Proceedings of FIKUSZ '12 Symposium for Young Researchers, 2012, 161-169 pp Published by Óbuda University http://kgk.uni-obuda.hu/fikusz

How Kournikova can help to steal data?

Keszthelyi András, Ph.D.

Óbuda University, Keleti Faculty of Business and Management
Institute of Enterprise Management
address: H-1081 Budapest, Népszínház u. 8.
e-mail: keszthelyi.andras@kgk.uni-obuda.hu

Abstract: As not only the amount of data stored digitally in computers but our dependency of these data, too, increases day by day it is of critical importance to prevent unathorized data accesses. To gain access to other parties' data and, on the other hand, make it as hard as possible is (and has always been) a heavy fight between the data owners and the spies, only the tools have changed since ancient times. Https has become part of our everyday life as an excellent arm to protect the sensitive data of confidential communications from accessing our gmail mailbox to netbanking. Https is based on a two-key encryption standard which, according to the publicly known results of mathematics, cannot be attacked directly. In theory. In practice there exist roundabouts. In this paper I show a possible and low cost technical-organisational solution of such an attack which could be performed because of some malpractice of IT-managers: manipulation of top level certificates.

Keywords: data security, certificates, manipulating top level certificates

JEL code: L-86 Information and Internet Services; Computer Software

1 Introduction

At the very beginning of computer networking there were only 'real programmers1' around there, they planned the basic protocols and programs for themselves. Security in today's meaning was not a point of view at those times, for nobody thought that after a few decades everybody would be allowed to access the network. In other words: all the traditional network protocols are plain text ones, which means that all the communication data travel via the network as plain text, including user names and

[1] "The real programmer" is part of computer programmers' folklore to describe the archetypical "hardcore" programmer. See e.g. http://www.ee.ryerson.ca/~elf/hack/realmen.html

passwords. The http protocol our browser uses when surfing the internet is also such a protocol. [2]

Demand for secure communication arose very soon. There has been a lot of methods to hide, in other words to encrypt, the original meaning of plain text data. Computers with their high computational speed began a new era not only in data encryption but in data decryption and cracking as well.

2 Technical background

One-key encryptions may be 100% insoluble, at least in a mathematical meaning, but their big problem is that participants of the communication must change the key in a secret channel which means personal meeting practically. In modern business life there is no possibility for that.

Mathematicians have provided us methods without any need for a secure channel for key exchange. This simplifies the use of data encryption not only in business life but in private life as well. These methods use two keys for each participant one of which is the secret or private key and the other one is the public key. Any text encrypted with a key can be decrypted only with the given key's pair.

The first and best known method for two-key encryptions is the RSA-algorithm published in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT; the letters RSA are the initials of their names in the same order as on their paper. [7]

The first application which implemented the RSA-algorithm was developed by Philip Zimmermann in 1991. [8]

No need for a secure channel for key exchange is a great advantage, but it has its price: the two-key encryption algorithms are not 100% safe. They can be deciphered in certain conditions in *theory*, but in *practice* it would need unreal amount of resources.

Let us see an illustration for that: try to imagine doing some mathematics. Everybody can multiply two numbers in a reasonable time even if the numbers were very big ones. Let these numbers be two 100 digit primes. The multiplication of them can be computed relative easily. Having only the result of the multiplication try to do the prime factorization of it - it could be computed but it is beyond hope. According to new results in mathematics this may change perhaps in the near future, but this is not sure at the moment. [1]

2.1 “Man-In-The-Middle” attack

Instead of having unbelievable computational resources one might find some workarounds. There are a lot of different possibilities, one of which is the so-called MITM, the “man-in-the-middle-attack” or “monkey-in-the-middle” attack. This type of

attack is possible when the public keys are tampered with, i.e. the public key the user has belongs to someone else the user thinks. In this case the “man in the middle” can not only eavesdrop but even alter the content of the communication in a way that original communicating parties will not recognize. Just as in the following example:

A Spanish speaking bandit held up a bank in Tucson. The sheriff and his deputy chased him. When they captured him, the sheriff, who couldn't speak Spanish, asked the bandit, who couldn't speak English, where he'd hidden the money. "I will not tell it you", he replied in Spanish. The sheriff put a gun to the bandit's head and said to his bi-lingual deputy: "Tell him that if he doesn't tell us where the money is right now, I'll blow his brains out." Upon receiving the translation, the bandit became very animated. "I've hidden it in the churchyard under the oak tree", he answered in Spanish. The sheriff leaned forward. "Yeah? Well...?" The deputy translated: "He says he wants to die like a man."

Two-key encryptions have two main security rules of critical importance.

2.2 Basic security rules

The first rule of security is to keep one's secret key according to its name: in total secret. If someone gets some other one's secret key, he or she can read the messages sent to that person or make digital signatures in that person's name.

The second rule: When you use someone's public key, you must be sure it has not been tampered with. You may trust a new public key from someone else if, and only if, you got it directly from its owner (this would mean you have a secure channel for key exchange), or if it has been signed by someone else you trust. Make sure no one else can tamper with the public keys you collected. Maintain uninterruptible physical control of both the public key ring and your secret key and keep a backup copy of them. For more details and explanation see the original PGP documentation by Phil Zimmermann. [10]

2.3 Certificate authorities

Anybody can sign digitally documents which contain someone else's public keys and some identification data of its owner, let the owner be a private person or a company. These documents are called *certificates* and these people are called introducers. You collect signed public keys, or in other words certificates. "As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys." [10]

These introducers may be enterprises as well, for it is a good business opportunity to issue certificates for some fee, while the issuer enterprise has an efficient way to

distribute its own authentic public key in all over the world. Such an enterprise is called a certificate authority (CA). There are Cas which are worldwide known and a lot of them are local CAs.

2.4 Certificates and security

If you need security while using the World Wide Web you will you will use HTTPS protocol (Hypertext Transfer Protocol Secure), e.g. to reach the web-based services of your enterprise, or for internet banking etc. HTTPS protocol is a combination of the original HTTP and the SSL protocol which combination provides encrypted data traffic between the client and server computer first. Second, which is very important, too, the server computer is identified, because before providing any sensitive data, e.g. a password, we must know that we are connected to the right computer.

The identification of the remote computer is accepted when its certificate is digitally signed by someone else whom we trust, because to be trusted is a trasitive relation.

This is based on major CAs whose public keys come pre-installed in the web browsers software to be used for signature checking. In other words "I trust some certificate authorities (e.g. VeriSign Inc., Netlock Kft.) to tell me who I may trust"). So an HTTPS connection to a website, or better to say: to a remote computer, can be trusted if (and only if) all of the following two conditions are true:

a) The website provides a valid certificate which means it was signed by a trusted certificate authority directly or indirectly. It is possible that the biggest international CAs sign certificates for only the bigger CAs, bigger ones for the less ones, the less ones for the local ones etc.

b) The certificate identifies the website correctly (visiting https://uni-obuda.hu and receiving a certificate for "uni-obuda" and not for "uni_obuda.hu").

2.5 MITM

Let us suppose that there is something wrong with the certificate of the remote computer. In such a case the web browser running on the client machine will display an error message to inform the user about the security problem (“Unable to verify the identity of uni-obuda.hu as a trusted website”) and gives the possible reasons.

At this point the user has no possibilities to decide whether his/her browser talks to the real uni-obuda.hu server (and he/she has an outdated browser version which does not contain the appropriate top level certificate), or someone tries to personalize the uni-obuda.hu server to steal his/her password.

So user is warned but he/she has the right to click OK to go on whether because he/she checked the certificate of the remote computer e.g. by phone, or because is bored of the popup windows and would click automatically OK to anything.

This means that if someone wanted to do a man-in-the-middle attack, he or she ought to solve two problems. First he/she ought to hijack the normal data traffic to his/her pirate computer. There are a lot of technical possibilities for that, I described one among them in [4]. The so-called Kaminsky-bug is another real threat as well, as it is investigated in [9].

The second problem such an attacker ought to solve is to make the user click OK for the browser security message. Users will probably click OK e.g. if they are accustomed to the situation when the often used server has no valid certificates (as it was the situation in 2009 at our university with the Neptun server). This makes possible a mass attack because all the colleagues and students clicked OK at those times, I'm afraid.

Or, which is better from the point of view of an attacker, he/she has to make the browser not display the security message at all.

3 Avoiding the security message in case of a MITM

To avoid the security message being displayed is impossible, of course. Of course, once again, it is impossible in case of the normal flow of operation, so it needs to tamper with the certificates stored in the user's computer.

The store of the certificates may differ regarding the operating system, browser and their version. Firefox browser, e.g., stores its certificate database in the users' profile folder. This means that in most cases they are stored in user space because users need to manage their certificates, and different users may have different set of certificates.

The security message will not be displayed if the fake server's certificate is signed by a trusted CA or it has been validated by the user i.e. he/she accepted the given certificate permanently when the security message was displayed, or he/she has imported the certificate into the browser as a trustable one.

So the question is: “How can an attacker tamper with the certificates stored in the user's computer?”

There are a large number of possibilities to do that, history of computer security is full of tools (and counter-tools, of course) to tamper with the remote user's files. In general: a remote user's file may be tampered with via:

a) software bugs,

b) security holes in softwares,

c) social hacking (by convincing the user to install some updates manually e.g.),

d) any kind of other dirty tricks which makes the user click (see Kournikova type e-mail viruses).

Let us see how Kournikova virus worked (or works in case of not having an appropriate antivirus software). User received an email from a friend or colleague which said “See this” and user found attached file Kournikova.jpg. When he clicked on the attachement, due to default settings the Kournikova.jpg.vbs script was executed by the VisualBasic interpreter instead of displaying a picture of Anna Kournikova.

So if an attacker wanted to carry out a targeted attack first he/she would have to fire up a pirate server having a self-signed certificate, which certificate, of course, would not be accepted by any browsers. Next he/she would have to put the certificate of the pirate computer into the collection of trusted certificates in the targeted user's computer.

As for the first step there are known possibilities, as described in 2.5. To make certificates, including self-signed ones is possible for anyone with the appropriate certutil software tool.

As for the last step, to make a small program run on the targeted user's machine, there are so many possibilities, that a motivated attacker probably will find the successful solution, especially on the ground of the human (stupidity;) factor. As I have just checked, the virus scanning software of our university lets bash shell scripts through without any remarks.

This possibility of tampering with certificates is a serious security risk. Companies ought to take this threat into consideration more seriously. In the first 20 results of a google query (certificate “information security regulation” in Hungarian language) there are no relevant links. In the IT security regulation of our university, too, there is not a word about certifications and their management.

4 A possible solution

How we could get rid of this threat? Locally stored certificates must be owned by the system administrator, i.e. must not be writeable by the normal user. This implies that in everyday life users use the personal computer as restricted users and not as system administrators. At enterprises this is the preferred way of operation (system administrators do not want extra work for themselves), but private users at home usually use their computers as superusers because of convenience.

In case of companies IT security regulations should contain the rule of restricted users and the rule of superuser owned certificate files as well as the regulation must define the process of importing new certificates for the restricted users.

In private life, at home, these basic rules ought to be applied, too, without any written IT security regulations.

5 Teaching and learning

In our age, which is called information age, it is very important to teach not only theoretical stuff but practical examples as well. As not only the amount of digitally stored data increases day by day, but our dependency of these data as well, IT security is one of the most important fields both in private and business life.

As a teacher I have to call the attention that the above discussed problem is not only the problem of the IT sector but that of the education as well, not only in general but in specific fields, too. Not only because https protocol itself is used in education widely (scholar information systems) but because even teenaged children may be in danger if they do not know what they do when they use the https protocol (facebook.com, gmail.com e.g.). The young generation ought to learn the theoretical background as well as the practical applications. You cannot call the students' attention to such problems too early, because investigating the skills and knowledge of the students in the fields of computer sciences not only in Hungary but in Central Europe as well we find an alarming situation. [5] [6]

Data security and legal data protection are in close connection with each other. Personal data must be protected according to Act. CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act"), especially in case of personal data concerning health, addictions etc. To understand and perform global telecommunication and its tools and the protection of personal data needs specific professional skills in health sector, obviously. [3] So it is very important in the entrepreneurship education to the health sector to see problems and methods of critical importance.

6 Summary

It is very important to keep the confidentiality of our sensitive data. The HTTPS protocol, based on the RSA-algorithm, and certificates are strong and excellent tools to secure the data traffic between a web server and the client machine and to prove that the server is the real and legal one. The browser (in the name of the user) will believe the identity of the server if the server's certificate can be checked by one of the locally stored top level certificates at last. The most important security rule would be to store these certificates in a secure way. Instead of this in case of typical installation of the operating system(s) and the browser(s) the top level certificates are stored in a rather simple way: in user-writeable files.

An attacker can tamper with the content of this file either by using some software security bugs or by making the legal user do a mouse click or press an enter. If the attacker succeeded to insert a fake certificate into the local certificate database (s)he may be able to carry out a targeted man-in-the-middle attack in such a way that the

user's browser will not realize that. In such a case either the password of the user may be stolen or the content of the data traffic may be observed and altered.

To prevent this attack users ought to realize the importance of keeping the certificates in a secure way, for wich purpose a user-writeable file will not fit. The minimal precaution would be to change the ownership of the file(s) containing the certificate database from user to sysadmin without write access for the user.

As far as enterprises are concerned in data security they ought to declare this rule in their official IT security policies as the least step. They may think of not using top level certificates at all, too.

References

[1] Ball, Philip: Proof claimed for deep connection between primes. Nature.com, 10 September 2012. http://www.nature.com/news/proof-claimed-for-deep-connection-between-primes-1.11378 http://index.hu/tudomany/2012/09/12/meglehet_a_primszamok_kozotti_kapcsolat/

[2] Fielding, R. - Irvine, UC - Gettys J. - Mogul J. - DEC - Frystyk H. - Berners-Lee T.: Hypertext Transfer Protocol - HTTP/1.1. MIT/LCS, 1997.; http://www.rfc-editor.org/rfc/rfc2068.txt

[3] Garaj, E.: Using of Moderation Techniques to Develope the Entrepreneurial Skills in Health Education. Practice and Theory in Systems of Education, Vol. 5. Number 2., 2010, pp. 145-162, HU ISSN 1788-2591 (Online) HU ISSN 1788-2583 (Print) http://www.eduscience.hu/

[4] Keszthelyi András: Price, Value and Security. How to Manage a Database on sy's Own. Proceedings of FIKUSZ'09 – Symposium for Young Researchers, Budapest Tech – Keleti Károly Faculty of Economics, Budapest, 2009., pp. 109-119.

[5] Kiss, G.: Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course / TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4. ISSN: 2146 – 7242, pp. 222-235.

[6] Kiss, G.: Comparison of the Programming Knowledge of Slovakian and Hungarian Students / Procedia of Social and Behavioral Science Journal különszám, ISSN: 1877-0428, p. 10. (accepted)

[7] Robinson, Sarah: Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. SIAM News, Volume 36, Number 5, June 2003. pp. 1-4.

[8] Schneier, Bruce: Applied cryptography: Protocols, algorithms, and source code in C. Wiley & Sons, New York, 1996. (2nd ed.) pp. 265-301.

[9] Süttő, Dániel: DNS monitorozó eszközök vizsgálata a .hu Top Level Domain környezetében. Diplomamunka, Pázmány Péter Katolikus Egyetem, Információs Technológiai Kar, Budapest, 2012.

[10] Zimmermann, Philip: The official PGP user's guide. MIT Press (Cambridge, Mass), 1996. ISBN 0262740176. Originally part of the PGP programpackage: ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf pp. 47-50.