Project Proposal

Computer Science, Rhodes University

02 March 2009

1 Project Title

The proposed project is entitled :
Management, processing and analysis of cryptographic protocols

2 Probelm statement

The use of cryptographic protocols as a means to provide security to webservers and applications at the transport layer is becoming increasingly popular; however it is difficult to analyase traffic this sort of traffic as it is encrypted. We note some cases of this :

- ISP's are often served with court orders to provide logs of clients activity; but this data is often encrypted.
- Attacks that use HTTPS as their means of entry are harder to detect once again as they are encrypted. "Increasingly Sophisticated Web Site Attacks - Especially On Trusted Web Sites"
- Its often difficult to debug errors related to cryptographic protocols once again due to the encrypted nature of the data

We note that there is a need for a set of unified tools to decrypt encrypted data and perform anaylsis of this data. We approach the probelm from the perspective that we have legimate access to the encrypted data (whether it be stored or live) for analysis and decryption. We further assume that access to the stream will be available to ensure that initial exchanges can be analysed.

3 Objectives of research

Gain knowledge in the use of tools used for analysis of cryptographic protocols such as modSSL, SSLDump and TCPDump

Given encrypted data in the form of stored pcap files (extending to live pcap streams) can we determine the algorithm used and then together with the recovered session key to decrypt to plain text. Of course the algorithm used for encryption is dependant on the protocol used and the algorithms that were negotiated between client and server. This system needs to be both unified and cross-platform.

- Develop a means to store temporal keys such that they aren't in danger for a long period of time .
- Given diffirent decrypted data and the key and algorithm used; the data must then be decrypted to plain text.
- Provide some analysis of the data
- Provide implementation for SSL, TLS and SSH at the minimum.
- Extend for a number of diffirent protocols and application

4 Relevance and background

A protocol is a set of rules and regulations that govern the transmission of data over a network. Cryptographic protocols are protocols that use cryptography to distribute keys and authenticate the participants involved to ensure that data in an attempt to ensure that data is transfered over a network safely. The network is usually assumed to be hostile, in that it may contain intruders who can read, modify, and delete traffic, and who may have control of one or more network principals[3]. Protocols are probably the most difficult part of cryptography[6]. A cryptographic protocol must be able to achieve its goals in face of these hostile intruders.

SANS one of the most respected Information Security trainers and certifiers released a list of the top 10 security menaces for 2008 (compiled by 10 security veterans). The number 1 security menace for 2008 was :

"Increasingly Sophisticated Web Site Attacks - Especially On Trusted Web Sites"

"..web site attacks have migrated from simple ones based one or two exploits posted on a web site to more sophisticated attacks based on scripts.. attackers are actively placing exploit code on popular, trusted web sites where users have an expectation of effective security"

5 Project Design

5.1 Phase One (Preparation phase)

During phase one a large amount of research will be done on the protocols involved; flowcharts/pseudocode of each are to be designed to provide a better understanding. A revisiting of the choosen language to be used for development to allow for quick and efficent development. Installation/configuration of any software that is required will be completed in the phase. Data sets are to be selected for later analysis.

5.2 Phase Two (Experimentation phase)

Experiment with generation of SSL certificates using openSSL (possibly other means aswell). Experimentation with modSSL and openSSL to find anything of use. Investigate SSLDumper to see whether it can be used to reclaim public keys. Investigate a means to store the symmetric keys effectively.

Figure 1: Proposed system design flowchart

5.3 Phase Three (Implementation Phase)

Develpoment of the web based interface and individual tools needed. Firstly a means to store the symmetric keys must be developed. Methods to extract a public key from a data stream need to be developed together with algorithms to decrypt the encrypted dependant on which algorithm was used to encrypt the data. A means to determine what algorithms were used in the encryption.

5.4 Phase Four (Extension Phase)

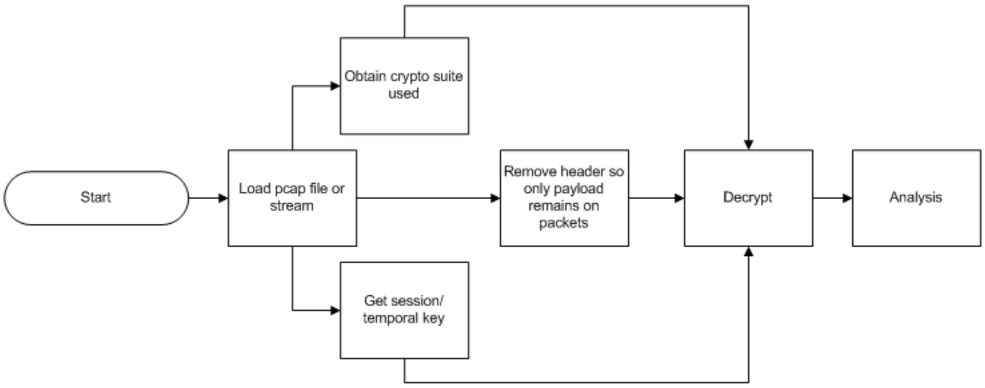
If phase three was completed in a short period of time then it may be possible to consider other excluded protocols/applications; this would require a reiteration of phase two and phase three.

5.4 Phase Five (Analysis Phase and Testing Phase)

Extend the program to provide statistics etc.

6 System Overview

The system is proposed as follows; intially the system will be started; it will then be pointer to a pcap file or a alternatively a live pcap stream. The cryptographic suite used will be obtained by inspecting the intial transactions made bewteen the client and server. The session key will also be extracted by observing the traffic sent. The private key we assumed in the probelm statement will be provided. The header will then be removed from the packets leaving payload. Using the temporal key, private key and knowing what algorithm that was used to encrypt the data; decryption will then occur. The plaintext will then be analysed appropriately.


Obtain crypto suite used
Start
Load pcap file or stream
Remove header so only payload remains on packets
Decrypt
Analysis
Get session/ temporal key

7 Timeline of Project Progression

Week	Activity Description
09 March - 15March	Develop project website using a CMS
16 March - 29 March	Gain proficiency in tools to be used (openSSL)
30 March - 20th April	Produce draft literature review
21April - 27 April	General investigation of cryptographic protocols

4 May - 11 May	Investigate methods of storing temporal keys
18 May - 25 May	Investigate methods of decrypting SSL
26 May - 4 May	Investigate methods of decrypting TLS
5 May - 11 May	Investigate other protocols like SSH
12 May - 26 May	Package decryption methods into tools and test them
27 May - 1 June	Finalise Literature review and hand it in
2 June - 12 June	Examinations
14 June - 27 July	Develop front end for system and begin testing
28 July - 9 August	Implement analysis into system and inspection of code
10 August - 1 September	Extend to other protocols
2 September - 7 Septemeber	Develop thesis outline
8 Septemeber - 13 September	Draft of short paper on thesis
14 September - 30 September	First chapter drafts
1 October - 9 November	Hand in thesis

References

[1] Bruno Blanchet. Automatic verification of cryptographic protocols: A logic programming approach. 2003.

[2] Ran Canetti. Security and composition of cryptographic protocols: A tutorial. 2006.

[3] Catherine Meadows. Formal methods for cryptographic protocol analysis : Emerging issues and trends. 2003.

[4] Alan Paller. Top ten cyber security menaces for 2008. 2008.

[5] Schneier. *Applied Cryptography*. Wiley and Sons, 1996.

[6] B. Schneier and N. Ferguson. *Practical Cryptography*. Wiley Publishing, 2003.

[7] Sun and Wang. An approach to finding the attacks on the cryptographic protocols. 2000.