing protocols
- SNMP network management
- Telnet and FTP access
- E-mail access
- Database access
- File sharing
- Etc.

# Cryptographic authentication

- Fully encrypted and authenticated exchanges
  - e.g. SSH2, (IPSEC IKE)
- Cryptographic challenge-response but plaintext
- Digital signatures
- Centralized authentication servers, such as Kerberos
- Esoteric methods, such as zero-knowledge proofs






# “Private networks”

- Routing used to create virtual private internets for each customer
- Typically based on frame relay, ATM, or MPLS; virtual routers
- Not secure against network-level attacks or untrustworthy operators

- Encrypting VPNs create private networks by encryption
  - Only form of VPN that has controlled security
  - Sometimes managed by a specialist service company
- Driven by two needs
  - Creating virtual private networks for organizations
  - Accessing such closed networks from the public Internet securely

# Firewalls

- Limit the number of computers and devices that are exposed to external threats, making it less relevant whether they have implementation bugs or configuration errors that cause security problems
- Only protect the external perimeter, no protection against internal attacks
- Frequently include VPN technology to encrypt traffic to other sites and to remote users
- Not completely foolproof, but a “minimum requirement”






# VPNs (Virtual Private Networks)

- Significant cost savings by using encryption instead of having operators do something
- Only way to provide controlled security between two points
- Large networks require PKI for security
- IPSEC is the standard protocol for encrypting IP traffic

# Public Key Infrastructure

- Key to making large-scale security systems (VPNs, e-mail security etc) practical
- Banking, government, binding digital signature applications have not taken off yet
- Key problem: how to make PKI scale world-wide and to numerous applications
  - Trust issues: are Central American governments trustworthy, or should they be excluded from trade?
  - Will CIA or KGB or Mossad be able to fake binding contracts in everyone's name?
  - How to run a global PKI in practice?
  - How to make solutions interoperate globally on global networks?
- Expect major changes in this area in the mid term




SSH® - Making the Internet Secure™

# Security standardization

- IETF (Internet Engineering Task Force) has key role in standardizing security for IP networks
- Only standards can gain global acceptance
- Intelligence agencies and export have in the past had significant influence on security standards
- A lot has been done, but a lot still remains to be done

http://www.ipsec.com
http://www.ssh.com
Copyright © 2000 SSH Communications Security Ltd.

# Key remaining problems

- Security for the routing infrastructure
  - Encryption does not help if routing attack cuts traffic entirely
- No widely deployed replacement for passwords available
- Current PKI solutions do not scale to global use
- Wide-scale e-mail security currently not widely used
- Management issues for security are still in a state of flux
- Paying for access and related authentication and accounting mechanisms are still at an early stage






# Summary

- Many global IP networks coexist
- Different networks have different security requirements and management architectures
- No integrated solution exists, just pieces for point solutions
- Security of the network infrastructure is key for dependable networks and stable information society