

Security Issues on Home Teleworking over Internet

Kenji Rikitake

KDDI R&D Laboratories

November 21, 2001

Teleworking gains popularity

- Most business tasks are teleworkable
- Workers self-manage the tasks
 - Where, when, how, and how long
- Need to preserve the Quality of Lifestyle
 - Less commuting hours and more free time
 - Requirement of caring family members
 - Autonomous person considered valuable

Issues on Teleworking over Internet

- System Performance Issues
 - Adequate for document handling
 - Optimization needed for audio-visual tasks
- Security Issues are Critical
 - Always-on links increase vulnerabilities
 - Ordinary workers don't care about security
 - Solution: secure systems and education

So what we've got to do now for home teleworking?

- Making teleworking security policies
 - Security-protection procedures for home
 - Education for home information security
- Securing teleworking systems and links
 - Secure communication tools for home computers
 - Privacy-protection tools for home
 - Raising awareness for potential risks

Organizational Security Policies and Teleworking

- Teleworkers are no exception
 - Understanding policies is critical
 - Teleworking systems can be vulnerabilities
- Two major core issues:
 - Information access rights management
 - Keeping sensitive information confidential
- Classified tasks are not teleworkable

Information Security on Home Teleworking

- Teleworkers must do on their own
 - Guarding business equipments
 - Preventing potential hazards of incidents
- Home security and privacy
 - Thieves and spies want your information
 - A dedicated room is critical for working
- Uninterruptible power supply is a MUST

Keeping Sensitive Information Safe at Home

- Family members may become the risks
- Shared equipments are dangerous
 - Messages revealed from a FAX machine
 - Shared phone lines can be wiretapped
- Sharing computers can be harmful
 - Individual data must be kept private
- Unused media must be promptly destroyed into pieces

Administrative Issues of Secure Teleworking

- Workers expect risk-free environments
 - Corporate networks are usually well-protected
- Home networks are exposed to risks
 - They are usually not protected at all
- Immediate protection needed for home
 - Anti-virus software with proper updating
 - Per-host firewall for each and every host

Secure Communication Tools for Teleworking

- Securing TCP connections
 - SSH (secure shell)
 - SSL (Secure Socket Layer)
- Securing IP datagrams and networks
 - VPN with IPsec
- Securing end-to-end messages
 - PGP for email

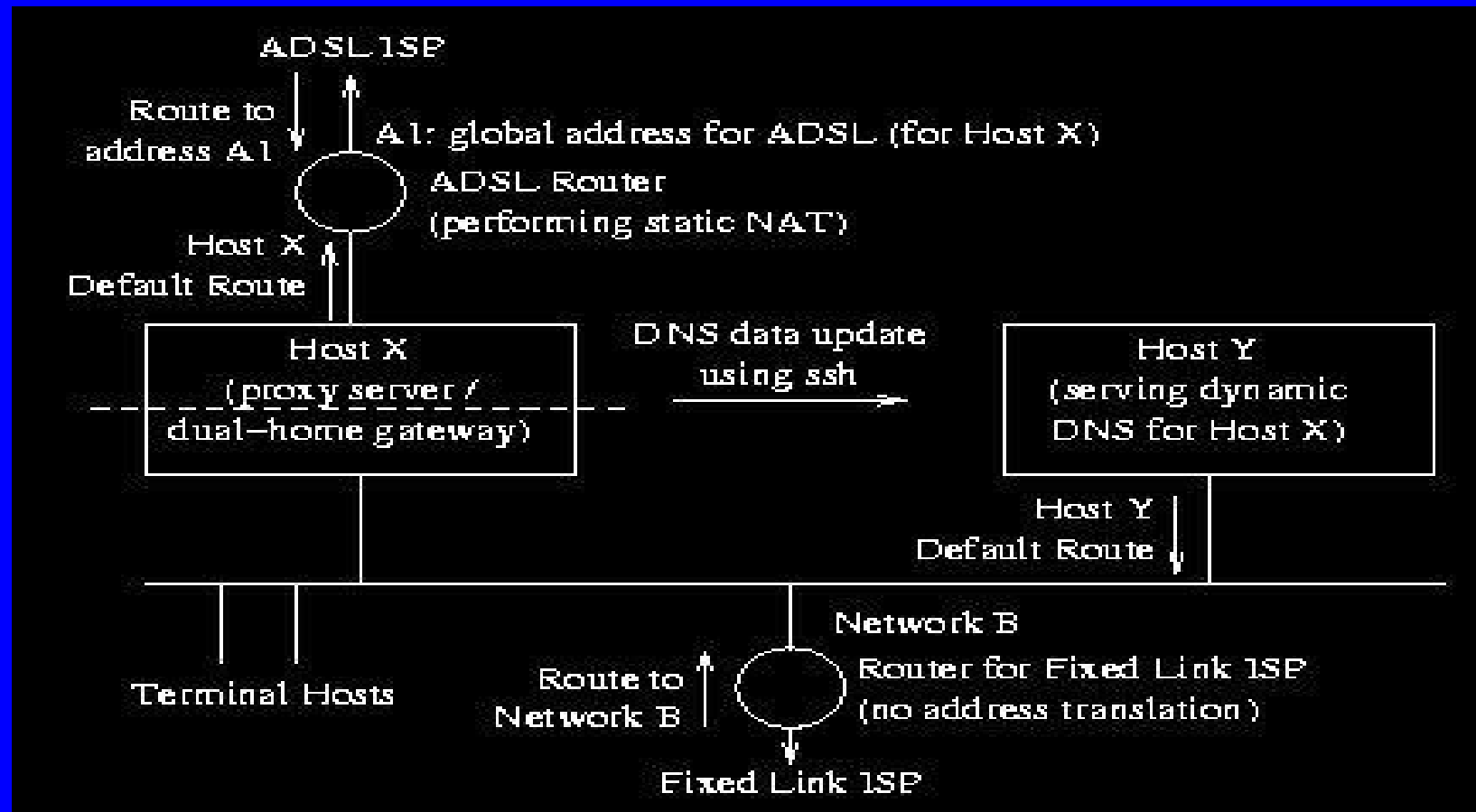
Our Teleworking Systems

- Two remote teleworking branches
 - Kyoto branch office
 - Rikitake's home in Toyonaka, Osaka
- ADSL connectivities
 - Firewalls to provide corporate-level security
 - Adequate performance for daily tasks
 - Inexpensive comparing to leased lines

So what we do over teleworking links?

- Document tasks with no difficulty
 - Web-based operation with VPNs
 - Remote printing over VPN tunnels
- Some experimental tasks
 - Remote login over SSH
 - Secure POP3 over SSH
 - Internet Phone System: MeeTwo

Our showcase - Rikitake's home systems



Lessons Learned

- ADSL bandwidth: adequate for business
 - uplink 512kbps, downlink 576k/1.2Mbps
- Internet Phone needed to redesign
 - voice quality insufficient
 - at least 16 to 32kbps for voice needed
- IPsec VPN system flexibility needed
 - single-host only; subnet capability needed

Conclusions: we can do more

- Home teleworking works well
 - Autonomous workers make the most of it
 - Writing documents is fully teleworkable
- Real-time tasks need more bandwidth
- Security is the top-priority issue
 - More risks will show up on home networks
 - IPv6 will reveal more systemic vulnerabilities

End of Presentation

Acknowledgements to:

Dr. Hiroshi Nagata, our mentor

Mr. Tohru Asami, our president and leader

Dr. Shin-ichi Nakagawa, CRL

Dr. Mieko Kimura, TRILS

and the members of KDDI R&D Labs.