Volume 1 Issue 2

PLUS PAGES QUARTERLY

Concepts in Voice and Data Communications

In This Issue:

This quarterly newsletter is being provided by **Tel Tech Plus, Inc.** in our continuing effort to keep you better informed about our products and services and items that relate to or affect those products and services.

TEL TECH PLUS & THE NMCI PROJECT

GREG STEARNS, CHIEF OPERATING OFFICER

Since late 2000, Tel Tech Plus (TTP) has been engaged in the $6.9 billion Navy Marine Corp Intranet (NMCI) project that is building the world's largest private intranet. Initially TTP was asked by Rancho Santa Fe Technologies – Mission Critical Systems (RSFT-MCS) to install fifty voice and data drops at Naval Air Station North Island, but that scope of work quickly expanded to 500 drops and then to installing the copper and fiber infrastructure in the server farm and network operations center (NOC) located at North Island.

As the NMCI project gathered momentum in early 2001, TTP became involved in seven more server farms at Lemoore, China Lake, SPAWAR Point Loma, Port Hueneme, Point Mugu, Fallon, and Commerce Point. Additionally, TTP wired the entire Commerce Point campus, which included NMCI executive offices and a help desk.

Our high quality of work coupled with our responsiveness to requests helped us to get the attention of other NMCI partners and enabled us to move into other areas of the program. We provided outside plant engineering services to General Dynamics at Fallon, and also provided inside plant installation services at Point Mugu. Wam!Net contracted us to rack, stack, and patch the active components (e.g., Cisco switches and storage area network devices) of the base area network (BAN) and local area network (LAN) that are located in the server farms. Additionally, Wam!Net contracted us to provide inventory management and asset tagging services. RSFT-MCS engaged us in the intermediate distribution frame (IDF) roll-out west of the Mississippi in which we conducted site surveys and managed IDF cabinet installation at a variety of bases.

In early 2002, TTP installed the cable infrastructure in three more server farms in Hawaii including Ford Island, Camp Smith, and Kaneohe Bay. As we closeout 2002, we remain engaged in the IDF roll-out.

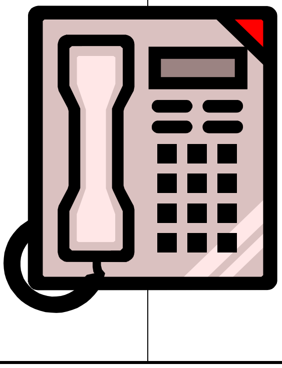
The quality of our work and the responsiveness to our customers on the NMCI project are the same standards we apply to our general market customers. You can rest assured that when Tel Tech Plus does a job for you, it will be done right the first time.

Tel Tech Plus, Inc. is licensed and bonded by the state of California (#00732562) and is a corporate member of BICSI® and the Better Business Bureau of the San Diego and Imperial Counties. The company is a certified installer for products made by such leading manufacturers as Vodavi, Siecor and Siemon and we support their manufacturer warranties.

Customer Support After Hours

Randy Quinn, Operations Manager

How do we deal with problems after hours? Our normal hours of operation are Monday through Friday 8:00am to 5:00pm with the exception of holidays of course. When you call during regular hours a live receptionist will answer calls then transfer your call to the customer service dispatcher. After hours your call is answered by our automated attendant then you can select our emergency mailbox and leave a message. When you leave a message, please include the name of your business, your name, address where the problem occurs, a good “call back” number, and the nature of the problem. When the technician calls you back (within 30 minutes) he will have an idea of what is happening and just in case you can’t be reached at your call back number he can determine if he needs to go to the job site.



What determines if a call is an emergency? We consider a call an emergency if you are unable to dial out or receive calls, a combination of both, 25% or more of your phones or lines are dead, or you are a business that operates well beyond normal working hours or days. If you have a problem that is less than that you can leave a message for us to service you the next available working day. We bring this up because there is a premium charge for after hours call outs, so it is better to wait until the next available working day if it is not an emergency.

To sum it up, anytime you call we will take care of your needs, whether it is an emergency, or not.

The Network Cable

Jim Stewart, RCDD

How important is that network cable I plug into my computer?

In today’s fast paced business environment, local area network (LAN) speed is critical when building a highly productive and successful company. It is no secret that corporate America, along with the United States military are constantly striving to improve the flow of information and the speed at which it arrives at its destination. This continuing technology advancement has become vital to our economy as well as the security of our country.

Whether your information is traveling across the room, or across the country, the pathway it travels has now become the most important element in constructing an efficient and effective network of communications. Billions of dollars are spent annually installing high performance cabling systems and building data centers to improve network speed, security, and the quantity of information that is transferred across a network.

Have you had your network connections tested lately? Those connections are the key elements to supporting fast and effective data transmissions. The copper cable that goes from your workstation to the communications room is often overlooked as the difference between having a workstation that is just functioning and a workstation that is highly productive.

Having the proper network cable installed on you LAN is the first step to laying the foundation for an efficient and effective network.

Better Return On Investment with Windows 2000 and XP

Phil Schlesinger, IT Manager

Every once in a while, I get the question: "Should I upgrade my Windows PC or server to Windows 2000 or XP?" Nine times out of ten, my answer will be "Yes.." Here's why:

1) Greater stability: Each newer version of Windows has proven to be far more stable than the previous versions. They crash less, and when a crash does occur, usually Windows can compartmentalize it so you can continue working without a problem. How many times have you heard a technician tell you to take two reboots and call back in the morning?
2) Better security: Windows 2000 and XP include better security features - they're harder to hack and they can be locked down more easily (to prevent the "tinkerers" from breaking their own PCs, which in turn costs you more money).
3) Use more equipment: As far as I am aware, no one is still developing drivers or software for Windows 3.1. Only the second version of Windows 95 (aka OSR2) supported USB, and even then, only a limited version of it so all of those neat USB drives, network adapters, and other gadgets cannot be used on those PCs.
4) Use more software: Because of the economic downturn and the dot com bust, software companies cannot afford to pay for the development and technical support of software that is compatible with both the older and newer versions of Windows - so they opt to support the newer versions only, leaving the rest out to dry. Perfect example: Microsoft Office 11 (to be released the middle of next year) will only be able to be used in Windows 2000 and XP.

Wireless Networking - The Right Way To Secure It

PHILIP H. SCHLESINGER, MCSE, CCNA INFORMATION TECHNOLOGY MANAGER

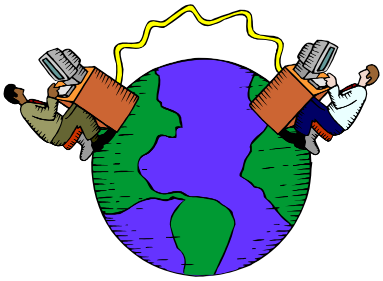
This is the second of many articles on company-wide computer security, explaining the threats to every company's computer systems and how to defend against them.

As you may be well aware, the technology is now available to wirelessly connect to your company network and the Internet at numerous locations: anywhere inside or outside your office or your home, at coffee shops, bookstores, delis, restaurants, hotels, airports, and convention centers.

What you might not be aware of is that by default, practically all wireless networking (WLAN) equipment comes out of the box with the security features disabled. If your company is running a WLAN for the benefit of your customers, you don't necessarily need to have a high level of WLAN security; however, if you are running a home or office WLAN, high WLAN security is a must. If you've read or heard about the recent World Wide War Driving (WWWD) event, the organizers of that event demonstrated that most people have deployed wireless networking without understanding what a WLAN is to a hacker: the equivalent of putting a network jack next to your front door with a big sign that says "PLEASE HACK ME".

Don't believe me? With some rather cheap equipment, it is easily possible to stand outside of some office buildings and be able to grab an address on some unknown company's network if that company has not implemented enough WLAN security. A big, bad hacker could then eavesdrop on data transmissions and steal valuable secrets, attack that company's computer systems, and launch attacks on computers outside of that company's network. The hacker could then walk away, and when the Feds came a-knockin', the company owner wouldn't have any explanation of what happened.

About 25-35% of installations the WWWD surveyed actually had turned on the main security feature offered with WLAN: Wired Equivalent Privacy, or "WEP" for short. WEP uses a mathematical cipher code (called a "key") to encrypt WLAN data transmissions over the air so nobody, theoretically, can eavesdrop on the data and steal it, modify it to cause damage, or even get access to a WEP-protected WLAN without knowing the exact WEP key.



WEP by itself, however, is a rather weak form of protection for two reasons:

a) WEP implementations usually involve "static WEP", or sharing an unchanging key across all of the members of a WLAN, so if one computer is compromised (as an example, a laptop is stolen), the WEP key needs to be changed for every computer on that WLAN.

b) b) The technical design of includes many flaws, such as an improper implementation of the RC4 algorithm, which makes it relatively easy to figure out the static WEP key no matter how long that key is. All it takes is that cheap hardware that I mentioned earlier and some readily available free software that's on the Internet. Sniff packets for about an hour or so while sitting in the parking lot or in the suite next to yours and a hacker can discern the static WEP key. Then, your company's network is theirs to be used as they please.

So if static WEP isn't the answer, how does one solve these problems? Simple: whenever considering a WLAN for your office or home, always require the following configuration from your computer staff and/or consultants:

1) RADIUS authentication (sometimes referred to as 802.1x): this means that before a computer is given access to a company WLAN, the logon credentials - a user name and password, a thumbprint, a smart card, etc. - are compared to a centralized database of users for authorization and access. RADIUS, in case you're wondering, stands for Remote Access Dial In User Service.

2) 2) Dynamic encryption, per session, per computer: instead of one shared key as with static WEP, use dynamic encryption on the WLAN to issue each authorized computer a unique, computer-specific WEP key. This key should be set to change every 15-20 minutes, keeping every computer's key unique in the process. The buzz word to look for is "TKIP", or Temporal Key Integrity Protocol as this will be the standard in 6 months.

3) 3) If you are away from your office and home and want to use a public WLAN - such as at a coffee bar, bookstore, restaurant, hotel, conference center, or airport - use Virtual Private Networking (VPN) and/or Secure HTTP (addresses starting with "https://" as opposed to "http://"). This will stop eavesdroppers at the locations from listening in on your sensitive information. For more information on VPN, you will soon be able to view a new IT Services section of our web site (http://www.teltechplus.com/ITServices.html

4) Install a software firewall on every WLAN connected computer. There are other attacks that hackers can do against WLAN's - a software firewall will stop the easier attacks and practically all of the more difficult ones.

Continued page 4

Wireless Networking,

Continued from page 3

5) By default, WLAN equipment broadcasts this information to alert WLAN equipment of its presence – it's the equivalent of a searchlight with a message "there is a WLAN here". A free program called NetStumbler, combined with a GPS unit, can permit hackers to scan areas while driving to make a map of future WLAN's to hit; with the SSID broadcasting, it makes it even easier to find your specific WLAN.
6) Most important of all, pay for a site survey of the location before implementing a WLAN to make sure all of the equipment will be optimally placed for maximum usage and minimum leakage to areas outside your office or home. In the process a technician can make sure that none of your employees have put in their own unprotected WLAN equipment when you weren't looking, thereby exposing your network to hacking. Then, have the site surveyed at least once every few months to verify and reaffirm your established protections.

My team of experts at Tel Tech Plus are fully trained and equipped in planning, installing, and maintaining all the components of computer infrastructure - desktops, laptops, & servers; wired & wireless networks; Internet firewalls & VPN; and comprehensive anti-virus protection. Please feel free to contact me by phone at 760-598-6233 x111 or by email at pschlesinger@teltechplus.com if you have any questions about your current or future configurations.

Better Return On Investment,

Conitnued from page 2

5) Microsoft has a policy that operating system software is supported for only five years, so if something goes wrong and the problem is related to a bug in Windows 3.1, 95, and soon 98, you're up a creek without a paddle.

All of this translates into more headaches and band-aid solutions to keep older systems running - and therefore more downtime and higher tech support bills.

Inside Future Issues:

IT Information

Phone Systems/
Voice Mail Updates

Company News

Wireless Information

Cabling Updates

Future Technology
Guides

Microsoft Patch Watch

Philip L. Schlesinger, IT Manager

Microsoft published twenty-one security bulletins during the period of September, October, and November 2002. Eleven were marked critical. The big winners? Microsoft Windows had ten, followed by Internet Explorer with 8. One of the patches is for a real doozy of software hole: unpatched, a computer with the hole can permit a hacker with the right computer code to take on your identity and, in some cases, gain control of your PC. Here's the catch: Microsoft released a patch in the beginning of September, and has since revised the patch three times because each previous version did not fix the problem completely. In simple English, we're up to version 4.0 for this patch, and I wouldn't be surprised if they need to fix it a few more times. So much for Microsoft's "trustworthy computing" initiative...

Software patching is one of the many tasks involved with the design, implementation, and maintenance of computer systems. While a good firewall can protect your company's network from hackers on the Internet, if your servers and workstations aren't patched and firewalled themselves, they are open to attacks from people within your company as well as from careless downloads of email-based viruses and Trojan horses. My IT team can keep your company's computers and network in tip-top shape and show you how to stop these types of attacks cold.

For more information, please feel free to give me a call at 760-598-6233 x111 or email me at pschlesinger@teltechplus.com.