The use of Cryptosystems and Encryption Technologies in Communication Security

BLERINA ÇELIKU
RAFAIL PRODANI
Departamenti i Shkencave te Natyres dhe Humane
Universiteti "Fan S.Noli" , Korçë
blerina.celiku@yahoo.com
rprodani@yahoo.com

Abstract

Cryptography is a science that focuses on creating new algorithms used in different cryptosystems and encryption technologies to protect the information that is considered important to us. There are many ways that we communicate with others on computers, and 95 percent of those communications are not secured against secret listeners. We have nowadays complex networks and we have to choose what cryptographic system or program we need to protect our data and communications. The data may be in storage areas or in transit. Whether we realize it or not, there are a lot of ways that we deal with some form of encryption every day. As businesses now rely heavily on the Internet and other forms of networks to buy, sell, organize, inform, provide services, they also deal with the fact that these networks are transmitting very sensitive data. We log on to a network, send an e-mail, do a transaction, use the ATM, buy a music DVD and there are so many solutions to handle the above operations secure and safe. Secure e-mail, Instant Messaging, Secure e-commerce, Online Banking, Virtual Private Networks (VPN-s) and Wireless Security are some of the solutions used and easy implemented. Also we need to authenticate users that log on to a network and currently the majority of networks around the world only require a valid User Name and password. That is not enough sometimes and there are a number of very good authentication systems that utilize encryption. Human identity theft is one of the most common problems in network security and there are so many devices used to prevent this. We study these technologies and decide what is the best option in different situations for us.

Keywords: *Cryptosystem, e-commerce, VPN, encryption, Wireless security.*

1. Introduction

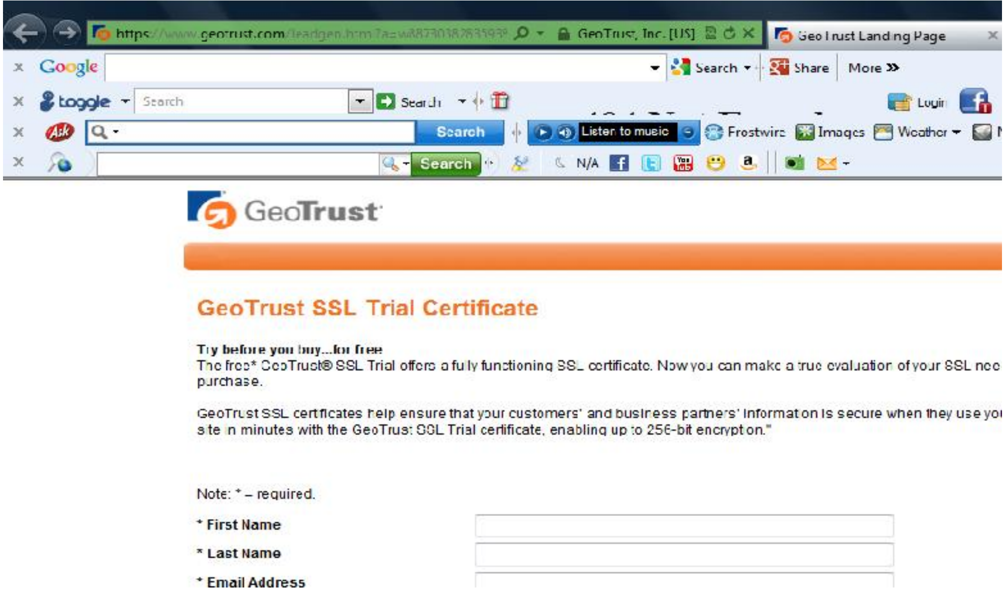
Nowadays many systems require a certain amount of training of both administrators and users to manage, maintain and to use the systems. Data security is such a discussed theme and the difficulty is that we deal with complex networks. We have data in local area storages and in communication. There are different mechanisms and solutions to protect data in storage or in transit. Encryption is a process that is used in so many cases and we need technology to handle that. In cryptography, the operation for hiding data is called algorithm. Algorithms used in programs today are mathematical functions with the instructions written in different programming codes. It all depends on our needs as to which algorithms we will use in our system. A cryptosystem is basically the combination of three elements: the encryption engine, keying information and operational procedures for the secure use. Almost every encryption program can be considered a cryptosystem because it has everything together in one package. The encryption engine is the part of the software that starts the encryption with the selected algorithm, and the keying system is the portion of the software that creates and sometimes manages the keys needed to encrypt and decrypt data. The operational procedures are how all of these parts interact and how the output or result is formatted. So, almost every encryption product is a cryptosystem. Thus we have a complete infrastructure of encryption programs, hardware and network connections. Algorithms used in encryption programs are symmetric and asymmetric. In symmetric algorithms is used only one key and in asymmetric ones are used two keys. Symmetric algorithms work much faster than asymmetric algorithms and some cryptosystems use both types in their software package. This is what we call a *hybrid* cryptosystem. Usually with this type of system asymmetric algorithms are used to exchange two keys between sender and recipient, and a symmetric algorithm actually does the encryption.

2. Encryption and everyday uses.

Businesses now rely heavily on the Internet and other forms of networks. Our personal data may be transmitted over un-trusted channels. Computers interact continuously with us and we need to protect very sensitive data. Let see some examples of everyday encryption.

- *Network logons and passwords*: When we log on to a network, either at home or at work we are asked for a User-ID or User-Name and a password. When PCs first appeared they didn’t have the capability of networking, so there was no need for such security. But when networking software became generally available, businesses realised the need to keep unauthorized users off the networks and to determine which sections of a network the staff were allowed to roam. The User- ID and password was the logical choice for controlling access. Because there are various networking applications not all the logon procedures were developed the same way. Some sort of encryption had to be used to protect the passwords because passing passwords from the user’s computer to the server in plaintext was not a good idea. Microsoft has a method called LANMAN (Local Area Network Manager) to store the passwords and this method is a weak one. If our system has LANMAN enabled and we don’t need it, we may just disable it.
- *Secure Web transactions*: When we purchase something online with our Web browser, we have interacted with at least one form of encryption. We should ensure that any web site we order from is using at least 128- bit encryption because otherwise, all of our personal information such as our credit card number or other data is probably being stolen. Prior to 1995, there was no technology in place to ensure secure Web transactions. Today it’s very easy to hijack a transaction between our computer and a Web site and we may be sending our credit card number to an imposter without even realizing it. In order to correct the problem of the Web sending and receiving data in the clear, some fixing had to be done to the HTTP protocol that handles the sending and receiving of data. S-HTTP (Secure HTTP) was created so messages and files could be sent encrypted. S-HTTP doesn’t actually provide the encryption; it just makes it possible for encryption to be added on. But not all Web browsers and servers can use S-HTTP. Another fix created to solve the security problem was the creation of SSL (Secure Socket Layer) that is designed to allow a secure connection between our browser and a Web server, and all data that travels between the two can be encrypted, not just individual messages like S-HTTP. SSL also doesn’t actually provide the encryption; it just makes it possible for encryption to be used. SSL has become a sort of standard, and all Web browsers and servers are capable of using it. There are two levels of encryption available: 40-bit and 128-bit. The bit is the size of the key and the longer the key, the better the security. SSL and S-HTTP have very different designs and goals, so it is possible to use the two protocols together – and some businesses and banks do use both. We will know when a secure connection has been established when a small key or lock appears in our browser’s status bar, and the URL has changed to “https” instead of just plain “http”. For example when we try to have a trial SSL certificate from

https://www.geotrust.com/ we note that we have https. This is shown in figure 1.Also we can examine Web site certificates to check that they are authentic to verify a merchant or bank’s identity.



GeoTrust

GeoTrust SSL Trial Certificate

Try before you buy...for free
The free* GeoTrust® SSL Trial offers a fully functioning SSL certificate. Now you can make a true evaluation of your SSL nee purchase.

GeoTrust SSL certificates help ensure that your customers' and business partners' information is secure when they use you site in minutes with the GeoTrust SSL Trial certificate, enabling up to 256-bit encryption."

Note: * – required.

* First Name

* Last Name

* Email Address

Figure1. SSL certificate

- *ATMs*: What we should do without ATMs nowadays! Banks have had to add much more physical security to their ATMs in the past few years. The magnetic strip on the back of ATM card contains a wealth of information that is picked up by the bank’s computers when we slide our card into the slot or in a merchant’s point-of-sold machine. One of bits of data on the strip is our encrypted account number. When we enter the PIN, our encryption key is compared to an encrypted account number to see if they match. If they do, we can continue with the transaction; if they don’t the machine doesn’t allow access. The implementation of encryption when handling transactions has to be good or the security can be breached. In 2001, two university student researchers in England found a huge hole in the way most systems were handling encryption of the account number. They found that the first four digits of the account number were always sent in the clear and they used this information to eventually get the 3DES key used for encryption, and so were able to demonstrate that they could crack up 7000 PIN-s per hour.
- *Music and DVDs*: This is such a normal thing to copy a DVD movie or to download music from the Internet, but sometimes this is impossible because exists such a thing like DMCA (Digital Millennium Copyright Act of 1998) that allows film and music companies to protect their copyrights with encryption. Each DVD player sold has a computer chip in it that contains a decryption key so it can read the encrypted portion of a DVD disc. The computer chip is also contains a country code that matches where the DVD player will be sold and used. When the DVD discs are made, a section of the disc is encrypted by the music industry’s proprietary system called *CSS* (Content Scrambling System). This system encrypts part of the disc with a country code — sort of like the country codes for the telephone system. One code is used for North America, another for the South Pacific, and so on. If we buy a DVD player in Japan and try to play a DVD bought in America, the disc won’t play. That’s because CSS is an access control system that prevents the playback of discs on players that don’t have the decryption keys that the movie industry provides to authorized manufacturers. There’s a man in Norway who owned some DVD movies and wanted

to watch them on a computer he built, but the computer did not have the ability to read the encrypted code on the DVD discs. So, he wrote a program he called DeCSS and installed it on his computer. So he could now watch his movies on his computer. He was so pleased with it, he put it on the Internet to distribute for free.

- *Communication devices*: There happened in so many cases that conversations over cell phones were not a secret because were listened by certain persons. The majority of cell phones in America have their phone numbers and voice transmissions encrypted, but only to a certain point. The part of the call between the cell phone and the tower is encrypted, but as soon as the conversation reaches your provider's gateway to the land-line phone system, it's decrypted. All land-line telephone communications (with the exception of government and military systems) are unencrypted. If you know how and where to place a gator clip and a phone receiver, you can listen in on anyone's phone calls. The GSM (Group Special Mobile) wireless phone is the standard in Europe and is the world's most widely used cellular technology. More than 215 million digital phones use it worldwide, including more than 100 million in Europe and 5 million in the United States. GSM transmissions are encrypted, but the A5/1 algorithm keys, which are used to scramble and unscramble the data, are much shorter than advertised and thus much easier to break.

3. Secure Communications

There are many ways that we communicate with others on computers, and most of those communications are not secured against secret listeners. Let see some of them.

Secure e-mail

E-mail sent in the clear can be read by someone other than the intended recipient. E-mail servers could be hacked and we need to encrypt e-mails because sometimes we have to do with very sensitive information that shouldn't be read from others. Also we need to ensure the confidentiality and safety of the informants. Given all cryptosystems available, e-mail encryption is probably the easiest and cheapest system to implement. By "easiest" system, we don't mean to imply that the setup is without problems, but it is very lot easier than setting up a full PKI system. PKI stands for public key infrastructure.

The two most common solutions for encrypted e-mail are S/MIME *(Secure/Multipurpose Internet Mail Extension)* and PGP *(Pretty Good Privacy).* MIME was created as a standard for transferring different types of files attached to e-mails, such as GIFs, JPEGs, DOC files, and so on. The *S* in S/MIME indicates a standard for incorporating secure encryption standards into the protocol. S/MIME works, but different e-mail clients use it differently, and the results are not always very good. On the plus side, S/MIME is cheap and is included in most e-mail systems and e-mail clients (such as Outlook and Eudora). We can set up S/MIME in Outlook Express and obtain the digital certificates needed to sign and encrypt our e-mail messages in cooperation with someone else to exchange messages with.

Because there are interoperability problems with S/MIME, it might be better to go with a vendor who has developed special implementations of S/MIME that have been altered to ensure better interoperability. Baltimore and ArcticSoft are two companies that come to mind with good products.

PGP was created by Phil Zimmermann at a time (1991) when the government was intent on keeping encryption technologies out of the hands of common people. At that time, the only legal use of cryptography was by the military or government systems. Today PGP is a corporate entity, and its use has become a type of standard and is probably the most widely used e-mail encryption software in the world.

PGP is available as freeware (Gnu PGP) or as commercial software (PGP Corp). It's an encryption and key-sharing protocol with a user interface to use with popular e-mail programs such as Outlook or Eudora. Another plus to PGP is that it has the ability to encrypt files and storage, where S/MIME does not have that capability. Two PGP versions to be considered are PGP International and GnuPG that offer free PGP programs available for different operating systems and platforms.

Instant Messaging (IM)

IM in its default installation not only introduces all kinds of security holes into our network, but almost anyone can read our messages. To the rescue are secure IM servers and clients. They are reasonably priced or sometimes even free, and some systems come with a secure IM server as well as secure clients. Some of the programs use symmetric key encryption while other programs allow us to use public/private key pairs (we encrypt with our private key; the recipient decrypts with our public key). If we use our own IM server, all text is encrypted as it travels across the wires and as it sits on the servers. If we are using a public IM server, we have to be sure we trust that server and find out what its security policies are.

Secure e-commerce

Any Web server that collects private information from customers should be considered an e-commerce server, and all possible protections should be implemented. Traditionally, only Web sites that conduct sales or financial transactions have been considered e-commerce servers. We buy an air ticket online or transfer some money; in both cases we do commerce and this has to be secure. Because of new privacy regulations, it may be in our best interest and our customers if we own a business to make our Web site more secure by using encryption. Encryption is an acceptable form of protection, but encryption of the data in transit is not enough. In short, SSL and S-HTTP are not good enough. We must encrypt the database and/or servers containing the information. In addition, if the information is stolen or released, we must notify people of the security breach.

Most secure Web servers use SSL and/or S-HTTP. Both of these options will encrypt the data as it travels across the wires to prevent the hijacking of information in the clear. On the other hand, these options do not encrypt the data that stays on the Web server or that is transferred to the database server. To be totally safe, we should encrypt the data on both the Web server and the database server. We have to implement the best security possible and to double-check our security policies and procedures.

Online banking

Online banking is just another form of e-commerce. We're collecting and disseminating personal information across the Internet. The Federal Gramm-Leach-Bliley Act of 1999 laid down regulations on safeguarding personal information collected, especially if the collecting is done online. In addition to protecting the data coming, going, and resting, we should also be making sure that the user logon IDs and passwords/passphrases are encrypted.

Virtual Private Networks (VPNs)

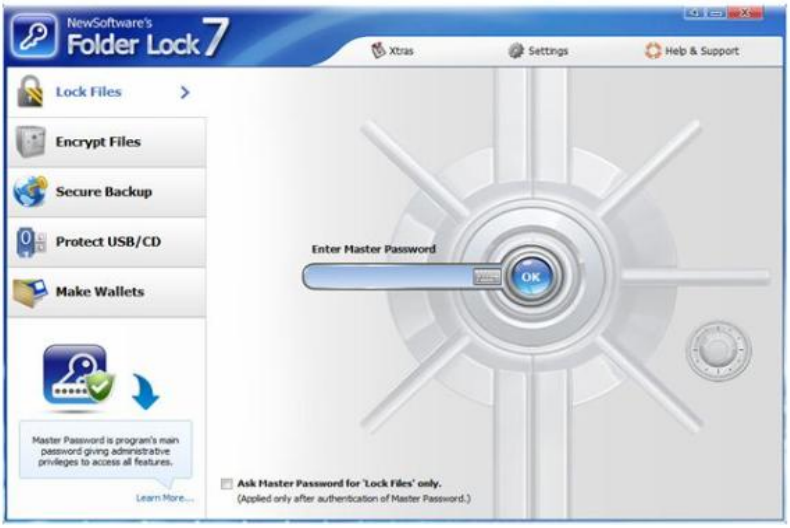
When businesses communicate over the Internet, there is no protection implied. Businesses began to see the need for a safer alternative as they did business with remote partners and employees in remote locations. Thus, the *Virtual Private Network* (VPN) was invented. VPNs use encryption to protect the traffic between any two points. It's like building a tunnel with special access controls between two different places. The tunnels aren't available to everyone. Before we can enter the tunnel, we must prove our identity, our packages must be of certain types, and the delivery address must be verifiable. VPNs have been around for enough years now to consider them a standard security mechanism. On the other hand, the way vendors create their VPN hardware and software is not necessarily interoperable. If we are communicating with someone who doesn't have the same sort of setup, it may take a few days or weeks of juggling cables and commands to gets it working correctly. VPNs are capable of encrypting two different ways: *transport* and *tunnelling*. The transport encryption sets up a secure, encrypted link across the Internet wires, and it encrypts the data we are sending to the other end. The encryption is invisible to the user — other than passwords, passphrases, or a special card to plug into the computer, the user doesn't have to press a button that says "encrypt" or "decrypt." The other form of VPN encryption, tunnelling, not only sets up a secure, encrypted link between two points, but it also encrypts the headers of the data packets. That's better. If we set up a VPN for our customers, business partners, and employees, they can gain some comfort in the fact that their data isn't travelling in the clear. VPNs are relatively easy to set up now, and we can usually find experienced staff to install and manage them. Sometimes it takes a little effort to get two different VPNs talking to one another, but that can be solved and many vendors are including VPN capabilities in their routers so the system is practically "plug and play." We just have to change the default settings such as the administrator password. VPNs are great at protecting the data in transport, but they do not encrypt the data on our drives, that data is still in the clear.

Wireless (In) security

The introduction of portable computers in the '80s was such a great thing on computer technology and today wherever we are we can connect to the Internet and surf the Web, with no wires, but for every advantage there is a disadvantage. That is very true for wireless networking. By default, anyone within radio wave distance can use our Internet connection and probably can hop on to our network. Shortly after wireless networking made its appearance, hackers created very small software programs that search the airwaves for unprotected wireless networks. If we have a look over the network lists of open wireless networks can be found on the Internet, and in some cases can be indicated where the network is located and what we need to do is to log on. This is called the wireless "insecurity." Wireless access points and wireless network cards are very easy to install. Wireless networks do have some security capabilities, and one of them currently in use is *WEP* (Wired Equivalent Privacy). WEP encrypts the packets going out over the air. It doesn't encrypt them particularly well, though, and much of the information about the network is sent in the clear. There are many hacker programs available that can crack the basic configurations of WEP, too. AirSnort and WEPCrack are two popular programs. Because WEP employs fairly weak encryption, we can add to the security by adding a VPN and an authentication process. This will greatly enhance our security, but we should never give a wireless network totally trusted status. Day by day there are appearing newer and more secure versions of wireless protocols, and we have more choices to make our data secure and safe. Or we just can buy totally secure, NSA-approved wireless access points.

4. Protecting data in storage

We now that is important to protect data not only during transmission but also in storage areas. There are several programs that can handle this and one of them is Folder Lock7 that is shown in Figure 2. Folder Lock7 is a program that is used to protect or encrypt files, folders, partitions, removable drives, USB-s etc. It uses the 256-bit AES algorithm to encrypt objects. Files, folders or drives are protected with a password.



Master Password is program's main password giving administrative privileges to access all features.

□ Ask Master Password for 'Lock Files' only.
(Applied only after authentication of Master Password.)

Figure2. Folder Lock7

Conclusions

We do different applications every day either at work or at home and the most important thing is to be careful with sensitive information. Banks or some other systems have implemented forms of security but what if we run our own business? If we have to cooperate with remote clients we need a website to be more successful but also we have to confront the idea that the risks are much more in getting the important data, especially client data and therefore we need a kind of protection. We have to be informed about the traditional forms of encryption and these are not difficult to be implemented but there are hardware-based solutions and software-based solutions implemented on different systems nowadays and we must be able to determine what kind of protection we need in our case. This protection has to be easy to set up, not very expensive and acceptable for our business. We can use some of the above solutions or we can set up a full PKI which requires not only a great work but also knowledge on servers, software and digital certificates.

References

1. Introduction to Cryptography Mark Vandenwauver Katholieke Universiteit Leuven, Laboratorium ESAT-Groep COSIC
2. Cryptography for Dummies by Chey Cobb, CISSP by Wiley Publishing, Inc.
3. Feistel. H, May 1973: Cryptography and Computer Privacy, Scientific American, Vol.228, no.5, pp.
4. Menezes A, Oorschot P.van and Vanstone S, Handbook of Applied Cryptography, CRC press (1996).
5. Schneier Bruce, Applied Cryptography 2nd edition, John Wiley & Sons [ISBN 0471128457].
6. http://journals.tubitak.gov.tr
7. www.crypto.com
8. www.cerias.purdue.edu