Implementation of Efficient Two-Factor Authentication for University Computer Systems

Gordon W. Romney and Paul D. Juneau

National University, 3678 Aero Court, San Diego, CA 92123, U.S.A.

ABSTRACT

The implementation of an efficient two-factor authentication process for users to gain access to university computer systems was developed by students in an undergraduate Information Technology (IT) security course. Many universities use the less-reliable, single-factor authentication of a process ambiguously referred to as NetID for faculty, staff, students and alumni. Although referred to as NetID, the process and technology may vary widely across universities. Witnessing the inadequacy of NetID to provide a secure university infrastructure, students were challenged to develop an improved, more secure authentication protocol. They based their solution upon an SSL secure web-site that also required a client browser certificate. This process combined the standard ID-Password of the web site (first factor) with a less-known feature of SSL, a client browser certificate (second factor) unique for each user. To make it not only secure but efficient the students cleverly stored the second factor component in a secure, portable container on a USB flash drive that makes it usable on computers in class and out of class.

Key Words: authentication, multi-factor authentication, SSL, digital certificate, browser certificate, portable certificate, and Agile Problem Driven Teaching

1. INTRODUCTION

1.1 User Authentication

Authentication, in an IT security context, has to do with authenticating the identity of a computer user. In order for authentication to be possible, a user must first be registered, or enrolled, as a valid subscriber on a specific computer system. This process normally produces a couplet of a "username" plus a "password/number." Examples are registering for a) social security number, b) library, or c) university or employment access privilege. Enrollment processes vary in quality and thoroughness and only security policy as specified by the controlling organization can determine true identity verification for a specific user. It is not the purpose of this paper to address identity validation or prove "I am who I say I am."

1.2 Authentication Factors

Features of authentication are referred to as "factors". Authentication normally consists of linking a "username" with one or more factors. The security authentication factors frequently referenced are (Smith, 2002):

Things you know … such as a PIN number or password
Things you have … such as a smartcard or digital certificate
Things you are … such as a biometric personal attribute: fingerprint, or iris image

One-factor authentication employs one of the factors, and, most frequently, is something that you know, such as a password. Two-factor authentication is a combination of two of the factors, such as a password and a digital certificate. As the number of factors employed increases, so does the security confidence increase. Hence, three-factor authentication is considered the most robust form of authentication. In a like manner, the implementation complexity and cost associated with the authentication increases as the number of factors employed increases.

1.3 The Need for More Than One-Factor Authentication

The Information Age challenge, to every person (persona), is that most enrollment processes, irrespective of whether they are online or in ink, a) are assumed to be adequate for authentication purposes because they assign some number or password (secret or not), b) are not secure because they are a default ONE-factor authentication, c) do not validate the identity of the persona, d) are easily compromised or hacked because they are the weakest, and e) facilitate identity theft

Normal username + password authentication can be compromised for a multitude of reasons; and, because it is the easiest and cheapest to implement, continues to be used by the majority of university and industry web-based Internet systems. This couplet is something that the persona knows and, consequently, can be hacked by brute force or by "man-in-the-middle" attacks. The username structure in practice is a combination of last name and first name and sometimes numeric additions. Usernames are frequently publicly known or can be determined through social engineering analysis where an attacker obtains information by non-technical means. Universities, also, are notorious for providing insecure wireless environments subject to hacking (Romney, 2008). Given multiple tries, hackers have readily available software that will allow them to crack most passwords because humans, for recall purposes, like to use words that occur in human language dictionaries. "When an attacker gets hold of a legitimate username and password, he won't need a lot of skills to 'hack' into the system." (Password Hacking, 2009)

1.4 University Computer System Authentication

One-factor authentication, consisting of a username + password couplet, called NetID and employed by unique software in virtually every instance, is used by the majority of universities in the U.S. (BYU, 2009; Cal State U East Bay, 2008; Cornell U, 2009; Duke U, 2008; Harvard U, 2009; Princeton U, 2009; Purdue U, 2009; U Mass Amherst, 2008; U Washington, 2008; U Wisconsin, 2008; and Yale U, 2009). NetID is simply a convenient acronym but does not designate a common software origin. The universities' security policies are as diverse as the versions of software. In most cases the usernames are assigned for the life of the recipient, on campus and later as an alum off campus. Most are vulnerable to personas with dual roles, such as a student and a staff member, being compromised (Romney, 2008). UMass Amherst is somewhat unique and allows different passwords for different roles (U Mass Amherst, 2008). Most of these systems are LDAP-based and the directory information is not private nor anonymous.

The MIT Kerberos Consortium manages a Kerberos authenticated platform that is made available to universities that is considerably more robust. It is still one-factor authentication but relies on a trusted third party model of the university Kerberos system maintaining a database of

clients and their secret keys which the system generates and provides to the users (Schneier, 1996; Smith, 2002). For a persona, the secret key is an encrypted password. Kerberos generates a ticket that the persona presents along with an authenticator to a server. An eavesdropper cannot replay the ticket and authenticator at a later time. The overall system, however, does require careful administration. This platform permits universal "single sign-on" within and between federated enterprises and peer-to-peer communities (MIT Kerberos, 2009); (Duke U Kerberos, 2009; MIT U Kerberos, 2009; U Washington Kerberos, 2009).

Other unique Kerberos-based systems are employed at MIT, Stanford and Carnegie Mellon (Stanford U, 2009 and Carnegie Mellon U, 2009). The Stanford system does allow a persona to control what is displayed in the online directory, but the stored information is not private nor anonymous.

From this brief survey, it is apparent that the majority of universities find a NetID, one-factor user authentication satisfactory. The author has found the one-factor solution to be highly vulnerable in most university settings, particularly due to eavesdropping and man-in-the-middle attacks. The move to Kerberos by some of the more technologically-advanced universities such as Carnegie Mellon, MIT and Stanford demonstrates the sensitivity to vulnerabilities associated with simple NetID one-factor authentication and their attempt to mitigate such vulnerabilities.

One-factor authentication involving Kerberos uses symmetric key cryptography with the advantage that its trusted third party maintains management of all secret keys. Key management over an extended period and key revocation are basically eliminated. The cost is more than traditional NetID but less than two-factor authentication alternatives for over 20,000 users. Two-factor authentication involving something you know and have such as digital certificates generally has not been used in university environments, the author suggests based on his experience of having done so in healthcare, due to the complexities of implementing asymmetric Public Key Infrastructure (PKI). Two-factor authentication involving something you know and something you are is even more cumbersome because of the biometric readers required at many locations (Stevenson & Romney, 2008). Three-factor authentication is used in data centers, high risk financial operations, certification authorities and special research facilities in industry and university research. In these instances, PKI and biometrics are frequently the selected technologies with a characteristically much higher operational overhead.

1.5 Agile Problem Driven Teaching Utilized

In keeping with the Agile Problem Driven Teaching (APDT) pedagogy employed in the National University (NU) School of Engineering and Technology (SOET) described by Dey (Dey et.al., 2009), and, specifically, the BS IT Management (ITM) program (Romney, 2009), the search for improved authentication for smaller enterprises and select university settings was structured into an APDT problem and assigned to undergraduate students in the ITM470/475 IT Security sequence of courses. APDT, as used in ITM similarly to Problem Based Learning, focuses on real-world problems. “Agility” components are introduced to more closely simulate the real-world workplace that students encounter (Agile Manifesto, 2001; Alleman, 2002; Alleman, 2009). These agile components introduced allow students to be creative in discovering alternate solutions and “work-arounds” to a problem. Employing APDT methods in instruction better

prepares students for the workplace. *The defined Problem was to design and implement a useable two-factor authentication process for use by small enterprises and on the SOET WebPortal by less than one thousand faculty, staff, and students.*

1.6 Secure Sockets Layer and Transport Layer Security

Each of us, when we make a purchase, makes use of what was originally called the Secure Sockets Layer (SSL) protocol that was developed and introduced by Netscape (Lee, 2007). The Internet Engineering Task Force (IETF) later renamed and enhanced the standard Transport Layer Security (TLS), to emphasize that it works at the transport layer of the OSI model. For SSL v1 and v2, authentication was a one-way process handled by the server. SSL/TLS uses both symmetric and asymmetric cryptography (Smith, 2002; Panko, 2003) in order to secure the transmissions between a server (for example at Amazon.com) and a user's client browser on their laptop. For the asymmetric component, the server uses a server SSL certificate normally obtained from a trusted certification authority like Verisign. Usually the acceptance of the SSL certificate by the client browser occurs without any intervention by the user, and a padlock symbol, as shown in Figure 1.6.1 appears on the browser to indicate that the transmission between client and server is now securely encrypted.

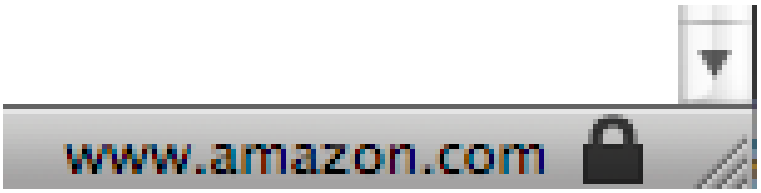

Figure 1.6.1 SSL Padlock Symbol on Browser

When the browser is closed, or the session terminates due to non-use, the secure communication closes.

1.7 SSL Client Authentication

In SSL v3/TLS, the less well known, and frequently unused communal authentication of both client and server is applicable. Not only is there the SSL Server certificate as previously discussed, but a client browser certificate is used as well. Thus, those who desire to access the server must be pre-enrolled and be possessors of a client browser digital certificate. The certificate exchange is done via x.509 certificates, and public key cryptography is used to start the connection. Two to four seconds is required to establish the secure connection. Once authentication is made, the channel is secured with symmetric key cryptography methods and hashes, typically RC4 or 3DES for symmetric key and MD5 or SHA-1 for the hash functions (IBM, 2007).

1.8 Security Students Architected a Two-factor Authentication Solution

ITM students accepted the APDT problem to design and implement a useable two-factor authentication process using the SOET WebPortal architecture shown in Figure 1.8.1.

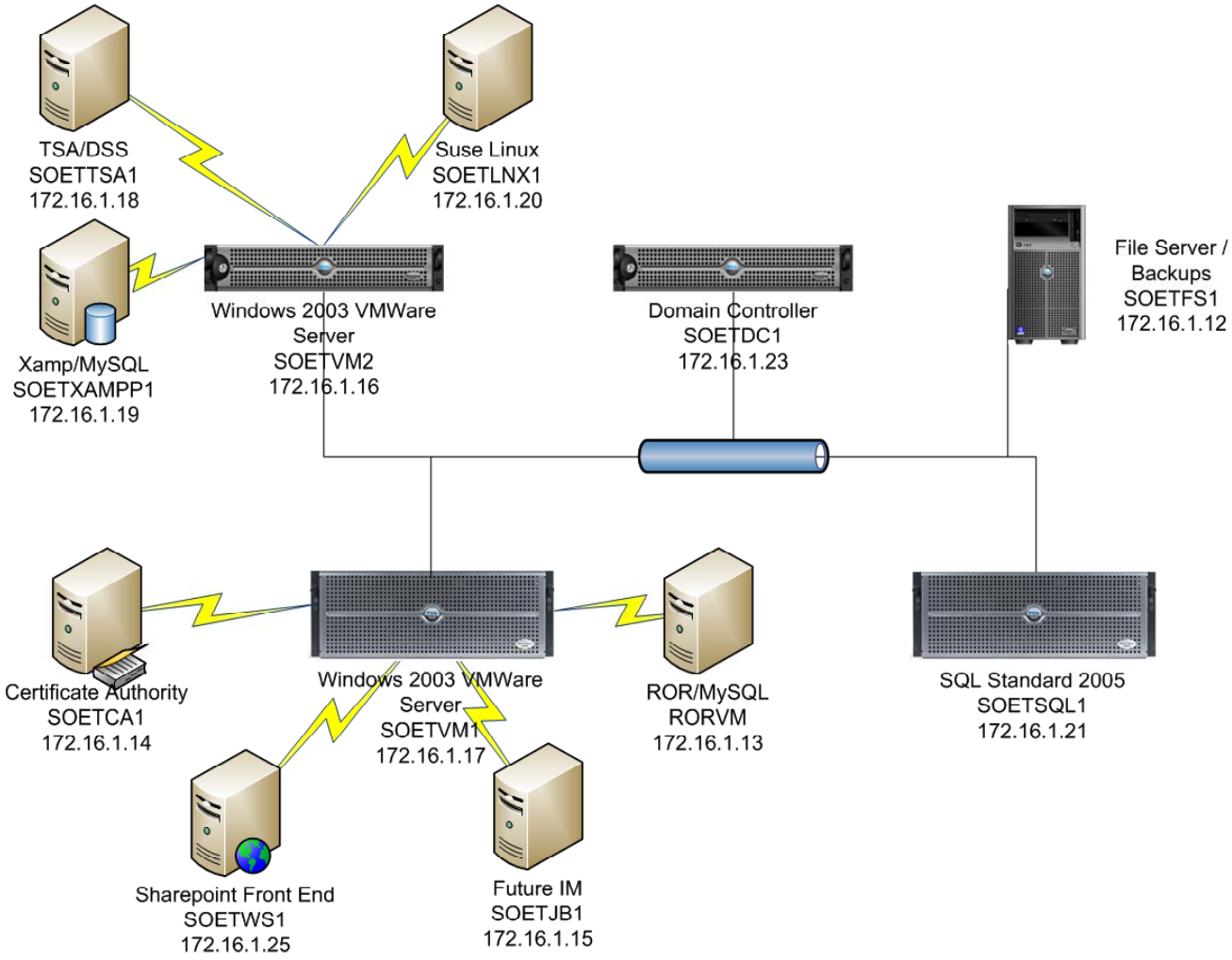

Figure 1.8.1. SOET WebPortal

The WebPortal environment was initially architected by the student co-author, Juneau, and implemented by his team of students using Microsoft (MS) .NET technology with Windows 2003 Server. Other preliminary projects were the installation of MS Internet Information Services (IIS) 6.0, with Active Directory and Domain Controller, a Certificate Authority and Windows SharePoint Services (WSS) 3.0. The security component that is the purpose of this paper, and the Problem addressed in Section 1.5, above, was to provide a useable two-factor authentication process for users who want to access the WebPortal, and, initially, the SharePoint Front End server SOETWS1 that is to the left on the bottom row in Figure 1.8.1.

Juneau's team decided to employ Secure Sockets Layer (SSL) and require a client to present the following two authentication factors in order to gain access to the WebPortal: 1) the first authentication factor (something you know) of a username and password couplet, and then 2) the

second factor (something you have) of an SSL client browser certificate and it requires its own additional, (something you know), of a secure pass phrase. The Plan was to complete the following steps:

1. Designate and authorize two administrative roles to be played following Security Best Practices:
    a. a System Administrator (SysAdmin) with administrative rights to all necessary processes.
    b. a Certification Authority Administrator (CAAdmin) with administrative rights to all certificate management processes.
2. Have the SysAdmin enroll the clients (students and instructors) with username and password couplets into Active Directory. Have the clients change their passwords.
3. Have the SysAdmin apply for a Secure Sockets Layer (SSL) server certificate via web access for the IIS server via the Certificate Authority SOETCA1.
4. Have the CAAdmin issue the pending SSL server certificate via the Certificate Authority.
5. Have the SysAdmin install SSL on IIS.
6. Have all clients apply for personal SSL client browser certificates via web access to the Certificate Authority; an individually secure pass phrase must be specified.
7. Have the CAAdmin issue the pending personal SSL client browser certificates via the Certificate Authority.
8. Have the clients download their issued certificate into the browser they have selected using the previously specified secure pass phrase.

The clients were all located in a SOET classroom and would use the standard classroom Windows workstations for the exercise. The final objective was to see a client a) bring up a browser, b) specify the URL for the SOET WebPortal and be prompted to specify her username and password, c) be prompted to present the client browser certificate that had been stored in the workstation browser and specify the secure passphrase, and then d) be allowed access to the SOET SharePoint Home Web page.

2. THE TEAM EXECUTION OF THE PLAN

One key objective of the APDT model is to not only use Agile methods in teaching, but to employ them in programming and project management. Over the extent of the course, the student teams were being trained in the methodology of Agile Project Management. Raising a project manager from the level of “uninspired taskmaster” to that of “visionary leader” can effectively be achieved by employing Agile Project Management (Ccpace, 2009). Challenges were encountered in the execution of the Plan defined in Section 1.8, and adjustments to strategy and “workarounds” had to be made. Examples of these ‘glitches’ or problems so typical of IT, identified and solved by the team, are those described in Sections 2.1 through 2.3. Sections 2.4 and 2.5 deal with issues caused by the client user, the instructor, modifying the deliverables.

2.1 Inability of the Web Server to Join the SOET Domain

The problem encountered was the inability of the CA server to communicate with the Web server. This was caused by the Routing and Remote Access (RRA) network service in MS Windows Server which was enabled and included activating the Network Address Translation (NAT) feature which masked the IP of the CA server making it inoperative. Simply disabling the RRA network service created no additional problems and allowed the CA to function in order to issue digital certificates.

2.2 Inability to Create and Install the Certificate Authority Web Server

The problem encountered was the inability to create the Certificate Authority Web Server. It was discovered that this was a loading sequence issue. When MS Server 2003 CA was installed first and IIS second, the CA did not work. Reversing the order and installing IIS first and then installing MS Server 2003 CA allowed the creation of a CA web site that was crucial in order to apply, issue and download digital certificates.

2.3 Inability to Access the Default Web Page Under IIS

The problem encountered was when attempting to access the web server, the default web page of the ISS server was reporting to users that the server required them to use a secure connection. When we added "s" to the "http" in the address bar, it would redirect them to "http://soet-web/index.aspx". Somehow, the server process left the "s" out of the default web page. Through research and some handy JavaScript code, we were able to create a custom 404-3 error that would redirect requests to the correct site using SSL.

2.4 User Client's Requirements Change

IT emphasizes synergistic solutions between technology, people and processes to successfully resolve enterprise computer problems. In the ITM program, students learn that people, namely the client, drive the development process. IT professionals, with their knowledge, skills and set of technology tools attempt to meet the requirements specified by the client. In almost every development instance, the client's perception of the desired product evolves. That was the case in this particular instance as the instructor, serving as client user, changed a requirement that the browser used in the authentication process needed to be not only MS Internet Explorer (IE) but also Firefox.

The team, in an attempt to meet the client user's changing requirements tried, unsuccessfully, to replace the working IE browser with a Firefox browser. It found that Windows Server 2003 CA would not allow Netscape version 6.2.2 and later browsers to perform enrollment through the Web enrollment pages. The following command entered at the command prompt resolved the problem: certutil -setreg ca\CRLFlags +CRLF_ALLOW_REQUEST_ATTRIBUTE_SUBJECT
The team's perseverance prevailed with success.

2.5 Team Discovers an Enhancement that the User Client Couldn't Do Without

Over the duration of the execution of the Plan, the team continuously discussed the proposed solution to the problem specified in Section 1.5 with the client user and discovered that both the client user and the team were not satisfied with step 9 in the Plan specified in Section 1.8. This step called for the clients to install the personal browser certificate in the browser of the classroom workstation. Such an installation constrained the authentication process to a static workstation. Portability of the certificate is what was needed. The team searched and Juneau discovered an Open Source secure, portable container provided by TrueCrypt that would allow the encrypted storage of browser certificates (TrueCrypt, 2009). Furthermore, it would allow the installation of portable applications including Firefox (PortableApps, 2009).

3.0 TRUECRYPT PORTABLE VIRTUAL ENCYPTED CONTAINER

The objective is to have a browser digital certificate securely stored on a portable USB flash drive that one can take to the classroom, home or any Internet café and use to gain access to the SOET WebPortal using two-factor authentication.

TrueCrypt.com provides an Open Source portable, virtual encrypted drive capability (TrueCrypt, 2009). A USB flash drive with a minimum of 128 MBytes is required as the physical storage device. TrueCrypt is executable software for either Windows or OS X that creates a container, or file, on which a volume is defined. A container is just like any normal file as it can be moved, copied or deleted and has a filename. Military grade encryption, AES-256, is used to encrypt/decrypt all files moved to/from the container under password control. All of this is done automatically by the TrueCrypt software.

3.1 Portable Firefox and Browser Certificate Storage

For this example of authentication, a USB flash drive was installed on a workstation. A TrueCrypt volume was created, encryption algorithm selected, and password specified. For more general usage, Firefox was designated the browser of choice. Portable Firefox was downloaded and stored encrypted in the container. A client browser certificate was requested as step 6 in the Plan of Section 1.8. Step 7 issues the certificate, and the client downloaded the issued certificate as step 8. This certificate was imported to the Firefox browser and stored encrypted. The TrueCrypt volume was dismounted, and the USB flash drive was stopped and unplugged.

3.2 To use the TrueCrypt Container

The portable certificate vault may be taken to any workstation, plugged in and used to bring up Firefox. If the SOET SSL URL is specified, the browser certificate will be activated and both factors of authentication implemented to allow access to SharePoint on the WebPortal via a secure SSL transmission. Otherwise, Firefox functions as a normal browser which it is. Figure 3.2.1 illustrates the Client Browser Certificate being presented for authentication to go to the ASEE PSW09 Meeting web page. The Calendar page is revealed under the certificate.

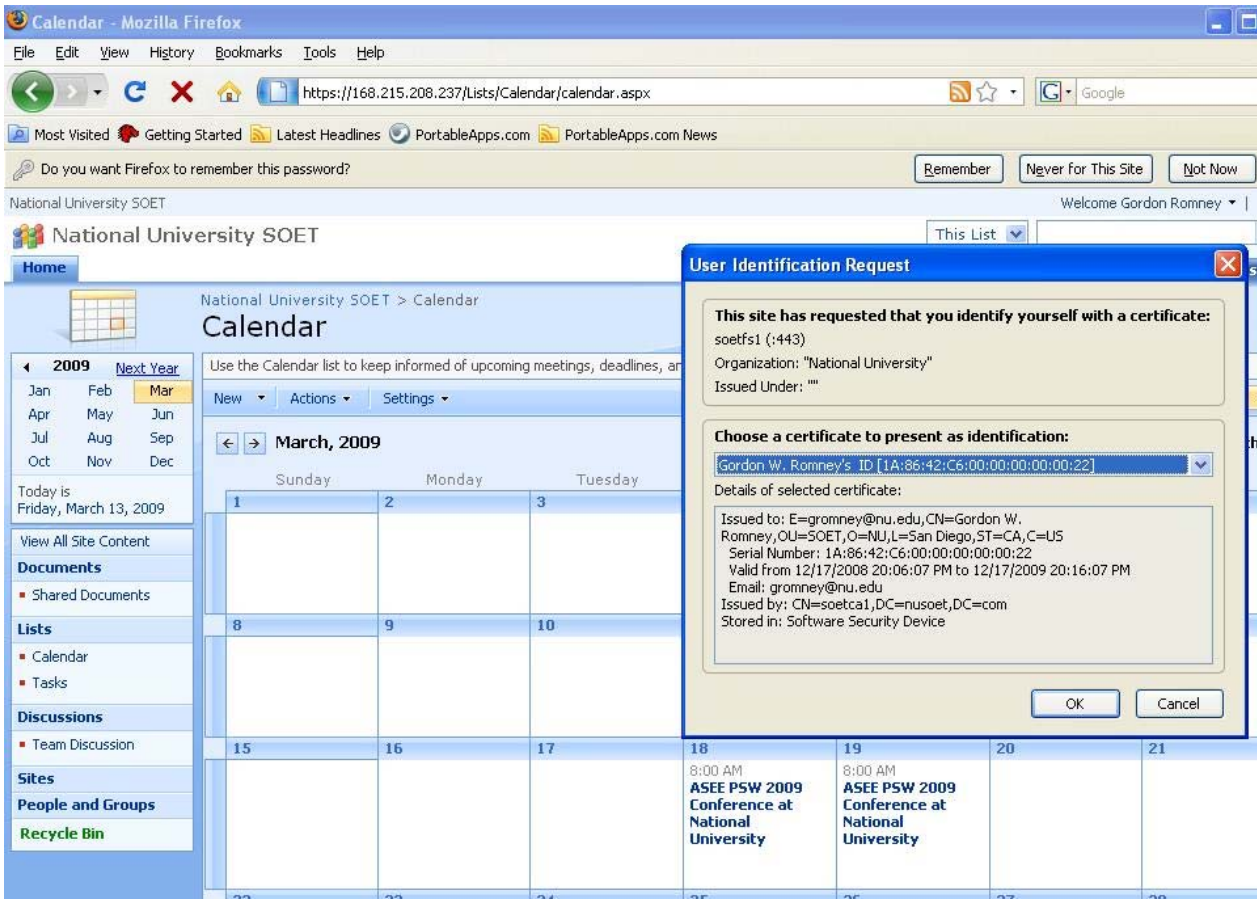

Figure 3.2.1. Client Browser Certificate and SOET SharePoint Calendar

The certificate vault is fully encrypted by military grade cryptography. The certificate issued to the user is only accessible out of the vault under password control as it is called up by the browser.

4.0 Conclusion and Future Research

The defined Problem was to design and implement a useable two-factor authentication process for use by small enterprises and on the SOET WebPortal by less than one thousand faculty, staff, and students. The Learning Objectives of developing the solution to this problem in an agile manner in keeping with Agile Project Management were met most satisfactorily by the student team as workarounds to "glitches" were effectively implemented. Additionally, the team demonstrated a mature approach to dealing with client user modifications to the original project requirements which is one of the fundamental tenants of the Agile Manifesto (Agile Manifesto, 2001). Most impressively, the team demonstrated a superior ability to be constantly communicating with the client user which, in turn, led to the mutual accord to pursue the TrueCrypt encrypted portable container solution. The absence of such communication would not have produced a most novel and critically important solution. This effort produced a satisfactory two-factor authentication solution applicable to not only the SOET NU university environment, but one that is viable for many small to medium sized business enterprises that want to augment the quality of their security beyond standard username + password solutions.

The constraint of a maximum of "one thousand" personas is based on past experience in managing personal certificates. The security policies can be established such that certificate revocations are not an issue. Most universities, after all, keep user NetIDs for life. Storage, likewise is not a major constraint since disk storage costs continue to decrease. The greatest concern is in developing a streamlined process for enrollment and certificate downloading into TrueCrypt containers. Research will need to be done to determine the limiting factor associated with this portable certificate vault solution.

Another issue of concern to NU is that a substantial number of NU students are associated with the Navy, Marines and Department of Defense contractors. The recent ban in 2008 on the use of USB jump drives presents a slight impediment. The TrueCrypt portable container, however, can be stored on mini-CDs.

Future research in the area of Kerberos and pursuit of the MIT Kerberos Consortium have merit.

A most intriguing authentication methodology that uses the cell phone as a second factor of authentication is marketed by PhoneFactor.com (PhoneFactor, 2009). This we anticipate to pursue in future research.

REFERENCES

Agile Manifesto. (2001). http://agilemanifesto.org/
Retrieved 16 February 2009 06:45 UTC.

Alleman. (2002). G.B. Alleman, "Agile Project Management Methods for IT Projects," Niwot, CO 80503, Chapter X in *The Story of Managing Projects: A Global, Cross–Disciplinary Collection of Perspectives*, E. G. Carayannis and Y. H. Kwak, editors, Greenwood Press / Quorum Books, 2002.

Alleman. (2009).
http://www.niwotridge.com/Resources/Columns&PublishedArticles.htm#Chapters
Retrieved 14 February 2009 12:32 UTC.

BYU, (2009). https://y.byu.edu/ae/prod/person/cgi/createNetId.cgi
Retrieved 15 February 2009 12:24 UTC.

Cal State U East Bay. (2008).
http://www.csueastbay.edu/ics/helpdesk/HDNetIDFAQS.html
Retrieved 29 November 2008 13:33 UTC.

Carnegie Mellon U. (2009). http://www.net.cmu.edu/docs/arch/netbar.html
Retrieved February 20 2009 14:34 UTC.

Ccpace. (2009). Ccpace.com white paper, "Agile Project Management,"
www.ccpace.com/Resources/documents/AgileProjectManagement.pdf
Retrieved 14 February 2009 19:49 UTC.

Cornell U, (2009). https://netid.cornell.edu/ Retrieved 15 February 2009 12:14 UTC.

Crowley. (2003). E. Crowley, "Information System Security Curricula Development," *CITC4'03*, pp. 249-255, October 2003.

Dey et.al. (2009). P.P. Dey, T.M. Gatton, M.N. Amin, M.F. Wyne, G.W. Romney, A. Frarahani, A. Datta, H. Badkoobehi, R.Belcher, O.Tigli and A.P. Cruz, "Agile Problem Driven Teaching in Engineering, Science and Technology," ASEE/PSW-2009 Conference, San Diego, CA March 18-20, 2009.

Duke U. (2008).
http://www.oit.duke.edu/netid-security/netid/
Retrieved 29 November 2008 13:27 UTC.
Duke U Kerberos, (2009). www.security.duke.edu/netid-authentication.html
Retrieved 3 March 2009 16:34 UTC.
Harris. (2008). S. Harris, "All-in-One CISSP – Exam Guide," Fourth Edition 2008, McGraw-Hill, New York, New York 10121 ISBN: 978-0-07-149787-9.
Harvard U, (2009). www.ssrn.com/SiteLic_orgSubscribers.cfm?netid=810024
Retrieved 15 February 2009 12:09UTC.
IBM. (2007). IBM, "Using the Secure Sockets Layer protocol for secure communications," http://publib.boulder.ibm.com/infocenter/wasinfo/v1r0/index.jsp?topic=/com.ibm.websphere.ihs_2047.doc/9atssl.htm
Retrieved 16 August 2008 04:10 UTC.
Lee. (2007). H.K. Lee, "Cryptographic Strength of SSL/TLS Servers", Ihttp://www.imconf.net/imc-2007/papers/imc130.pdf
Retrieved 20 March 2008 04:23 UTC.
MIT Kerberos. (2009). http://www.kerberos.org/
Retrieved 6 March 2009 13:25 UTC.
MIT U Kerberos. (2009). http://web.mit.edu/Kerberos/dist/
Retrieved 6 Marcb 2009 13:17 UTC.
Password Hacking. (2009). http://www.techexams.net/technotes/securityplus/passwords.shtml
Retrieved 4 March 2009 15:23 UTC
Panko. (2003). R.R. Panko, "Corporate Computer and Network Security," 2003, Prentice Hall, Upper Saddle River, NJ 07458, ISBN: 0-13-038471-2.
Phone Factor. (2009).
http://www.phonefactor.com/how-it-works/white-paper/download/
Retrieved 9 March 2009 17:52 UTC.
PortableApps. (2009). http://www.portableapps.com
Retrieved 19 November 2009 16:43 UTC.
Princeton U. (2009). http://www.princeton.edu/tigers12/infotech/your_princeton_netid/
Retrieved 7 February 2009 22:02 UTC
Purdue U. (2009).
www.itap.purdue.edu/security/files/documents/RASCCIAv13.pdf
Retrieved March 4 2009 18:28 UTC
Romney. (2008). G.W. Romney, "There Exists a Critical Need for Role-based IDs in a University IT Infrastructure in Order to Meet Security Best Practices," International Computer Science and Technology Conference, San Diego, April 2008.
Romney. (2009). G.W. Romney, "The Integration of Ruby on Rails As An Agile Teaching Tool in IT Curricula," ASEE/PSW-2009 Conference, San Diego, CA March 18-20, 2009.
Schneier. (1996). B. Schneier, "Applied Cryptography," 1996, John Wiley & Sons, Hoboken, NJ 07030-5774, ISBN: 0-471-12845-7.
Smith. (2002). R.E. Smith, "Authentication – From Passwords to Public Keys," 2002, Addison-Wesley, Upper Saddle River, NJ 07458, ISBN: 0-201-61599-1.
Stanford U. (2009). https://sunetid.stanford.edu/
Retrieved 7 March 2009 16:12 UTC.
Stevenson & Romney. (2008).B.R. Stevenson and G.W. Romney, "Analysis of Near-infrared Phase Effect on Biometric Iris Data Demonstrates Viability of An Iris-scan Biometric Device for Identity Authentication in Public Venues," International Computer Science and Technology Conference, San Diego, April 2008.

TrueCrypt. (2009). http://www.truecrypt.com
Retrieved 8 March 2009 15:46 UTC
UC Irvine. (2009). http://www.ucop.edu/irc/itlc/ucfedauth/IMCriteria/UCI/IM-Criteria-UCI.html
Retrieved 7 March 2009 15:24 UTC.
U Mass Amherst. (2008). http://www.oit.umass.edu/spire/logon/preferred_role.html
Retrieved 29 November 2008 14:24 UTC.
U Washington. (2008). http://www.washington.edu/computing/uwnetid/
Retrieved 29 November 2008 11:38 UTC.
U Washington Kerberos. (2009).
www.washington.edu/computing/infra/shibboleth/uwash-incommon-pops.doc
Retrieve 4 March 2 2009 18:54 UTC.
U Wisconsin. (2008). http://helpdesk.wisc.edu/page.php?id=4966
Retrieved 29 November 2008 16:46 UTC.
Yale U. (2009). www.yale.edu/its/accounts/netid.html Retrieved 3 Mar 2009 23:12 UTC.

BIOGRAPHY

Gordon W. Romney, Ph.D. is a Professor in the Department of Computer Science and Information Systems, School of Engineering and Technology, at National University. He is Director and Senior Research Scientist of the SOET Cyber Security and Information Assurance Laboratory.