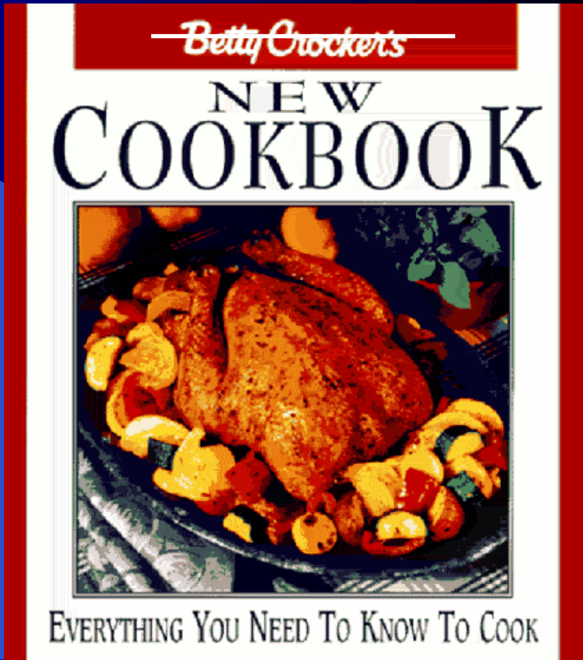
Security for Telecommuting and Broadband Communications a.k.a. “Telecommuting Security Cookbook”

Rick Kuhn

NIST Computer Security Division

csrc.nist.gov

NIST’s



Rick Kuhn kuhn@nist.gov
301-975-3337

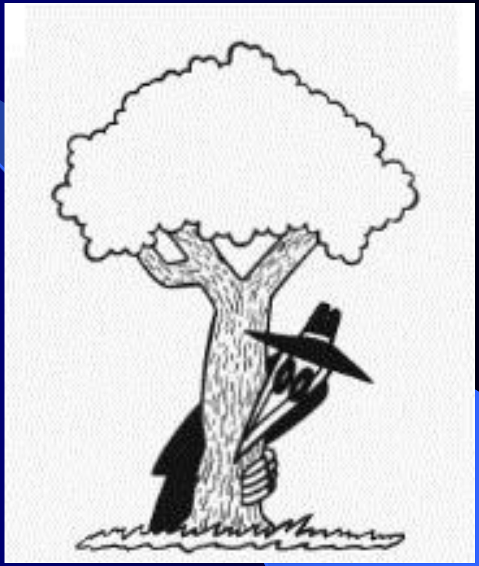
Tim Grance grance@nist.gov
301-975-4242

New NIST Recommendation

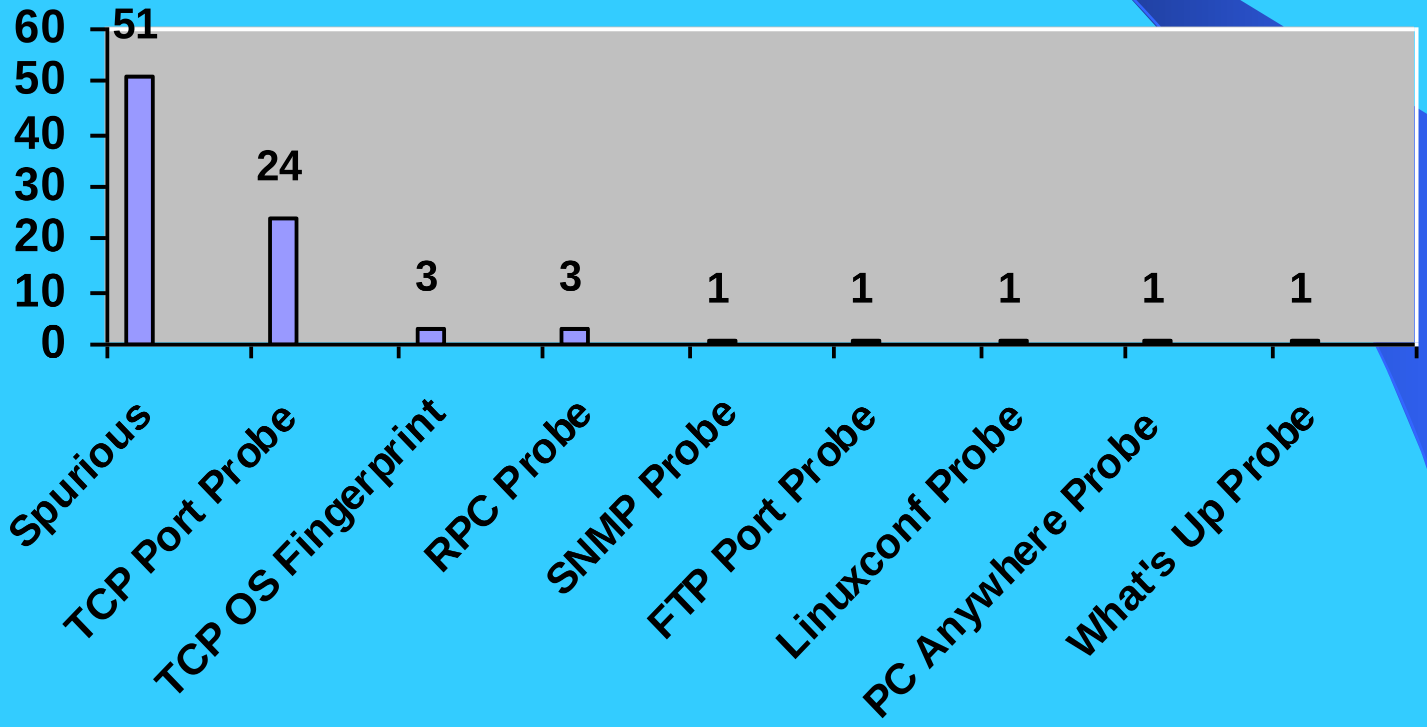
- For users, system managers, and agency administrators
- Step-by-step instructions on
  - Personal firewalls
  - Securing web browsers
  - Securing PC configurations
  - Home networking
  - Virtual private networks
  - Telecommuting architectures
  - Agency/enterprise considerations

What's different about broadband?

- Always on
  - Longer exposure to internet
  - User less likely to notice attack
  - May be permanent IP address
- Higher speed
  - Downloads of malicious code faster, less noticeable
  - Faster probes for vulnerabilities



10-Day Record of Intrusion Attempts



Personal firewalls

- First line of defense
- Estimates are more than 90% of home PCs have some vulnerability to Internet
- Good software firewalls available at low or no cost (examples listed in document)
- Stand-alone firewalls for home machines very cheap – under $100

Firewalls

- **Establishing a secure firewall configuration** – explains how to set up firewall
- **Running an online security assessment** – free scanners listed
- **Firewall features** – lots of variation among products

Firewalls – What to Look For

- **Logging** – track IP address of suspicious packets, some let you find out where packets from (‘whois’)
- **Port hiding** – does not respond to unsolicited contacts
- **Automatic lockout** – disable connection when computer not in use

Firewalls – What to Look For

- **Connection notification** - lets you know when a program attempts to send out from your PC - detects spyware
- **Paranoia level tuning** - pre-configured settings for desired security level
- **Password protected configuration**
- **Configurable rule set** - advanced feature

Personal firewalls – what to do

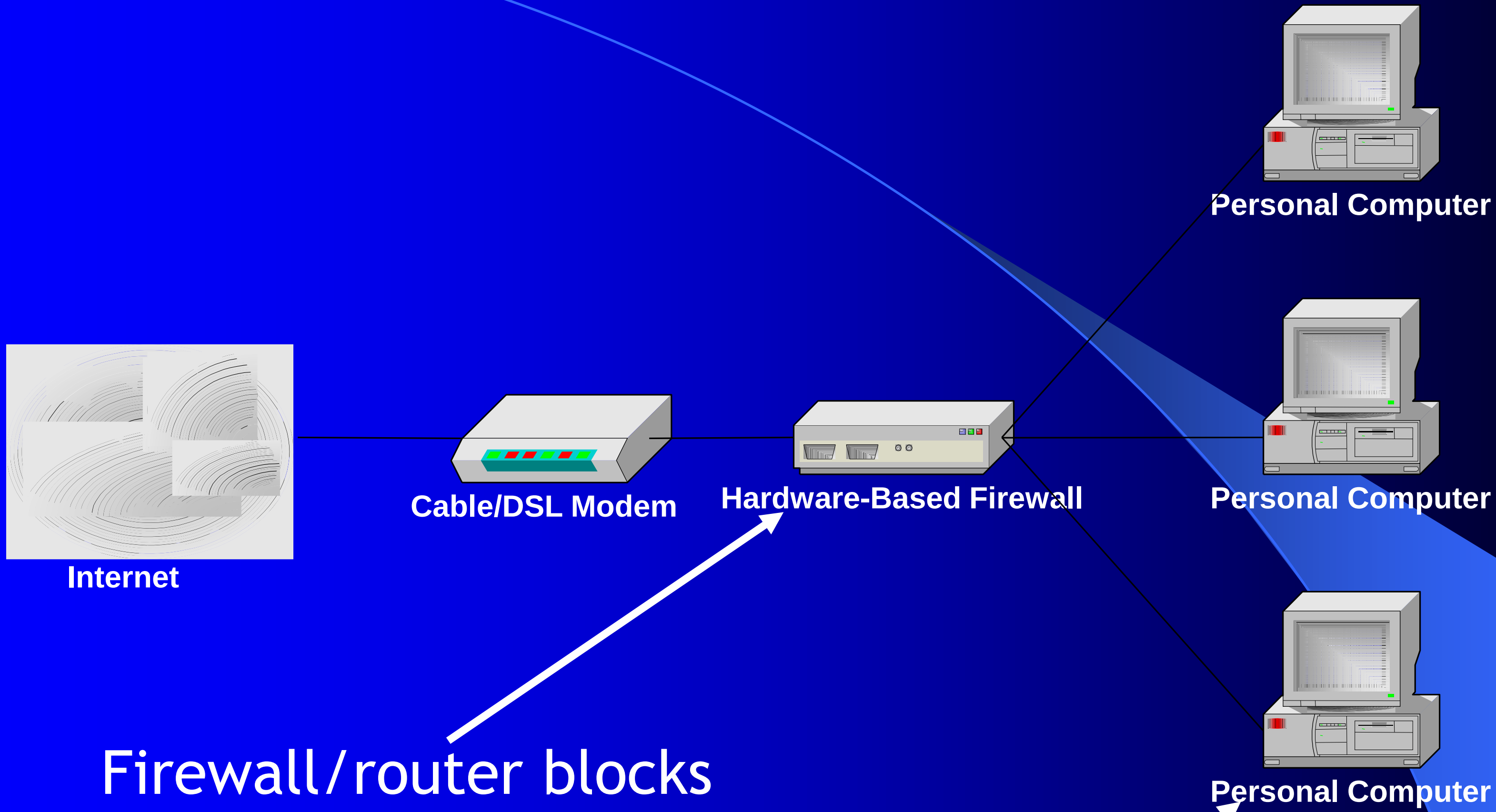
- All home networks connected to the Internet via a broadband connection should have some firewall device installed.
- Install stand-alone hardware firewall
  - Blocks incoming traffic, hides PC
- Install software based firewall
  - Can block suspicious outgoing messages and and alert user
- Run an online security scan

Stand-alone Firewalls – How to Set Up

- Change default admin password
- Check for software/firmware updates - software load may have changed since firewall was shipped
- Disable WAN requests - hides existence of PC to unsolicited messages
- Ensure that all unnecessary ports closed
- Restrict or disable remote administration - usually can use direct USB connection for firewall admin

Software Firewalls – How to Set Up

- Log IP address, date/time of infractions
- Drop incoming packets to known insecure services – e.g. NETBIOS if not needed
- Enable stealth mode – no reply to unsolicited packets
- Shut down connection when not in use
- Enable connection notification – to detect spyware



Firewall/router blocks unneeded ports

Software firewall blocks spyware and Trojan horses

Securing Web Browsers

- Browser Plugins – a dozen or more usually
- ActiveX – becoming ubiquitous on IE
- JavaScript – almost impossible to do without
- Java Applets – needed for multimedia
- Cookies – almost universal

Securing Web Browsers – what to do

- Review plugins and disable unneeded ones
- Use built-in Active X security features, take precautions on using it
- Disable cookies unless needed, or allow only session cookies; delete frequently
- Consider use of internet proxy server if very concerned about privacy

Securing PC Configurations – what to do

- **Strong passwords** – most basic requirement
- **Securing file and printer sharing** – only as necessary
- **Updates** - Reducing operating system and application vulnerabilities updates
- **Virus checkers** –essential, configure to run weekly or more often

Securing PC Configurations - what to do

- Protecting yourself from e-mail worms and viruses
- Spyware removal tools
  - Some free tools to remove spyware
  - Some software firewalls can detect spyware
- Encryption software to protect privacy

Home Networking

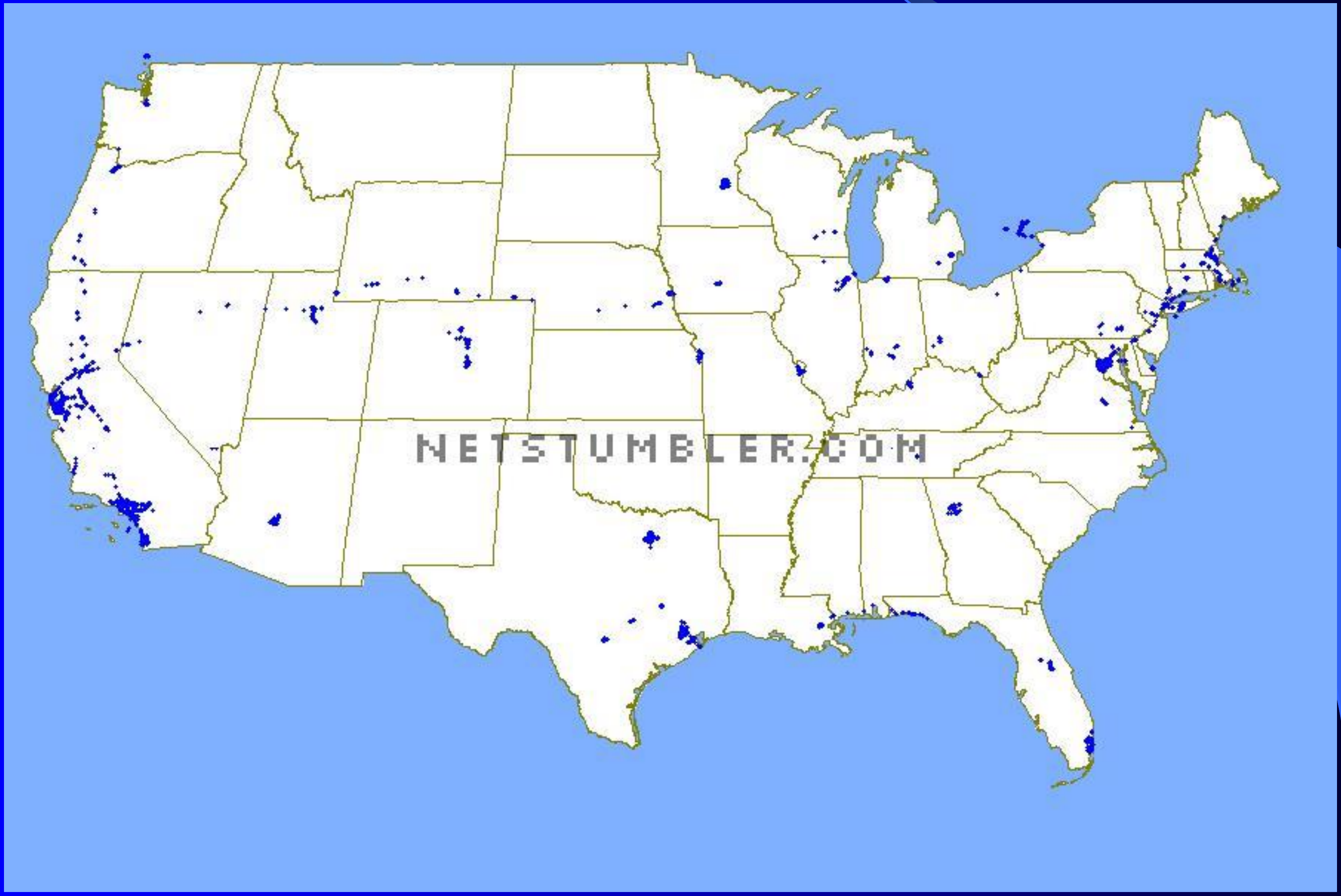
- Ethernet Networking
- Phone-Line Networking (HPNA)
- Power-Line Networking
- Wireless Networking
  - HomeRF
  - 802.11 and 802.11b – WEP intended to provide security equivalent to wired (but doesn't!)

Wireless Networking Security Issues

- Server set ID (SSID) sent unencrypted – attacker can eventually obtain SSID, which enables them to connect to your network
- 802.11b WEP encryption flawed – publicly available software can crack 802.11b with enough packets - home networks reasonably safe, office networks not (theft of service)
- Remote admin (SNMP) with default password
- Denial of service risk inherent in wireless

Home Networking Security

- Wired – OK Wireless – not so OK



Wardriving, “drive-by hacking”

- Available on Internet from people with too much time on their hands:
  - Perl scripts to break 802.11b “wired equivalency protocol” (WEP)
  - Plans to build sensitive antennas using parts from Home Depot and Pringles can

“Drive-by hacking” Risks

- **Privacy** - moderate
  - Don’t put sensitive information on wireless
- **Theft of service** - more serious
  - Campus or business park - easy for hackers to mask identity - your organization gets blamed for intrusions
  - Home - less concern, but don’t ignore

Home Networking – what to do

- Use file and printer sharing only as necessary
- Change default
  - admin passwords and
  - SSIDs
- Use encryption, even if it is not perfect

Virtual Private Networks

- **VPN security** - connectionless integrity, data origin authentication, confidentiality or privacy, traffic analysis protection, access protection
- **VPN modes of operation**
- **VPN protocols**
- **Peer authentication**
- **Policy configuration**
- **VPN operation**

Virtual Private Networks – what to do

- First ensure that needs can't be met with less expensive tools
- Agency system admin responsible for configuring VPN and providing telecommuter with proper software
- Educate users on correct operation

Telecommuting Architectures

- **Voice Communication** – security considerations of different types of phones
- **Electronic Mail** – different ways to handle it based on security requirements
- **Document and Data Exchange**
- **Ways to combine** – to provide voice, email, and document exchange in cost effective ways

Voice Communication

- **Corded phone** – most secure; tapping requires physical connection
- **Cordless** – can be picked up on scanners, baby monitors, etc.; 900 MHz, 2.7 GHz more secure <u>for now</u>
- **Cell phones** – can be picked up with UHF tuner
- **Digital PCS** – more secure <u>for now</u>
- PC based voice communication (Voice over IP) – depends on security of your PC and Internet
- **What to do –<u> get a corded phone for office</u>**

Electronic Mail

- **Remote login** – may use unencrypted passwords (POP3)
- **E-mail forwarding** – user doesn't need to log in to central system at all; OK if email not sensitive
- **Virtual Private Network (VPN)** – great security but expensive and more complex to install/administer
- **What to do**– choose based on cost and what's more important, central system or email contents

Document and Data Exchange

- **Remote connection** – needs good administration
- **FTP and web file transfer** - likewise
- **E-mailing document and data files** – OK if material not sensitive
- **Virtual Private Network (VPN)** – secure but expensive
- **Physical transfer (sneaker net)** – secure but annoying
- **What to do**– choose based on cost and what’s more important, central system or document contents

Agency/enterprise Considerations for Telecommuting Security

- **Controlling system access** - strong passwords, one-time password generators, Smartcards, biometrics
- **Protecting internal systems** - restricted access, firewalls and secure gateways, location of resources, proxy servers, encryption
- **Protecting home systems** - **security policy, employee accountability, removable hard drives, data encryption, dedicated use, locked rooms or storage containers, home system availability.**

Agency/enterprise Considerations – what to do

- Establish standard security configuration for telecommuter systems
- Organization should provide pre-configured PC for home user
- Limit use to official duties (but assume this won’t always be followed!)

Top 10 User Precautions for Telecommuting

1. Install software firewall
2. Add stand-alone firewall (also)
3. Install anti-virus software
4. Turn off file and printer sharing (unless needed for home network)
5. Update operating system and browser regularly

Top 10 User Precautions for Telecommuting

6. Know how to turn off and delete cookies
7. Use strong passwords
8. Install spyware detection and removal tools
9. Use only amount of security necessary
10. Consider encryption or VPN software if you need it

Conclusions

- Telecommuting can be done with an appropriate level of security, at a reasonable cost!
- Security motto:
  you don't have to outrun the wolves,
  just the people you're with …

- *Contacts:*

– Rick Kuhn	kuhn@nist.gov	301-975-3337
– Tim Grance	grance@nist.gov	301-975-4242

- Web site: csrc.nist.gov