MANAGEMENT, PROCESSING AND ANALYSIS OF CRYPTOGRAPHIC NETWORK PROTOCOLS

Bradley Cowie[1] and Barry Irwin[2]

Security and Networks Research Group
Department of Computer Science
Rhodes University
Grahamstown, South Africa
[1]g06c5476@campus.ru.ac.za , [2]b.irwin@ru.ac.za

ABSTRACT

The use of cryptographic protocols as a means to provide security to web servers and services at the transport layer, by providing both encryption and authentication to data transfer, has become increasingly popular. This is due to a number of factors, including the declining computational cost of cryptography relative to the computational power available; the popularity of wireless communication protocols; and the emergence of information services as a major industry. However, we note that it is rather difficult to perform legitimate analysis, intrusion detection and debugging on cryptographic protocols, as the data that passes through is encrypted. Furthermore the use of HTTPS as an attack vector chosen by malicious individuals is of serious concern, as it could be difficult to monitor these sorts of attacks. In recent months, a number of new and interesting ways to exploit SSL have been revealed mostly using new variations on the MITM attack, which is particularly important in the light of the 2008 Debian openSSL fiasco. As websites increasingly make use of SSL/HTTPS security, they are in effect locking themselves out of being able to monitor their traffic for any kinds of attacks performed over this channel.

In this paper we assume that we have legitimate access to the data and that we have the private key used in the transactions and thus we will be able decrypt the data. The objective is to produce a suitable application framework that allows for easy recovery and secure storage of cryptographic keys; including appropriate tools to decapsulate traffic and to decrypt live packet streams or precaptured traffic contained in pcap files. The resultant process-

ing will then be able to provide a clear-text stream which can be used for further analysis. The framework should be implemented for protocols that use the standardized hybrid cryptographic protection system such as TLS, SSL 3.0 and SSHv2. These protocols constitute the bulk of encrypted traffic commonly seen today. An issue of concern is the recovery of the nonce, which could either be retrieved by changing the server applications or more practically by having another trusted system holding a second copy of the private key. An investigation as to how to sensibly store cryptographic keys is also required as they form a central component of this system. Existing systems relating to this problem are lacking in cross-platform compatibility; or are protocol specific; or handle the front of the communication and pass requests to the servers in clear-text, which would not be acceptable in split data centers. Ultimately this sort of software could be used in industry to allow for improvements in the use of cryptographic protocols. Development of new systems should be encouraged to use cryptographic methods from the beginning, rather than only implementing them as an afterthought.

KEY WORDS

cryptographic protocols, development framework, analysis

MANAGEMENT, PROCESSING AND ANALYSIS OF CRYPTOGRAPHIC NETWORK PROTOCOLS