Global Information Assurance Certification Paper

Robert L. Marchant
GSEC (St. Petersburg College, Fall 2001)
Version 1.4 (option 2, case study)

Introduction

I have 26 years of software and systems engineering experience. I am a Senior Principal Engineer at Raytheon Company where I am currently the Lead Systems Engineering (LSE) for Information Assurance for the Navy/Marine Corp Intranet (NMCI). I am an adjunct lecturer for St. Petersburg College, and a frequent speaker in our community schools and social clubs where I encourage our students to pursue careers in high tech fields. I chose to write about securing a home use Tiny Area Network (TAN) as a result of a visit from an old I friend who needed help securing her TAN. This paper is a case study about how I worked with her using the tools I learned in the Security Essentials Class to secure her home use network.

Abstract

Securing a Tiny Area Network (TAN) for home use is presented as a case study. The paper discusses the steps the author followed preparing for and working with the TAN users, starting with a site survey, through threat analysis, creating a simple security policy, to creation of a defense in depth strategy for mitigating the security risks.

The paper describes a scenario that can be used as a case study in a professional training environment. It encompasses in miniature most of the major steps an Information Assurance Professional should follow in securing a network, but without the handy checklists we are used to in the professional world. I had to perform site survey, define the threats, do a vulnerability assessment, define the risk, come up with a mitigation plan, implement the plan, and then train the users. Working through securing my friends TAN made me much more sensitive to the processes IA professionals use in creating secure network and network security policy, and perhaps better at describing these process to new employees.

The paper is easily converted to an interesting, and reasonably usable speech for civic and public education audiences. I have presented the material in less than 20 minutes. It can also serve as a road map for home users to follow in securing their TANs

Preparations

The "Users" are a family of five who will remain nameless. Mom is a secretary-bookkeeper at a local business, Dad is a very successful sales representative for an electronics part supply company, College Boy is an engineering junior at the University of South Florida who lives at home, High School Boy is a very gifted high school sophomore with an acute interest in computers, and Middle School Girl simply uses her computer to e-mail friends.

I was somewhat concerned about helping my friend because I did not want to provide a security solution that would require me to visit every week to fix a problem or explain how to work around a security feature. As a professional, I see repeatedly the resentment users have when first exposed to a secure environment. "Why can't I install my own software", is just one example of the many laments we have all endured. I certainly did not want to install a solution that would end a friendship. I have seen the results of too restrictive policies make a workable network too frustrating to endure, I did not want my friends to trash a secure network because of too many alerts or too many restrictions. Because of these concerns, prior to visiting the Users, I researched on the Internet to have URL answers available for what I guessed would be the Users questions, to have an idea of what products are available that are easy to install and maintain by the non-computer literate user, and to remind myself of what the threat is to the home user. Two articles I found to be very helpful are Windows 95/98 Computer Security Information[1] by the CERT® Coordination Center and Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters[2] by Jim Willert (from the Sans reading room).

Site Survey (Before)

The TAN contains three desktop computers and one laptop. Two of the desktop computers and the laptop are running Windows 98, Second Edition. One desktop was running Windows 95. All 3 desktops have phone modem (unconnected), CDs and floppy drives. All of the users can connect (manually) to a scanner and an external CD writer. The computers are connected through a D-Link DI-713P wireless broadband Router. Two of the Desktops connect directly to the Router via CAT5 cables, one desktop via a D-Link DWL-500 (PCI Wireless LAN board – this board is really a PCMCIA card model DWL-650 mounted in a PCI daughter board) and the laptop connect via DWL-650 wireless connection.

I interviewed all of the Users and then examined each computer to determine what how computers were being used and what applications might be used on them in the near future. The major applications per user are shown in the following table:

TABLE 1: Major applications and computer used per user.

Mom	Dad	College Boy	HS Boy	MS Girl
Laptop	Laptop	Windows 98 Desktop 1	Windows 98 Desktop 2	Windows 95 Desktop
Word		Word	Word	
Excel		Excel	Excel	
Publisher				
Quicken '99		Quicken '99		
Internet Explorer	Internet Explorer	Internet Explorer	Internet Explorer	Internet Explorer
Outlook	Outlook	Outlook	Outlook	Outlook

Express	Express	Express	Express	Express
		Netscape Communicator		
		Several engineering packages (e.g. Maple V, Pascal, TK	Games, Games, and more Games	
			Several Password protected ZIP files	

The wireless gateway was purchased to allow sharing of their Internet connection, which is provided by a very reliable and respectable local cable company. None of the users anticipated ever needing to use any file sharing capabilities and the only shared printer (an ink jet) was hosted off of the gateway. Their ISP allowed up to five e-mail accounts per customer, so each user has a unique e-mail address.

I used "The Twenty Most Critical Internet Security Vulnerabilities"[3] by the SANS Institute and the National Infrastructure Protection Center (NIPC) and the Cyber Security Test[4] by the National Cyber Security Alliance as references to create a quick security survey shown in Table 2. The results indicated a very typical non-secure environment.

Table 2: Home Use TAN security questionnaire.

Did you change any default security settings on your computers?	**No**
Do you know what a strong password is and do you use strong passwords?	**No, No**
Do you backup any data?	**Only Quicken**
Are your backups copied to an external device?	**No**
Do you use File Sharing?	**No**
Do you use Printer Sharing?	**No**
Do you use the internet to log into a remote computer?	**No**
Do you use any Virus Detection Software?	**No**
Do you use a firewall?	**Yes (on gateway)**
How often do you get e-mail from people or organizations you do not know?	**Daily**
When you receive e-mail from an unknown source, do you read it?	**No (4), Yes (1)**
Did you adjust any browser security settings? If so, How?	**No**

Threat Analysis
The most dangerous threat to home user is the attacker who wants to use someone else's computer to launch attacks on other computer systems, often against military (e.g. NMCI) government (e.g. the White House) or financial systems. Identity theft is perhaps the second most dangerous, and malicious destruction of the users computing environment third on the list. Areas of concern I identified are listed below, in order, from Internet in:

1. Password compromise (when accessing web sites without https, for example) could allow access to sensitive accounts. The users (all 5) used weak passwords and used the same passwords repeatedly (Mom, for example, used Dads name as her password). None of them ever changed any passwords.
2. Malicious content on web sites or malicious e-mail could compromise the content of the computers (e.g. personal information, use them as platforms to launch other attacks, or simply destroy the data on the computer.
3. Compromise of the wireless network with the same threat as in 2 above. (Mom installed the wireless router without changing defaults).
4. No malicious code detection or intrusion detection on any machines, again with the same threat as in 2 above.

My User family was amazed that anyone could or would ever consider using their computers to launch an attack (ignorance is bliss).

Defense in Depth (During)
There is no substitute for education, but I realized I could not provide enough training to make this family information security literate. The next best substitute I could provide would be an easy to follow security policy. I created the 10 security policies to live by list shown be lower as my inmost layer of defense.

10 Policies to live by:

1. Use strong passwords, change them frequently, and never use the same password for multiple applications. A good description of strong passwords is available at[6] http://www.microsoft.com/privacy/safeinternet/security/best_practices/passwords.htm/
2. Do not leave file sharing or printer sharing enabled. If you enable file or printer sharing, disconnect from the Internet first, disable before reconnecting to the Internet.

3. Turn your computer off, unless you're using it. Turn the gateway off if no one is using it.
4. Never open an e-mail from an unknown source.
5. Create backups of critical data, it is ok to network to a folder on another computer but be sure to comply with policy 2 above.
6. Low security settings are never to be used, Medium is ok for trusted environments, use High settings when exploring.
7. Update your security products weekly, run a full virus scan at least monthly.
8. Trust your content scanner. Never allow personal or financial data over an insecure connection. E.g. - if you don't see https, don't allow credit card numbers.
9. Check and know the security settings on all of your applications. When you upgrade an application (e.g. Office), double check the settings.
10. Stay out of the DMZ, do not open firewall ports without discussion, report all attacks to (ISP) security immediately.

On the computer

My first step to sit with Mom and do a little research on personal or family internet security (via yahoo, and yes, I had already done this research, but I wanted Mom to know how). During my after dinners discussion with the User family, I came to the realization that ease of use (e.g. settings like High, Medium, or Low for firewall protection) is a great deal more important, than knowing which port to block. I was looking for a package where the translation the User family would make for settings is low is bad, high is best but means a lot of warnings and extra step so I'll use it when I'm exploring, Medium is good when I trust where I'm going. Freedom Internet Privacy Suite, from Zero-Knowledge Systems (www.zeroknowledge.com), Norton Internet Security 2002, from Symantec (www.symantec.com), and McAfee Internet Guard Dog Pro, from McAfee (www.mcafee-at-home.com) all offered the ease of installation and use I wanted.

While Mom made a quick shopping trip looking for one the packages mentioned above, I started on the operating systems. For all Microsoft products I followed the guidance contained in "Using Microsoft Products Securely"[5] at URL:
http://www.microsoft.com/privacy/safeinternet/security/products/default.htm
Although Windows 98 2nd Edition is an insecure operating systems, it is reasonably stable and supports all of the applications the Users currently have. My second step in improving the defense in depth posture of the users was to upgrade the Windows 95 desktop to Windows 98, 2nd Edition so all computers on the TAN would be using the same software and so that I could upgrade the oldest machine to the more secure domestic encryption provided by IE rel. 6 (I did have to donate some excess RAM and a Windows 98 license from my personal stash). I also ensured that all operating systems updates had been posted to the other three machines.

I discussed Internet Explorer security settings and, after much debate with Mom and College Boy, assigned all browsers the default security setting of medium. This setting disables unsigned ActiveX and prompts for most ActiveX activity. Java, being somewhat more secure is allowed more access. Privacy settings were set to medium high to allow the family to decide what cookies will be allowed to use personal information.

I set Outlook Express to disable scripting by setting the security setting to restricted sites and then ensuring that scripting was set to off for restricted sites in the Internet Explorer security settings (custom setting for restricted zones).

Finally, I set Word and Excel security levels to High (Tools menu, Macro sub-menu, security).

Then we installed Symantec's Norton Internet Security (NIS) Family Edition 2001 on each machine (I had the primary user of each machine do the install). This wonderful package bundles all the security features the family needs into one reasonably priced package (Mom bought 4 copies at a local buyers warehouse for ~$60 each with $20 rebate on each copy). Included in the bundle a Personal Firewall, Privacy Control (a content scanner), Ad Blocking, Parental Control, Norton Rescue, and Norton AntiVirus (NAV).

As each member of the User Family (except Dad) was going to maintain their own version of NIS, I walked each through the tailoring of their system as I conducted the tailoring of Mom and Dad's machine. I did not allow any security settings below medium. In general the settings established are as indicated in the paragraphs below, which detail the settings on Mom and Dad's laptop.

NIS installs easily with clear help and clear guidance for the moderately computer literate home user. After slugging through the registration process, the first installation option to establish is for the personal firewall. Firewall settings are low, medium, and high. The low setting is essentially benign in terms of alerts and blocks most known hacker ports, it is essentially a routine (e.g. I visit these three trusted sites only) type of protection, for the User family who often visit sites they heard about from a friend (for example), I set the policy in place that low is bad. Medium increases the alert levels and blocks application Internet access until you permit it (you are notified of access request and allowed to temporarily or permanently enable or disable an applications access). The high setting is very restrictive and alerts on almost all activity. We originally set the level to high but Mom moved it to medium the very first time she used the computer. Medium is the recommended level.

During set-up, and as option anytime after set-up, NIS scans for Internet enabled applications. A list of specific applications permissions is available and settable. You can, for example permanently block any application, require the application to ask permission, or permanently enable. The rule set for the firewall is also settable but this

rule-set may be beyond the average user. The firewall also has an expert level control for Trojan horse settings.

Privacy control allows cookie management similar to Internet Explorer, the medium setting on NIS most closely matched our setting for IE. Privacy control also provides a content scanner. The content scanner implementation assists the user in the creation of specific data to be questioned when contained in an http transaction. The implementation in NIS leads the user to input primarily financial data but in reality will accept any character string. Content scanning on NIS does not scan https transactions.

Ad blocking, when enabled, allows the user to select a pop-up ad and "trash-it". A page, once selected, will be permanently blocked (after installing and seeing this feature on Mom's computer, I bought NIS for my system at home).

Parental controls allow setting the specific sites a user (child) can access or identifies specific sites to block (or both). Parental controls can also specify which applications a user can access. We did not select parental control on any of the User family computers.

NAV provides all inclusive virus protection (from floppy to e-mail). NIS provides one year of live updates for all NIS products (renewable annually for a moderate fee). NAV includes a scheduler that can schedule NAV scans, live updates, messages, or execution of any application. We enabled NAV, scheduled a monthly full computer scan, a weekly live update, and ran a full scan on the computer as the final step of our installation. To my amazement, only one virus was found, on all three machines (Stealth).

Our final step was to run Norton Rescue to create a set of Rescue disks. This utility dumps the operating system to floppy in a bootable form that will in most cases allow restoration of a trashed system. Somewhat more thorough than the one floppy Microsoft emergency disk, the Rescue dump on Mom's computer used 7 floppies. Rescue can also be used on zip disks.

Router

The D-Link router (DI-713P) is based on IEEE 802.11b, an inherent insecure router. The Sans reading room is full of articles on the inadequacies of 802.11b. In my opinion though, for home use, it is good enough. The Users (as I also do) live in a gated community where we know our neighbors, we know when strangers come through our neighborhood, and we know the best defense to a drive by hacker tapping a wireless network is a quick call to security and a well armed baseball bat. I did take the time to show all 5 users how to check the router, and how to tell who is using it.

The User household uses X10 home automation products (www.x10.com). Under protest from High School Boy, I had Dad hook up an X10 module to the Router and to the cable modem (High School Boy told me emphatically that the cable installer reassured him that the modem never needed to be turned off). Each computer already

had an X10 attachment (call a firecracker) that could control all X10 modules throughout the house. I showed all the Users how to use winipcfg.exe to query and reset their IP address and set the policy in place to shut off the modem and router when not in use.

The DI-713P has 4 rj45 connections, a serial port, and a parallel port. One rj45 was for the cable modem connection, two others connected two of the desktops. The parallel port is for a printer (and had a printer connected). The device is configured via a web interface at default address 192.168.0.1. Clients are assigned addresses in the 192.168 range. I left this default alone but had Mom restrict the total number of concurrent connected IP addresses to 4 by assigned the limit of address ranges to 192.168.0.100 – 192.168.0.103. The router allows MAC reservation and association (i.e. assign a specific MAC to a specific port), I showed Mom how to identify the MAC and we associated each computer to a specific port.

Mom (the original installer) never changed the default configuration admin login id of "admin", I had her set a new "strong" password and then stuck it on the monitors of all the desktops (I had to discuss with her that this password is ok to give to anyone in the house, just keep it in the house). I was pleased to discover that Mom had set a strong name as a wireless network id and had enabled 128 bit encryption. If she had not done this, we would have had to reset both wireless clients settings. The router has the ability to allow a remote admin host (via a specific IP address), has a DMZ (used by placing a specific client in the DMZ), and can allow special FTP service, all three of these features were disabled, and stayed that way.

The router also has a built in firewall. Mom never modified the defaults, and after a quick review, I saw no reason to change it (this firewall may have helped keep the infections level low).

ISP Selection

We have several options in our area for high-speed Internet access for home users. Fortunately, the Users were connected through the Cable provider I trust most in our area. I have met the Security Manager for the ISP and have been a user of this ISP for almost three years. The security provided by this ISP is outstanding. The Users don't know and probably wouldn't care about the details of intrusion detection, information assurance, firewalls, content scanners, or DOS attacks. I felt it important however, that all five of them know if and when they are or were attacked. With that in mind, I took the extra time to show them how to enable and understand the log created by their D-Link Router and how to create and monitor Internet activity status tracked by NIS. I then posted the phone number and e-mail address of the ISP security manager on the cable modem for them to use if anything suspicious did happen (in the 4 months since I worked with the family, they have never been attacked in a way that was detected by the router or by NIS, an outstanding compliment to the ISP).

Conclusions (After)
Not counting a most leisurely evening of research, this entire project took one night after dinner and a Saturday, but the process worked. I am confident the User's compute environment is as secure as can be expected for a non-computer professional home. Understanding the environment, the users, the threat, and the solutions available to mitigate the threat allowed me to create a security architecture for this family that they understand and can maintain, and (albeit primitive) a security policy that they can live with.

A quick recap of what I accomplished:

1. Provided brief security awareness to acquaint the Users with the threat.
2. Provided a 10 point security policy intended to address the specific needs of the Users.
3. Provided 3 layers of security for the Users, specifically I: improved (as well as possible on Windows 98) the operating systems and applications (IE, Outlook Express, Word, Excel) security settings. Helped install Norton Internet Security, Family Addition. Improved the security settings of the User D-Link Broadband Router.
4. Made the users aware of the value and importance of selecting the "right" ISP.

In the four months that passed since I worked with the users, we have only made one change to the architecture (well, only one they had to call me about), we used a feature of the D-Link router to open up the firewall for High School Boy to allow him to play Internet games with his friends. I don't have the details of how this change was made, to their credit, all I had to do was describe to them were to look for directions in the D-Link users manual. I guess my fears about having to visit weekly to fix security problems were unfounded!

1. Carnegie Mellon, Software Engineering Institute, CERT® Coordination Center. "Windows 95/98 Computer Security Information". URL: http://www.cert.org/tech_tips/win-95-info.html/

2. Willert, Jim. "Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters". October 22, 2001. URL: http://rr.sans.org/homeoffice/best_practices.php/ (access will require the reader to register)

3. SANS Institute and the National Infrastructure Protection Center (NIPC). "The Twenty Most Critical Internet Security Vulnerabilities". October 1, 2001. URL: http://www.sans.org/top20.htm/

4. National Cyber Security Alliance. “Cyber Security Test” . URL: http://www.staysafeonline.info/selftest.adp/

5. Microsoft “Using Microsoft Products Securely”. URL: http://www.microsoft.com/privacy/safeinternet/security/products/default.htm

6. Microsoft. “Security Best Practices Checklist, Strong Passwords”. URL: http://www.microsoft.com/privacy/safeinternet/security/best_practices/passwords.htm

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event