Global Information Assurance Certification Paper

Telecommuting Safely – Remote Node or Remote Session?
Mark Levine
2/19/2001

Many large companies have begun using telecommuting as a method to reduce cost and improve employee satisfaction. Unfortunately, the benefits gained by telecommuting come with the price of an increased security threat. Some flavor of VPN is commonly used to provide security for these home users. Regardless of which product or protocol ends up being used, serious issues remain. This has to do with the function that a VPN product performs, provide secure communication between two trusted entities. In the telecommuting model the home office is arguably not trusted. The lack of physical access control would indicate that no matter how trusted a computer is when first configured, after spending time at a users home, the state of a machine is in question.

In "A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs", Sean McAleer detailed many of the risks that are faced when a network attached device leaves the access controlled office environment. This paper will focus on remote employees using computers rather than wireless devices, with a focus on data moving outside the security perimeter of the trusted computer systems of a central office. As described by Bruce Schneier's article "security is not a product, It's a process." While VPN, PKI and encryption are powerful tools, they do not provide a silver bullet that solves all security issues. It doesn't matter how secure the front door is if all the windows are open. It is possible to deploy a solution that would allow an engineer to travel to a country like Israel, where travelers are routinely forced to turn over their laptops for examination, with no fear of data being compromised.

Traditional VPN – Remote Node

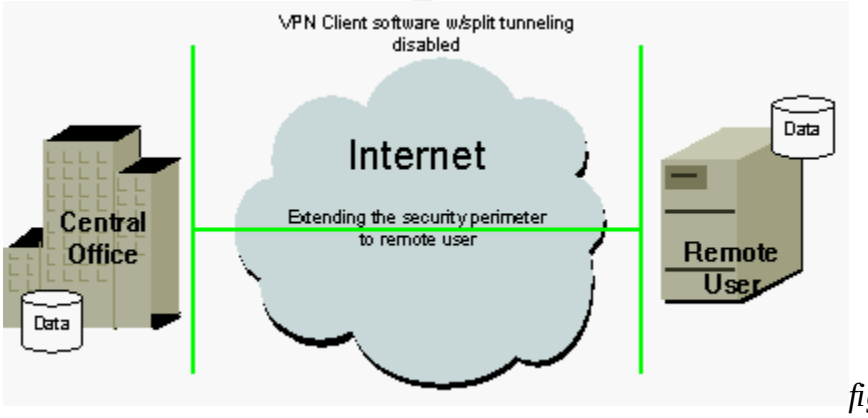

fig1

The simplest VPN solution consists of an Internet connection and VPN client software running on a computer. The first major risk involves split tunneling, the ability for the client to route traffic both to the Internet and the VPN tunnel. If the VPN client has split tunneling enabled, the client is on both the Internet and the central office Intranet at the same time, this has obvious risks. With split tunneling disabled the remote computer, in essence, is protected behind the central office firewall making this is a very secure

configuration while the tunnel is in place *fig1*. As long as the tunnel is in place and the state of the remote computer is known, the remote computer is part of the central office's trusted computer system.

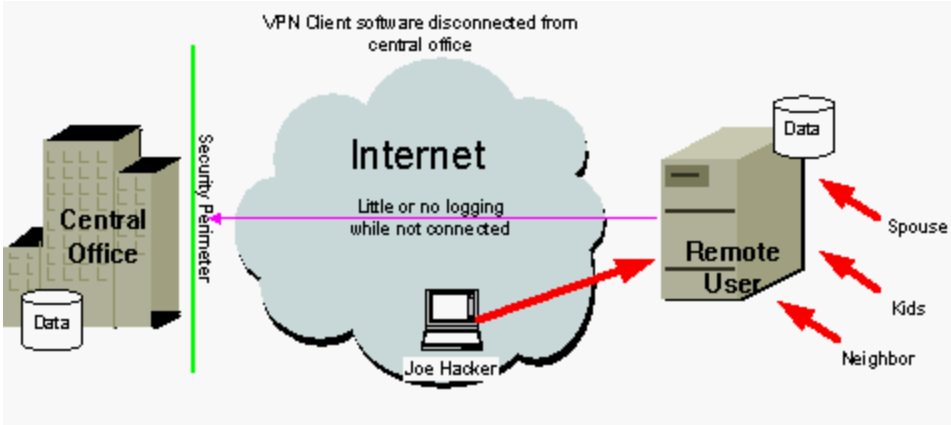

Fig2

The security issues appear when the VPN tunnel is not connected *fig2*. Data that was being protected by an enterprise class firewall and stored on a carefully monitored file server is now protected by a $39 personal firewall and some NTFS file permissions, if your lucky. And if the data is of a sensitive nature, the central office has legally lost track of that data. Using medical records as an example, the upcoming security standards mandated by HIPAA would consider this loss of control a major violation. The recently approved HIPAA privacy standards require the tracking all movement of patient sensitive information for six years.

While not addressing the any audit requirement, hard drive encryption software would provide a strong solution for the protection of data. But hard drive encryption software depends on the end user to decide what data needs to be protected. So if an end user decides that it is inconvenient to enter a pass-phrase to unlock an encrypted drive, they may start saving data to other locations on their hard drive, thereby bypassing the protection of encryption. Also, in the event of a hostile party gaining possession of the hard drive, the data could possibly still be retrieved if enough processing power was brought to bear.

Many IT professionals would look to using certificates or some form of PKI to add a layer of security to their VPN clients. In the context of a computer system in an uncontrolled environment, a certificate authentication scheme could be less secure than traditional password authentication. The strength of certificate based authentication is a function of the security of the private portion of the key pair. If a weak pass-phrase is used to protect the certificate, then it could be brut forced. Once compromised the certificate could be used to connect to the central office and possibly authenticate to additional internal systems. And unlike passwords that change regularly, certificates can be valid for a year or more.

All of the above issues are a result of the isolation of the remote machine with no method to report brut force attacks while not connected to the central office. There is also no method to report simple activity. Any data stored on the remote computer could be improperly transmitted or modified. And all record of these activities would only exist on the compromised system, a serious violation of the C2/CAPP standard for event logging. The moment the VPN link comes down the remote computer's state cannot be guaranteed and therefore cannot be a part of the central office trusted computer system.

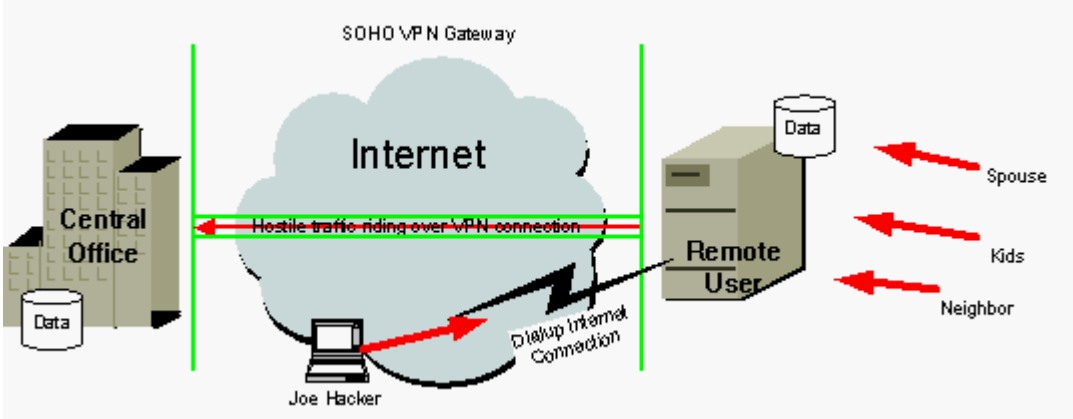

fig3

Marketed as an end all solution for telecommuting connectivity, SOHO firewalls with VPN capabilities are in fact a serious backdoor. They bypass the perimeter authentication that would traditionally take place before a remote user would have access to the central office internal network *fig3*. The VPN connection is based on the central site trusting the remote SOHO VPN firewall. There is not necessarily any verification that the remote computer is authorized beyond its connection to the trusted SOHO firewall. A worst case example of this would be a remote user who sets up a wireless network behind their company provided SOHO VPN gateway. If this wireless network was not setup properly, a neighbor could purchase a wireless network adapter and begin scanning your network is seconds. To make matters worse, many of these SOHO VPN gateways hide the remote network behind a single address. This would prevent the central office from even logging the true source of activity.

Remote Session

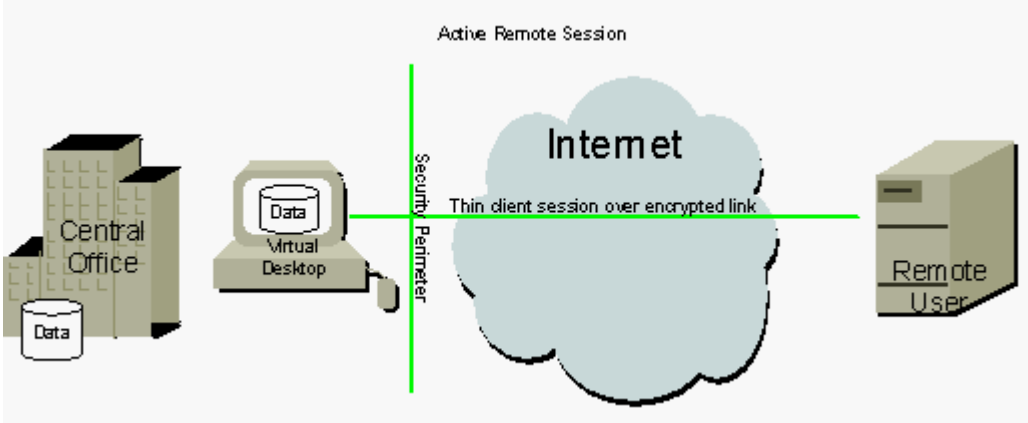

fig4

Yes, it is possible to correct all of the above mentioned flaws by adding addition layers of authentication and logging, but the object is to provide remote users access to the resources of a central office not to just to engineer a complex security system. An alternative to the remote node solution is the remote session, also referred to a thin-client solution. Remote session is a method of remotely controlling a virtual desktop behind the security perimeter without ever moving the actual data beyond the control of the central office *fig4*.

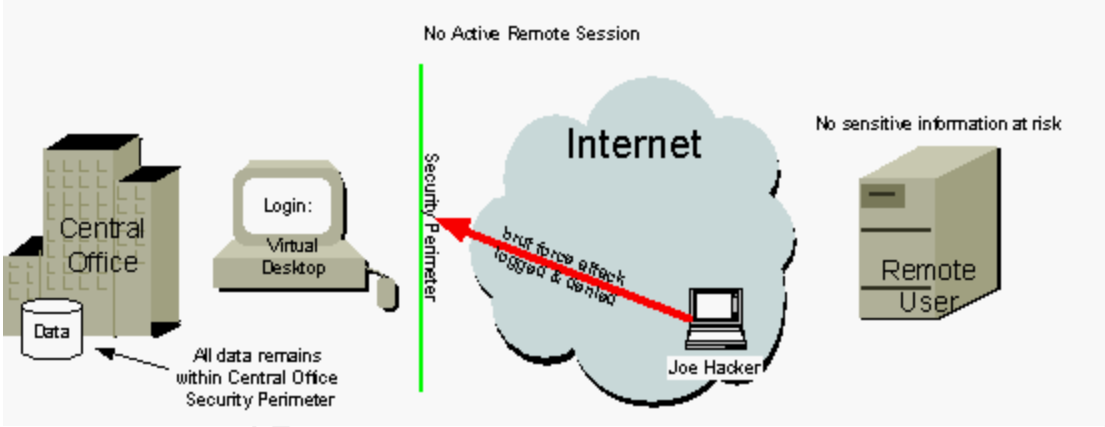

fig5

The beauty of this solution is that no data is stored on the remote computer. It is a trivial matter to prevent a remote user from copying data to their local drives or printing documents to a local printer. The only options left would be to use a screen capture program or take a photograph of the screen. The screen capture problem can be corrected by using a thin client device with no local storage or functionality beyond connecting to a remote session server. Taking a photograph of the screen moves far beyond a simple insecure process to a malicious act, and therefore should be prevented through user policies.

There are currently several products that could be used as the foundation for a remote session solution.

- Microsoft Terminal Server – uses the RDP protocol to display a Windows NT 4.0 or 2K session to the remote user. Provides no encryption of the session therefore would require the use of a VPN product. There have been several DOS attacks against RDP that could effect unpatched server. This should not be an issue since the Microsoft Terminal Server would be behind a VPN gateway so only authenticated users would have access to the RDP port.
- Citrix Metaframe – uses the ICA protocol to display a Windows NT 4.0 or 2K session to the remote user. The product includes Secure ICA, which provides 128 bit RC5 encryption of each session. Many vendors of thin-client devices with no local storage support the Secure ICA protocol. I can find no record of any DOS attacks or exploit that an unauthenticated entity could use to effect the Metaframe Server.
- AT&T Laboratories Cambridge, Virtual Network Computing – using VNC sessions would provide access to Unix and Windows based applications. VNC does not provide any encryption but can be tunneled in OpenSSH. While this is certainly not a turn key solution it could be very secure if properly managed.

Due to their single user per server limitations traditional remote control software like PCAnywhere are not suitable for deployment in a multi-user environment.

Using any of the remote session solutions mentioned would allow a travelling user to rest assured that relinquishing their laptop for hostile examination could compromise no data. A telecommuter, working out of their house, would have no concerns about letting a spouse or child use the computer. The remote computer is no longer a member of the central office trusted computer system, it is a portal with which a user with the proper credentials can view, create, modify, and delete information. When the connection to the central office broken the data stays safely at the central office. How safe the central office is, is another matter all together.

Sources

McAleer, Sean. "A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs" January 24, 2001
URL: http://www.sans.org/infosecFAQ/wireless/defense.htm (10 February 2001)

DEPARTMENT OF HEALTH AND HUMAN SERVICES
45 CFR Part 142 "Health Insurance Portability and Accountability Act of 1996"
http://aspe.hhs.gov/admnsimp/nprm/sec13.htm (20 February 2001)

Information System Security Organization (ISSO) "Controlled Access Protection Profile" 8 October 1999 URL:http://www.radium.ncsc.mil/tpep/library/protection_profiles/CAPP-1.d.pdf (15 February 2001)

DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985
URL:http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html (19 February 2001)

Counterpane Internet Security. “Crypto-Gram newsletter”
URL: http://www.counterpane.com/crypto-gram-9912.html#SecurityIsNotaProductItsaProcess (10 February 2001)

Netscape Communications Corp. "How Digital Certificates Work."
URL: http://home.netscape.com/security/techbriefs/certificates/howcerts.html?cp=stbmid (15 February 2001)

Citrix Corp. “SecureICA Option Pack.”
URL: http://www.citrix.com/support/solution/SOL00044.HTM (26 February 2001)

AT&T Laboratories Cambridge “Virtual Network Computing”
URL: http://www.uk.research.att.com/vnc/ (26 February 2001)