Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks*

Zbigniew Gołębiewski, Mirosław Kutyłowski, and Filip Zagórski**

Institute of Mathematics and Computer Science,
Wrocław University of Technology
{zbyh, mirekk, filipz}@im.pwr.wroc.pl

Abstract. We present very simple kleptographic attacks on SSL/TLS and SSH protocols. They enable a party, which has slightly manipulated the code of a cryptographic library, to steal secrets of the user. According to the scenario of the kleptographic attacks the secrets can be stolen only by a party having a secret key not included in the manipulated code. The attacker needs only to record transmissions. The messages transmitted are indistinguishable from the not manipulated ones (even for somebody that knows the kleptocode inserted). Therefore, detection of infected nodes based on communication analysis is much harder than in the case of classical subliminal channels.

The problems are caused by certain design features of SSL/TLS and SSH protocols that make them vulnerable for a kleptographic attack. We propose changes of these protocols that make them immune against this threat while all previous security features remain preserved.

Keywords: kleptography, SSL, TLS, SSH.

1 Introduction

Security of communication in public networks should be guaranteed by appropriate cryptographic protocols. They have to ensure that a malicious eavesdropper monitoring communication, inserting and deleting packets exchanged between two parties cannot achieve more than interrupting communication. It must be assured that the malicious eavesdropper can neither learn the contents of protected messages nor can change them or insert fake messages. Achieving these goals is absolutely necessary for instance for e-banking, e-voting via Internet, and generally for any legal actions which are performed on electronic way.

The SSL/TLS [] protocol is often claimed to be a universal remedy to all problems mentioned. This is particularly the case, when security system is presented to the consumers. The issues of security of home PC's are neglected. The problem of computer viruses is often discussed only on the level of crushing a PC. The issue of malicious viruses that perform an attack and try to remain hidden in the system is rather underestimated.

* Partially supported by Polish Committee for Scientific Research grant 3 T11C 011 26.
** Contact author.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 191–202, 2006.

1.1 Basic Threats

One of the major issues of security is that the system installed may already contain hidden *features* that are used by malicious producer to get information about the user and his activities. The cases of such an attitude have been reported, while probably most of the cases remain unknown to the public. As long as the source codes of an operating system and application programs remain hidden, it is quite easy to hide such features in a compiled code.

There are chances to uncover such activities by monitoring communication by a computer. Contacting remote servers by a computer without ordering such communication by the user might be a trace of malicious activities. The monitoring must be performed by an independent server, for instance by an appropriate gateway. In many cases a user has limited possibilities to perform such an analysis.

But the attacks against the user may be performed in a much subtle way. The critical information like cryptographic keys, seeds to pseudo-random number generators, may be encoded in a perfectly legal messages which are transmitted according to the protocol. Attacks of this kind are known to such basic cryptographic algorithms as Diffie-Hellman [4] key exchange or generation of RSA keys. In this case only a party knowing a secret key used to mount a subliminal channel may view the hidden messages. Note that the subliminal channel, based on steganography are more fragile with this respect. While slight modifications in digital pictures are allowed and may serve as a method of destroying the hidden data, a manipulation of cryptographic data exchanged by a protocol should lead to negative verification.

In the case of subliminal channels disseminating information might be a problem. Once a malicious code is detected it may be used by anybody to get access to information from the subliminal channel.

1.2 Kleptographic Attacks

Young and Yung presented kleptography [11,12,13], which is a technique to attack cryptography using cryptographic methods. Their attack is based on modifications of standard algorithms executed by a device or a software product. Malicious *kleptographic* code inserted into such a system leak the secrets of the user. The data transmitted as in an analogous way as for a subliminal channel. The main difference is that

- encoding for a kleptographic channel requires a public key contained in the kleptographic code,
- decoding information requires a private key that is not present in the kleptographic code.

So, a malicious party needs only to intercept transmission from a contaminated system. Nobody except him can make use of the kleptographic channel, in particular, reverse engineering and detecting kleptographic code does not provide access to the channel. Last not least, as in the case of subliminal channel, the