Chapter 1.24
Telework Information Security

Loreen Marie Butcher-Powell
Bloomsburg University of Pennsylvania, USA

INTRODUCTION

The sophistication of technology available to businesses as well as to homes has increased dramatically in the last 10 years. The speed of information exchange and the ease of use of computer software have become a major influence on the decision of businesses to allow unconventional working environments. As a result, telework has become an increasingly preferred option to working in the office (Manochehri & Pinkerton, 2002). In the early 1970s, Jack Nilles coined the word *telework*. Telework refers to an approved working arrangement whereby an employee—a teleworker—officially performs his or her assigned job tasks in a specified work area of his or her home on a regular basis (United States Department of Defense, 2002). According to the Communications Security Establishment's Telework Pilot Program (2002), telework has become a very important alternative work pattern, which allows employees to better manage their home life and work life in a complex society. Telework offers many advantages, including the following:

1. Substantial savings in physical facility-related costs, including rent, storage, and electricity;
2. Expanding labor pools without geographic restrictions (Hirsch, 2002; Mehlman, 2002; Motskula, 2001).

After the September 11, 2001, terrorist attacks on the United States of America, many corporations turned toward telework (Niles, 2001; United States Department of Defense, 2002). However, with the increased benefits afforded by teleworking, there are increased security risks, including viruses and data tampering (Atwood, 2004; Hirsch, 2002; Motskula, 2001; Quirk, 2002; Rubens, 2004).

BACKGROUND

In order to understand the importance of securing the infrastructure for telework, the scope of the term *security* from a telework infrastructure perspective must be defined. The term *security* leads

one to investigate the survivability of a network or related assets to an attack (Allen, 2001). This is the key to the integrity of the data resident on the network system and alludes to the flexibility of network assets to cope with internal and external intrusions and corruption (Allen, 2001). Further, the survivability of a network and its associated economics need to be assured, regardless of the transmission or storage media (Landwehr, Bull, McDermott, & Choi, 1994). However, the economics affiliated with security issues are not limited to the system level, but rather it can extend within the confines of the network infrastructure (Allen, 2001). According to Dhillion and Backhouse (2000), information systems security in a telework environment must address both the data and the changing organizational context in which data are interpreted and used.

Existing research has shown that in order to prevent sensitive data from being disclosed, modified, or made unavailable in transit between two endpoints, the communications link must be protected (Davis, 2001; Hercovitz, 1999). Threats that utilize or take advantage of the communications link can be wire tapping, replay attacks, man-in-the-middle attacks, war dialers, denial of service attacks, and buffer overflow attacks. Possible safeguards to help mitigate these threats include firewalls, authentication and access control measures, and virtual private networks (VPNs). However, VPNs have remained the most popular way to secure a telework infrastructure (Davis, 2001; DeSanctis et al., 1996).

VPNs use familiar wide area networking (WAN) technology and protocols. Generally, a client or workstation using WAN technologies sends a stream of encrypted point-to-point protocol (PPP) packets to a remote server or router. This same process occurs with VPNs, except instead of going across a dedicated line, the packets go across a tunnel over a shared network such as the Internet. VPNs allow teleworkers to gain remote access to a specific corporate network via the Internet by tunneling into the corporate intranet (Brown, 1999).

VPNs are a combination of tunneling and encryption algorithms that carry traffic over the Internet, a managed Internet Protocol (IP) network, or a service provider's backbone network (Stallings & Van Slyke, 1998). It provides encrypted tunnels through the Internet that permit off-sites to communicate securely. Tunnels provide a secure path for network applications. For example, if a teleworker wants to connect into the corporate network to access a company's intranet, this individual can dial into or connect to his or her local Internet service provider (ISP) and connect as though he or she were onsite. The teleworker can then initiate a tunnel request to the destination security server on the corporate network. The security server authenticates the user and creates the other end of the tunnel. Next, the teleworker sends data through the tunnel. Data are encrypted by the VPN software before being sent over the ISP or Internet connection. The destination security server receives the encrypted data and decrypts the packets. The security server forwards the decrypted data packets onto the corporate network. This same encryption process applies if any information is sent from the corporate network to the teleworker (Davis, 2001).

Traditionally, VPNs utilize both tunneling methods and encryption algorithms to carry traffic over the Internet. For example, network traffic reaches the VPN backbone using any combination of access technologies, including T-1, Frame Relay, Integrated Services Digital Network (ISDN), Asynchronous Transfer Mode (ATM), or simple dial-up access (Davis, 2001).

The most commonly accepted method for creating VPN tunnels is called Layer 2 Tunneling (L2T). L2T is created by encapsulating a network protocol such as IPX, NetBEUI, and AppleTalk inside the Point-to-Point Protocol (PPP), and then encapsulating the entire package inside a tunneling protocol. Traditionally, L2T VPN packets