Volume 12, Issue 3

May 2011

The Computer Club At Willow Valley

Inside this issue:

The President's Pen by Sid Paskowitz

Membership Your Computer Club has 489 members at this writing, including 144 lifetime members.

Thank You! First, I want to thank Gert Skelly for her outstanding work as Secretary of the Computer Club and I want to welcome Joan Burks, our new Club Secretary.

No More Paper Newsletters This Newsletter is the last Newsletter published in paper form. If you get a paper copy of this Newsletter, you need to let Dick Dressel know your email address so you won't miss out on getting future Newsletters.

Monitors Monitors, we need monitors—both kinds! We have computer towers that Ed Dahrsnin and his recycling team cannot use in assembling computer systems for Club members or donation to Lampeter-Strasburg School District because we don't have computer monitors to go with them. If you have a working monitor that is sitting in a closet or cage, please drop it off in the Manor North Computer Room Monday-Friday at 1:00 p.m. so Ed and his team can put it to good use.

There was no Computer Room monitor to open a Computer Room and

(Continued on page 2)

Election day, May 17, is coming. Have you ever thought about using the eSlate electronic voting machine? It is convenient, easy and quick. To learn how to use, visit Information Central or type the following on the address line of you browser and take an interactive tour: http://www.hartintercivic.com/files/eSlate.swf

Gene Simasek, Judge of Elections

Current Computer Security Issues by Al Williams

Cyberwarfare According to Reuters, as reported in zeenews.com on April 14, 2011, China is accelerating its attacks on US government agencies with 41,776 attacks reported in 2010. These attacks, known as Byzantine Hades by US personnel, focused on government secrets at a variety of agencies. This number does not include attacks on companies. In the past two years dozens of companies in the technology, oil, and financial sectors reported attacks. Many attacks are seeking proprietary information.

The attackers also collect information about senior personnel in the companies being attacked and then send detailed emails to individuals. This technique, known as spear-phishing, frequently persuades the individuals that the email is genuine. After clicking on a link, keystroke logger and command and control programs are downloaded onto the individual's computer which then enables theft of sensitive information.

(Continued on page 3)

Coming Programs

May, 2011-NorthAuditorium
Bob Davis, IT Manager
Willow Valley Networks

June, 2011
Ron Dillon, Resident
TV at Willow Valley

September, 2011
Gene Simasek, Resident
Lakes Wireless Setup

All programs are held in the Education Room at the Cultural Center on the 1st Thursday of the month at 2:00 p.m. unless otherwise noted.

President

(Continued from page 1)

make it available for other Residents a number of days in April. Any Computer Club member with basic computer skills who is willing to spend a couple of hours each month as a Computer Room Monitor is requested to contact Dick Dressel at 464-6508 for the North Computer Room (M-107) or Gene Simasek at 464-4605 for the Lakes Computer Room (E-308). Let Dick or Gene know if you would like training to help you feel more comfortable as a Computer Room Monitor.

Email Hoaxes About once a month I get an email from a Club member warning of the dire consequences if I did or did not do something on my computer. Add www.snopes.com to your Favorites and use that site to check out warnings before you pass them on to others. Hoax emails rely on unsuspecting individuals to perpetuate the hoax and unnecessarily frighten people and waste their time. Help stop the hoaxes by personally checking them out on reliable sources such as Snopes, and rather than spreading the hoax, notify those who send such emails so they can check them out themselves before upsetting you and wasting your time.

I previously was notified by a Resident that they had received an official-looking email from a well-known company that their account would be terminated if the Resident did not respond immediately and update their account. The response required the Resident to enter their account information, password and other personal and financial information. Legitimate companies don't do that!!! Don't be duped by a letter or email, no matter how official it looks. Contact the customer service phone number on your statement to verify any action you need to take. Chances are, they will tell you they did not send anything like that. However, just to be on the even safer side, get the name of the customer service representative who provided you with that information and file that name and the time and date of your call with your statements.

Library Holdings Information Central now has a link to the list of holdings in the Manor Library as well as author and title sequenced combined listings for the Meadow Ridge, Spring Run, Lakes Manor and Manor Libraries. If a document is not available in your own library, you can easily find if it might be in another Community library.

Vagrant Hard Drive We are missing an external USB hard drive in the North Computer Room. If anyone knows its whereabouts or has it, please let us know or return it to the Computer Room.

Yahoo I have used Yahoo Classic email for a number of years and rejected a number of newer versions Yahoo has proposed. I find the new Beta version of Yahoo email to be quite acceptable and have no complaints about using it. I would be interested in knowing if any Club members have found problems with it.

Looking Good In Print This column has taken me longer to write than usual because I am finding a need to change my writing style based on Tony Poulos' excellent presentation at the last Computer Club meeting. I hope I have eliminated all the double spaces at the end of my sentences. •

Current Computer Security Issues

(Continued from page 1)

The Chinese, to stymie any counter efforts by the US, are deploying a hardened operating system known as Kylin that replaces versions of Windows, according to the Washington Times, May 12, 2009 in an article titled "*China blocks U.S. from cyber warfare*."

Spamming The contents of an email address and user name database owned by Epsilon, a major provider of email marketing services for many well known companies, was stolen. According to SecurityWeek.com, April 2, 2011, in an article titled "*Massive Breach at Epsilon Compromises Customer Lists of Major Brands,"* Epsilon has over 2,500 clients and sends over 40 billion emails annually. Epsilon reported that only a small percentage, about 2%, of their database was stolen. It is expected that the stolen information will be used for spear-phishing, a technique known to be more effective than typical spamming. Companies known to have their information stolen include: 1-800-Flowers, AbeBooks, Air Miles, Ameriprise Financial, Beachbody, bebe Stores, Best Buy, Brookstone, Capital One, Citi, City Market, Dillons, Disney Destinations, Eddie Bauer, Eileen Fisher, Ethan Allen, Fred Meyer, Fry's, Hilton Honors Program, Home Shopping Network, JPMorgan Chase, King Soopers, Kroger, Lacoste, LLBean Visa Card, Marriott Rewards, McKinsey and Company, MoneyGram, New York and Company, QFC, Ralphs, Red Roof Inn, Ritz-Carlton Rewards, Robert Half, Scottrade, Smith Brands, Target, TD Ameritrade, and others.

Secure Logins In March, 2011, hackers stole a sensitive database from RSA, a major company providing secure login hardware for many US government agencies and companies. RSA has not identified the specific information stolen. The RSA system supports secure logins as follows: The user logs in with their user name, a PIN, and the currently displayed numbers on the RSA security device. This system implements "what-you-know" authentication, the user's name and PIN, and "what-you-have" authentication, the RSA security device. Many agencies and companies are concerned since the lack of information from RSA makes it difficult for them to determine the degree to which their log in security process has been degraded. For more information, see PC World's undated online article, titled "*After RSA Breach, Are SecurID Tokens in Jeopardy?*" For more information about authentication, see the article "*Is He Who He Says He Is?*" below. •

Is He Who He Says He Is? by Al Williams

What We Want To Do We all want to be able to talk privately, when we wish, without being overheard. For example, Bob wants to talk privately with Alice, who also wants to talk privately with him, but Mallory wants to listen to their conversation. Even worse, on the Internet Mallory may be able to pretend to be Bob without Alice knowing that she is talking with Mallory instead.

Bob's and Alice's simple need to have private conversations and to know without a doubt that they are talking with the person that they intended is also our need. This isn't hard to do when we are talking face to face and can be cautious, but it is harder when we can't see the other person. It can be hard to do even when using the phone. Have you ever spoken with someone who sounds like another person you know? It is possible to have completely private conversations on the Internet but hackers continually work to listen in using an inherent problem in the Internet.

Why Do We Have This Problem? At the heart of the problem is what we use to communicate over the Internet. We communicate using protocols, mutually accepted conventions defining the details of how

(Continued on page 5)

The Equipment Corner by Ed Dahrsnin

Refurbished Systems The following refurbished system is available:

#231: Compaq PD1010, desktop, Windows 98SE, 350 MHz Intel Pentium II, 6.09 GB Free Space, 64 MB RAM, No printer

#233: Gateway ATXSTF1 Select 1200, tower, Windows XP Home SP3, 1.20 Gigahertz AMD Athlon, 15.71 GB Free Space, 480 MB RAM, Lexmark Z43 Printer

#234: Dell 4550, tower, Windows XP Home SP3, 2.00 GHz Intel Pentium 4, 7.93 GB Free Space, 768 MB RAM, HP Photosmart C4480 printer

The systems are free to any club member. You must pick them up. Contact Ed at 464 6591.

Miscellaneous We have 3 volt CR2023 batteries (suitable for motherboards to keep the system clock running) and a variety of CD-ROM's, floppy disk drives, keyboards, 2-button mice, various power supplies, and assorted cables. Please contact Ed Dahrsnin at 464-6591.

Donations We are once again accepting the donation of used, *working*, tower and laptop computers (with power units and batteries) from club members along with all software CDs. You may deliver them to the North's Computer Resource room on the first floor of M building after 1 pm on Monday through Friday. No Macs or Mac parts, see Lee Wermuth or Bob Handler for additional information. •

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Club, contact Sid Paskowitz at 464-2127 or wvrccc@Yahoo.com

The Leadership

Officers

President: Sid Paskowitz

Vice President: Dan Drummond

Secretary: Joan Burks

Treasurer: Dick Dressel

Community Representatives

Manor: Robert Kemp

Lakes: Gene Simasek

Committee Chairpersons

Program: Dan Drummond

Training: Bob McRobbie

Equipment: Ed Dahrsnin

Technical Support: Larry Gallagher

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group: Lee Wermuth

Computer Room Coordinators: Dick Dressel, Gene Simasek

Microsoft Liaison: Ed Dahrsnin

Past Presidents

Larry Gallagher

Is He Who He Says He Is?

(Continued from page 3)

we communicate. The details are intricate but fortunately we don't need to know the details or the protocols to use our computers. But, it is helpful to know the current version has shortcomings and that our private communications could be overheard unless we take steps to protect ourselves.

A Statement Of The Problem Currently, we are using Internet Protocol version 4, which is known as IPv4. This version lacks an Identity capability. This sounds vague but is clearly explained by Kim Cameron, Microsoft's Identity and Access Architect. Here is the Problem Statement from his May 2005 article on "The Laws of Identity," which may be found at social.msdn.com.

"The Internet was built without a way to know who or what you are connected to.

"Since this essential capability is missing, everyone offering an Internet service has had to come up with a workaround. It is fair to say that today's Internet, absent a native identity layer, is based on a patchwork of identity one-offs. [*Editor: A one-off is a solution to a problem that is customized for one application. It is not a general solution.]*

"As the web increases, so does users' exposure to these workarounds. Though no one is to blame, the result is pernicious. Hundreds of millions of people have been trained to accept anything any site wants to throw at them as being the 'normal way' to conduct business online. They've been taught to type their names, secret passwords, and personal identifying information into almost any input form that appears on their screen.

"There's no consistent and comprehensible framework allowing them to evaluate the authenticity of the sites they visit, and they don't have a reliable way of knowing when they're disclosing private information to illegitimate parties, i.e., like phishing exploits. At the same time, they lack a framework for controlling or even remembering the many different aspects of their digital existence.

"People have begun to use the Internet to manage and exchange things of progressively greater real-world value. This has not gone unnoticed by a criminal fringe that understands the ad hoc and vulnerable nature of the identity patchwork and how to subvert it. These criminal forces have increasingly professionalized and organized themselves internationally.

"Individual consumers are tricked into releasing banking and other information through phishing schemes that take advantage of their inability to tell who they're dealing with. They are also induced to inadvertently install spyware, which then resides on their computers and harvests information in long-term pharming attacks. Other schemes successfully target corporate, government, and educational databases with vast identity holdings and succeed in stealing hundreds of thousands of identities in a single blow. Criminal organizations exist to acquire these identities and resell them to a new breed of innovators expert in using them to steal as much as possible in the shortest amount of time. The international character of these networks makes them increasingly difficult to penetrate and dismantle.

"Phishing and pharming are now thought to be one of the fastest growing segments of the computer industry, if you can call it that, with an annual compound growth rate of 1,000 percent. ("For example, the Anti-Phishing Working Group Phishing Activity Trends Report of February 2005 cites an annual monthly gross rate in phishing sites between July through February of 26 percent per month, which represents a compound annual growth rate of 1,600 percent.) Without a significant change in how we do things, this trend will continue.

"It is essential to look beyond the current situation and understand that, if the current dynamics continue unchecked, we are headed toward a deep

(Continued on page 6)

Is He Who He Says He Is?

(Continued from page 5)

crisis. The ad hoc nature of Internet identity cannot withstand the growing assault of professionalized attackers.

"A deepening public crisis of this sort would mean the Internet would begin to lose credibility and acceptance for economic transactions when it should be gaining that acceptance. But in addition to the danger of slipping backwards, we need to understand the costs of not going forward. The absence of an identity layer is one of the key factors limiting further settlement of cyberspace. Further, the absence of a unifying and rational identity fabric will prevent us from reaping the benefits of web services. Web services have been designed to let us build robust, flexible, distributed systems that can deliver important new capabilities and evolve in response to their environment. Such living services need to be loosely coupled and organic, breaking from the paradigm of rigid premeditation and hard wiring. But as long as digital identity remains a patchwork of ad hoc one-offs that must still be hard wired, all the negotiation and composability we have achieved in other aspects of web services will enable nothing new. Knowing who is connected with what is a must for the next generation of cyber services to break out of the starting gate."

For us, what Cameron says in his Problem Statement is essentially what we already have heard through the news and experienced as computer users. Although he goes on to propose solutions for the future in his article, we are in the position of needing to go from the problem to an understanding of what is currently being done by the web sites that we use, our ISPs, and any other Internet communication that we use. That's because as computer users, we must use what exists now while he and others work to bring better solutions.

Identity and Authentication Many who work in this field address the problem of identity, the fact of being a specific person, by addressing the issue of authentication. Here, authentication is used in the sense of proving yourself to be a specific person. That is, it is used in the sense of proving that you are who you say you are. From the perspective of the person or web site that is communicating with you, their question is: is he who he says he is?

What-You-Know We're all familiar with using a username and password to log in to get access to our email or a web site. This process has a technical name: what-you-know authentication. That is, you prove that you are who you say you are because you know the username and the password.

What-You-Have There is a problem, however. Usernames and passwords can be stolen, or given to others for them to use. For that reason, another form of authentication exists: what-you-have authentication. The idea is that you can't give away what-you-have if you want to continue to log in. Although we may have little or no experience with what-you-have authentication using our computers, we do encounter this type of authentication in our lives: We need to present a photo ID when checking in for our first appointment with a doctor. We need to use our ATM or debit card when getting cash from an ATM machine. The photo ID and ATM card are things that we have. They have been given to us by someone who has decided that we are who we say we are.

Multi-factor Authentication To have a stronger confidence that you are who you say you are, the what-you-know and what-you-have authentications can be used at the same time. When you use your ATM card, you are also asked for a PIN. You are providing the answers to two authentications. This is called two-factor authentication.

You may have worked for a company or agency that used a SecurID. This is a small hardware device that displays a new number every minute. When you logged into your company's, or agency's,

(Continued on page 7)

Is He Who He Says He Is?

(Continued from page 6)

network, you provided your username, password, and the number displayed on the SecurID. A server on the network recognized your username and password and knew what number was being displayed on your SecurID. If you entered that number, the server knew that you were logging in. Since the SecurID never displays a number twice this guaranteed that you had the SecurID in your possession. This is two-factor authentication.

Discover card offers one time credit card numbers for online shopping. Usage is similar to SecurID. At the time of check out, you enter a credit card number provided at checkout by Discover. The number is never used again which means that if anyone were to capture the credit card number at time of checkout that they could not use it later. The combination of your login information at that retailer and the one time credit card number is another example of two-factor authentication.

What-You-Are If someone stole your username, password, and the device providing what-you-have authentication, then anyone could pretend to be you. This led to the development of another type of authentication: what-you-are. In this type of authentication, something about your body that is unique to you is measured and used. For example, a fingerprint, or a scan of the retina of one of your eyes could be used.

You may have already encountered this type of authentication. There are laptops that will not start until an authenticated finger is placed on a scanner on the laptop. You've seen in movies secure rooms which can be entered only after a registered retina of an eye is scanned.

A problem is that fingerprints change as a person cuts his finger or a chemical changes the ridges on the finger. It is also possible to create molds of a fingerprint and successfully use them on a scanner. Another problem is that equipment to read the pattern of a retina is relatively expensive and bulky to use. The third type of authentication can fail.

Who-You-Know There is a fourth type of authentication: who-you-know. Referrals illustrate this type of authentication. In a referral, an individual vouches for your character and experience. If several individuals say essentially the same thing about you as you did about yourself, then there is increased confidence that you are who you say you are.

An example of this type of authentication is when a person is trying to log into a network requiring two-factors for authentication: what-you-know and what-you-have. They remember their username and password but they forgot the hardware device (such as a SecurID). They log in using what-you-know, username and password, and then ask the network for a token (a blob of alpha and numeric characters). They then ask someone else at work to help them log in. The second person logs in using their own username, password, and the number displayed on their secure hardware device. They then tell the network that they want to authenticate another person. They provide the token given to the person who forgot their secure hardware device. They state that they know the person who forgot their secure hardware device. In return, another token is provided to the second person who gives that information to the first person. The first person then can log in with their username, password, and the just provided token. This sounds very complicated, but it if you think through the steps it is straightforward.

In this type of authentication, there is a heavy reliance that the second person does indeed know the first. Obviously, it is possible that the first person is not who they say they are but it is not likely.

Where-You-Are The fifth type of authentication is where-you-are. This type of authentication relies on the fact that you probably will be in the same area of the country most of the time. If someone logs

(Continued on page 8)

Is He Who He Says He Is?

(Continued from page 7)

into an account of yours from another area of the country, it may not be you.

Facebook does this now. If you log into your facebook account from an area of the country that is away from home, facebook will send an email to you asking if you logged in and if you didn't recommending that you change your password.

Alternate Factor Names There are alternate names used for these authentication factors that you may see elsewhere: something-you-know, something-you-have, something-you-are, someone-you-know, and somewhere-you-are.

Putting Them Together Using these authentication techniques, it is possible to have a high degree of confidence that you are who you say you are when logging into an account. The more authentication techniques that are used, the higher the degree of confidence that you are who you say you are.

Authentication Systems As you know, what-you-know authentication is popular. You frequently log in with a username and password. There are systems on the web that pull these authentication techniques together to implement an identity system. Two prominent systems are OpenID and Microsoft's Cardspace, which is similar to OpenID. Unfortunately, both need a fair amount of knowledge about authentication to use them successfully. I plan to write about these in a future newsletter.

If you decide to use such a system, please be aware that there also is a need for the same care as there is when using a secure web site. First, look at the URL for the web site and verify that you are connected to the correct web site. Second, verify that https:// shows in the URL and that a padlock symbol shows at the bottom of your web browser or, if using Firefox 4, look at the site identity button next to the URL. Finally, and very importantly, use the padlock or the site identity button to view the web site's security certificate. Once you are satisfied that the certificate is valid, then proceed with usage of the web site. I'll write about security certificates in a future newsletter.

Identification, Not Trust It is important to note that these authentication techniques help to identity a person as being who they say they are. The techniques do not help to determine if a person is worthy of trust. For example, a murderer can be identified with certainty by many people but few would trust him.

Intent Of This Article The terms authentication and two-factor are beginning to appear in newspapers such as the Washington Post. The intent of this article is to familiarize you with the concepts of authentication and techniques for authentication, including associated problems. As time goes on, it is likely that all of us will be encountering and using two-factor or multi-factor techniques.

Learning More If you would like to learn more, the recommended readings are:

- Steve Gibson and Leo LaPorte, Episode #90, "Multifactor Authentication," May 3, 2007, www.grc.com/securitynow
- Steve Gibson and Leo LaPorte, Episode #94, "The Fourth Factor," May 31, 2007, www.grc.com/securitynow
- Steve Gibson and Leo LaPorte, Episode #95, "OpenID," June 2, 2007, www.grc.com/securitynow
- Steve Gibson and Leo LaPorte, Episode #98, "Internet Identity Metasystems," June 28, 2007, www.grc.com/securitynow
- Steve Gibson and Leo LaPorte, Episode #111, "OpenID Precautions," September 27, 2007, www.grc.com/securitynow
- Steve Gibson and Leo LaPorte, Episode #113, "Roaming Authentication," October 11, 2007, www.grc.com/securitynow •

Reviewer Acknowledgment

The following individuals kindly reviewed this issue:

Domenick Buttiglieri

Sid Paskowitz

Thank you,

Al Williams

Interested in reviewing the Computer Club newsletter before it goes to press, or providing advice about the content? Please contact:

Al Williams at atwms@comcast.net

Key Willow Valley Web Sites

These are URL links to key Willow Valley web sites. Please copy the URL to your browser's URL space, open the site, and then add them to Favorites/Bookmarks or create desktop icons.

Information Central: http://eventregistration.willowvalley.org/kiosk/cclub/index.aspx

Kiosk Home Page: http://eventregistration.willowvalley.org/kiosk/default.aspx

Resident Phone Directory: http://eventregistration.willowvalley.org/kiosk/cris%20files/phonesearch.aspx

Service Request: http://eventregistration.willowvalley.org/kiosk/ServiceRequest.aspx

Computer Club Newsletter: http://eventregistration.willowvalley.org/kiosk/cclub/p/Newsletter.pdf