MATEC Web of Conferences **41**, 05004 (2016)
DOI: 10.1051/matecconf/20164105004

Implementing Security in a University Network

Ioannis Diakakis[2], Ioannis Almaliotis[1,a] and Theodoros Mitakos[1]

[1]*Technological Educational Institution (TEI) Stereas Elladas, 34400, Evia, Greece*
[2]*Gymnasio Vasilikoy, Neofytou 80, Vasiliko, 34002, Greece*

Abstract: This paper describes the implementation of a revised security plan in the Technological and Educational Institution Stereas Elladas. This technology uses smart cards and 8 digits alphanumeric to provide high data security and encrypted communications in the university campus network.

1 Introduction

Internet is quickly becoming the largest marketplace, allowing commerce and business between parties who are physically distant and do not know each other. In many (or most) business relationships, the parties need to establish some trust in each other, by receiving references from trusted intermediaries. It is recognized that on the Internet this trust can no longer be facilitated through conventional password based security techniques. Thus, bank transactions, online shopping, sensitive information sharing, etc require a safer environment in order to take place. The ease of communication between people sharing common ideas and interests, no matter where they reside, can be considered as a new dimension in freedom.

However, internet's growth has generated the need of advanced security systems. New forms of software "weapons" have been developed, which cause overloading of servers, outages, denial of service and money loss to internet connected networks.

Especially in university campus networks, the problems in security and data safeguarding are being multiplied by the number of the university's students, which are devoted to a game of running malicious software, overloading network resources, causing all kinds of problems to systems and downloading massive data from the internet.

The Technological Educational Institute of Stereas Elladas located in Psahna County, has five Departments, over 400 workstations distributed over four buildings, using one **1 Gbit fiber optics line** to access the internet. Students and staff use the Internet to perform research and tasks, often through bandwidth-intensive flash presentation, videos and sound clips. Without a tight security system, the vulnerability of the network is too high leading to small availability, large access times and a lot of frustration from both our students and staff.

With the use of existing technology and the appropriate software applications, we can apply a **revised** Public Key Infrastructure (P.K.I.) based authentication scheme, which assures network security for professors and personnel (from now on called "users"), and tighten server security to a level beyond the scope of the biggest part of the attacks. With the completion of this proposal, the following steps take place:

i. The users acquire a smart card from the university's Network Operation Centre (NOC).
ii. Every time users access the campus network, they use the smart card to log on to the systems.
iii. The university's directory server validates the user from the certificate stored in the smart card and authorizes access to the resources, using a secure channel after the correct pin has been entered by the user.
iv. Each group of users retains its own rights in the campus network.
v. The original security infrastructure of the network remains with minor changes in order to incorporate the PKI system.
vi. Uses may have access from any station through out the campus.
vii. After finishing work, the user simply removes the smart card from the reader and is immediately logged off.
viii. Each card is paired with a code like a pin. The student has to put the card to the reader and then insert the pin into the system in order to log in. This way if a card is lost by a student no one can enter to the system and obtain the privileges of the student who has lost the card.
ix. If the pin enters incorrectly for more than 5 times then the card is locked and the user has to come to the NOC of TEI in order for the card to be unlocked.
x. Each semester the student is obliged to change the pin for security purposes.

2 The intensifying problem

The size of the problem is clear in the statistics of the Cisco 2014 Annual Security Report.
Attacks against infrastructure are targeting significant resources across the Internet.

Malicious exploits are gaining access to web hosting servers, name servers, and data centers. This suggests the forming of überbots that seek high-reputation and resource-rich assets.

[a] Corresponding author: ialmaliotis@teihal.gr

• Buffer errors are a leading threat, at 21 percent of the Common Weakness Enumeration (CWE) threat categories.
• Malware encounters are shifting toward electronics manufacturing and the agriculture and mining industries at about six times the average encounter rate across industry verticals.
• Malicious actors are using trusted applications to exploit gaps in perimeter security.
• Spam continues its downward trend, although the proportion of maliciously intended spam remains constant.
• Java comprises 91 percent of web exploits; 76 percent of companies using Cisco Web Security services are running Java 6, an end-of-life, unsupported version.
• "Watering hole" attacks are targeting specific industry-related websites to deliver malware.
• Indicators of compromise suggest network penetrations may be undetected over long periods.
• Threat alerts grew 14 percent year over year; new alerts (not updated alerts) are on the rise.
• Ninety-nine percent of all mobile malware in 2013 targeted Android devices. Android users also have the highest encounter rate (71 percent) with all forms of web-delivered malware

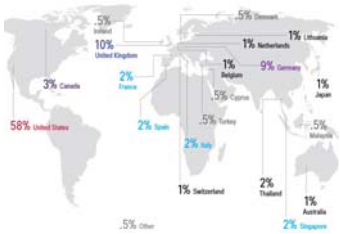

Fig.1. The size of the problem. The map shows the server compromising by country in 2013 Source: Cisco TRAC/SIO

In the following Figure (2) we present the number of attacks in T.E.I Stereas Elladas as they have been recorded in our logs for the period of Jan 2006 to Dec 2014. As we can clearly see the number of attacks increment is almost exponential during that period. This increment continues in an exponential form from 1999 - 2005 period. This fact shows clearly that the implementation of an even stronger security policy is required in order to ensure the integrity and reliability of the network.

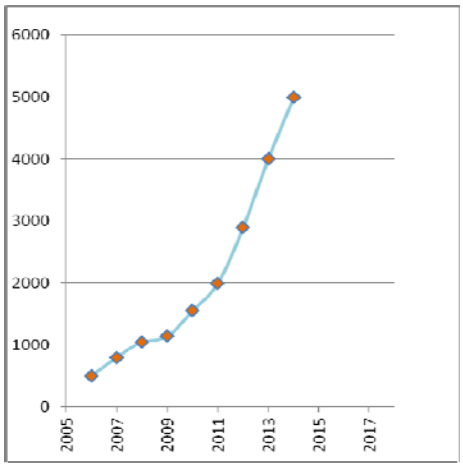

Fig.2. Number of attacks in T.E.I. Stereas Elladas for the period of 2006 to 2014.

Simple password authentication methods could be breached easily and were vulnerable to hackers, due to new attack technologies and the increasing processing power, which could be used for password cracking. The situation did not improve enough by the usage of more complicated passwords that included more than 8 characters or symbols. As a result, important data transfers and sensitive data transferred through campus networks can't be considered to be safe any longer. Even SSL connection are not considered unbreachable anymore as shown in Figure 3 below.

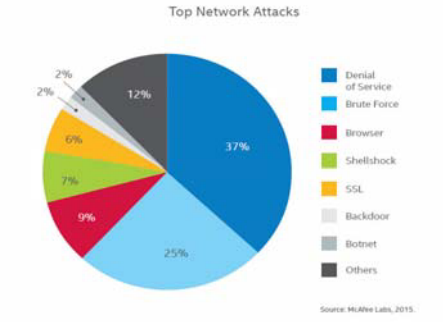

Fig.3. Most common network attacks detected in Q1 2015. - **Source: McAfee Labs 2015.**

In order to get over this problem, new authentication methods have to be adopted. They use advanced technologies to prevent unauthorized access to sensitive data and ensure safe transactions. Much like a passport proves identity in the offline world, public-key infrastructure (PKI) delivers a way to prove identity in the online world. Identity and authorization management (IAM) applications and encryption generally are considered two of the most important components of a layered security environment. Today it is not enough to assume that the person who has access to data is authorized, it is essential to confirm that authorization and make sure that the decryption protocols are followed in accordance with the company's information security policies and procedures.

In the Windows environment, IAM is an integral component of Microsoft Active Directory. While we've looked at numerous IAM tools enterprises can use, ranging from the Public Key Infrastructure (PKI) for small to midsize businesses to enterprise-class offerings that also include credential management, PKI is very popular amongst companies of all sizes.

3 Suggested solution

3.1 Solution Implementation

This solution consists of 3 basics parts: i. The PKI, technology, ii. The Client side and iii. The Server side. The logical structure of the solution is depicted in Fig 4.

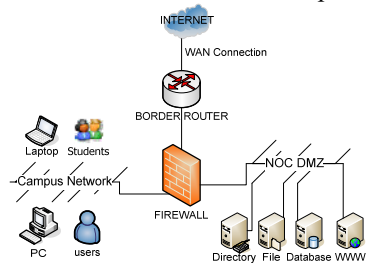

Fig.4. Logical structure of the solution.

3.1.1 PKI Technology

From an operational perspective, PKI is an encryption approach where a pair of cryptographic keys -- one public and one private -- are used to encrypt and decrypt data. A user can give someone their public key, which that sender uses to encrypt data. The owner then uses their private key to decrypt the data. This authentication and encryption approach originated in the British intelligence community in the early 1970s and has been used commercially for nearly 20 years.

But what can a PKI actually *do* for a company? According to Microsoft, here are some the key reasons to deploy this infrastructure:

- Control access to the network with 802.1x authentication
- Approve and authorize applications with Code Signing
- Protect user data with the Encryption File System (EFS)
- Secure network traffic IPSec
- Protect LDAP (Lightweight Directory Access Protocol)-based directory queries - Secure LDAP
- Implement two-factor authentication with smart cards
- Protect traffic to internal web-sites with Secure Socket Layer (SSL) technology
- Implement secure email.

A number of applications also can use the PKI certificates. Aside from the aforementioned email and network access controls, PKI also can be used for enterprise- and SMB-class databases, electronic document and forms signing, secure instant messaging, mobile device security, securing USB storage devices, Windows Server Update Services, Active Directory and more.

3.1.2 Client Section

The client section requires a computer, connected to the campus network, with a smart card reader installed on it. In order to work and communicate with the server the subscriber's smart card reader is required as well, whatever level of security the user chooses to have.

In addition to the PKI card the system will also require an 8 digit number which will be paired with each card in order to ensure maximum security in case of a stolen or lost card. The number will be changed in each semester with a new one by the user. The number will be validated by the validation server of the TEI through an SSL connection after the PKI card is inserted to the reader.

For remote access, an internet connection (DSL, or any other) will also be needed. Because of the small amount of data transferred, even a PSTN dial-up connection can be sufficient. This computer can be in the customer's home, work or anywhere else in the world, where internet is accessible.

Instead of the combination of smart card – smart card reader, the recent technological development provides a much cheaper solution, the USB Tokens, which are small electronic devices that can store the same information and be connected to a standard USB (Universal Serial Bus) port of any standard computer in the market today.

After being authenticated and authorized to access the campus network, the user gets access to the resources. During this session, all communication with the server is achieved using a secure tunnel with high encryption.

The 8 digit security code will be changed in each semester, when the student will be prompted to change the code. If not then the connection will not be validated and the user would not connect to the network.

In case of a lost or stolen card the user is obliged to come to the NOC of the TEI in order to obtain a new card an cancel the old one. Each student will be eligible for three cards throughout his/her student life. After the lose of the 3rd card the student will be permanent locked out from the university network for security reasons. He/she will be eligible for a new card after a decision is made from the council of the Institution.

3.1.3 Server Section

The server section consists of numerous combined servers that are located in the Network Operation Center of the university facilities, under close supervision.

The exact configuration of servers depends on the specific needs of each implementation, but a basic configuration will be satisfied with the following: i. Directory server, ii. File server / Web server, iii. Firewall and network equipment, iv. PKI Server

3.1.3.1 Directory Server

The directory server is responsible for:

- Authentication
  In order for the server to allow access to the campus network, an authentication procedure must take place. This procedure consists of the exchange of user credentials being transmitted encrypted, using the certificate that is stored in the smart card. The system allows access only when both the smart card and the user's password (or PIN) is provided. The certificate authentication is achieved because the directory server is configured to accept certificates issued from a specific CA (Certification Authority). In this case, the directory server allows access to certificates that are issued from the university's CA (or any other configured).
- Encryption
  Secure transactions of sensitive personal data, such as documents, research data, student grades and test results, need a strong encryption method. This is accomplished using an SSL (Secure Socket Layer) certificate in the server side. This certificate creates an SSL tunnel from the server to the client and back, allowing the secure transfer of all personal data and transaction history.
- Authorization
  The directory server allows access to the resources that should be available to the specific user. Depending on the user type, during user logon the server may guide the user's computer to run scripts, attach network

drives, log on to other servers, run programs, load roaming profiles and others.

- Accounting
  The directory server can also control and record usage statistics, monitor data access and log any unsuccessful attempt for unauthorized access to any resources.

3.1.3.2 File Server / Web Server

The file server may store user directories, maintain user profiles and be the storage place for user's sensitive date. The data stored on the server can also be encrypted using the same (or another) digital key. The web server can also be the host of web-based applications for users. All transactions with the web server can be encrypted using the same (or another) digital key.

3.1.3.3 Firewall and network equipment

The network infrastructure of the central system is consisted of the physical interconnection of the servers within the Network Operation Center, as well as their connection to the rest of the campus network. This connection is media independent and can be optical, wired, or wireless. The presence of a firewall is absolutely necessary, in order to protect the NOC from local and internet threats. For remote access, an internet connection should also be available.

3.1.3.4 PKI Server

Based on the complexity of the environment, it is possible to have a single server act as both the root and issuing CA. A two-tier hierarchy consists of the root CA with issuing CAs connecting up to the root. This is considered to be the most common design, although the architecture can be designed with a Policy or Intermediate CA sitting between the root and issuing CAs. In this design, the policy server could restrict the types of certificates an issuing CA could create.

3.2 Methods and Materials

The methods and materials used in this project are the following: i. PKI Infrastructure, ii. Cryptographic device (Smart Cards, USB Tokens), iii. RA (Registration Authority), iv. Servers, networking equipment, backup solutions, security guidelines, internet connection

3.2.1 PKI Infrastructure

For the implementation of this project, the university hosts a Certification Authority. This can be a local CA (based on Open CA or Microsoft Certificate Services) or a sub - CA of a trusted CA like Verisign, through various providers in Greece, or abroad.

3.2.2 Cryptographic Device

The cryptographic device could be a smart card or a USB token. In order to avoid the extra cost of the smart card reader, a USB token is preferred. This cryptographic device is used in order to produce and store the certificate. The certificate is produced in it using its embedded microprocessor and is stored in its EEPROM flash. A digital certificate is generated using the RSA algorithm and has a variable bit length, according to security requirements. A common cryptographic device can store an amount of 5 to 10 digital certificates.

3.2.3 Servers, networking equipment, backup solutions, security guidelines, internet connection

As mentioned before, a number of servers, a firewall and other network equipment are needed in order to implement PKI to a campus network. The servers would most commonly be based in x86 architecture.

For the directory server, either Microsoft's Active Directory or other LDAP-based directory servers can be used. The file server can be Microsoft's Windows 2008 Server and the web server can be any, like Microsoft's IIS or an open source web server as "apache web server", as long as it supports SSL certificates.

Finally, an internet connection is required in order to provide the services to remote locations, using direct access, VPN, dial-up or any other method.

4 Conclusions

With the implementation of this scenario we enhance the PKI technology, in order to secure the access of network resources and exchange sensitive data between the server and the clients. The solution is commonly used, reliable and it succeeds in offering a very secure network both from the side of server as well as from the side of clients.

Especially with the revised method, were in addition to the PKI key, an 8 digits alphanumeric code is needed in order for the student to gain access to the network resources, we believe that we maximize the security even in the case where the card or usb stick is lost or stolen.

The only disadvantages that someone could find in this solution is the extra cost for the Institution and for the student, the extra workload for the computing personnel in order to implement this method and the extra workload of the servers of the institution. But all these factors are minor in relation to the benefits achieved by the increased security of the Institution's network.

References

1. Bruce Schneier, *Applied Cryptography*. John Wiley & Sons, Inc, 1996
2. *Verisign Inc. guides*, http://www.verisign.com
3. *SysGillo Crypto Smart Card* http://www.incard.it
4. *OpenCard* , http://www.opencard.org/
5. *Microsoft CryptoAPI* http://www.microsoft.com
6. M.Papalabrou, I.Almaliotis, I.Diakakis, Secure University Campus networks using public key infrastructure (PKI) IWSSIP 2005.
7. Amir Herzberg, Access Control Meets Public Key Infrastructure, Security and Privacy 2001.
8. Internet X509 Public Key Infrastructure documents, http://www.ietf.org/ids.by.wg/pkix.html
9. Common Data Security Architecture (CDSA), http://developer.intel.com/ia1//security/documentation.htm
10. Simple Public Key Infrastructure (SPKI), http://www.ietf.org/html.chapters/spki- chapter.htm
11. M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis, The KeyNote Trust- Management System, http://www.cis.upenn.edu/~angelos/keynote.htm