Synopsis of Security: Using Kerberos Method to Secure File Transfer Sessions

Fadi Al-Ayed
School of Electrical Engineering and Computer Science
The Catholic University of America
Washington D.C. 20064. USA
93alayed@cua.edu

Hang Liu
School of Electrical Engineering and Computer Science
The Catholic University of America
Washington D.C. 20064. USA
liuh@cua.edu

***Abstract*— Secure file transfer sessions in File Transfer Protocol (FTP) is becoming an essential process of prevention and detection the intrusive behaviors nowadays. In this paper, we propose scalable stochastic fingerprints to secure and classify encrypted traffic in File Transfer Protocol (FTP) using Kerberos method instead of Secure Sockets Layers (SSL) method. On the first part, we define Kerberos method and its operational objectives which implemented in the server side of the FTP application. Additionally, we illustrate the strengths of using Kerberos approach and show why it is more efficient than SSL. On the second part, we demonstrate the concept to further improve intrusion detection in FTP by using the machine learning Markov model to evaluate and analyze the Kerberos parameters as its basic model structure having the concept that in a sequence of states. Lastly, we show the effectiveness of the Kerberos technique which results in a very good accuracy of application security.**

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General-Security and Protection; C.2.2 [**Computer-Communication Networks**]: Network Protocols

Keywords

File Transfer Protocol, Kerberos, Markov Model, User Sessions

1. INTRODUCTION

Many government sectors, industries, and banks are continuously using the traditional on-premise type of exchanging data remotely vial File Transfer Protocol (FTP). The main benefit of using FTP is to directly transfer data from the server for the clients' machines and vice versa, but are prone to intrusions. Cyber security, however, is one of the many concerns that is required to be tackled. Identifying what type of the encrypted traffic is a key challenging matter due to the growing and developing new type of applications that threatens the security of all users [2]. File sharing process between the server and client(s) is prone for attacks by illegally obtaining important information or data. Secure Socket Layers (SSL) is one such technology that establishes a decent connection between server and client(s) using an encrypted technique. File Transfer Protocol (FTP) refers to the protocol commonly used between client(s) and server to transfer all type of data over the internet. Most often, FTP uses SSL as its standard security authenticator [4]. Kerberos Authentication (KA), however, which is a security technique similar to Secure Sockets Layers (SSL), has a strong encrypted security protocol that deals with establishing a secure connection using more encryptions steps between the client(s) and the server.

Kerberos is known as a cryptographic approach in the computer network communications precisely catered for exchanging data between a client and a server. It intentionally helps in building a trusted and more secure connection for FTP applications. The core initiative behind Kerberos is to avoid sending password by using a ticketing system that hashes the password and sends it on both sides, server and client(s) for authenticity purpose. The Kerberos tickets has added validity of the requested ticket known as a timestamp on the encrypted hash since Kerberos depends on time synchronization between two sides, and having a clock time not more than twenty five minutes [3].

Although similar, in our analysis and evaluation - it has proven that Kerberos is more stronger or efficient than SSL in FTP since Kerberos Protocol uses a secured and trusted server as a mediator in the server side to build a mutual trust between the client(s) and server as an alternative of using a public key cryptography - digital certificate handled by SSL to make the client(s) believe that the server it is trying to connect to is what it intended to connect to. Even though Kerberos could also work using a public key cryptography [3]. Kerberos mediator is known as the Key Distribution Center (KDC) and it is the one that establishes and depends the Kerberos's tickets used by the server and clients which is aiming to produce a strong secure connection.

Kerberos works by using a sequence of encrypted messages between the server and client(s) to prove that each client is a real user. To be more specific, Kerberos has knowledge of a secret key or encrypted key that is known by only the client(s) and the authentication server and desires to be authenticated within a certain time frame. In view of the fact that the encryption and validation procedures of the keys between both the server and client(s), Kerberos provides a more secure and reliable connection than SSL.

978-1-5090-5510-4/16 $31.00 © 2016 IEEE
DOI 10.1109/CSCI.2016.193

The rest of the paper is structured as follows. In section 2 we describe some of the related work and previous techniques used in Secure Sockets Layer to disseminate information on File Transfer Protocol. In section 3, presents a methodology applied in this paper and our conceptual analysis approach. In section 4, presents the discussion. Finally, we conclude and future work in section 5.

2. RELATED WORK

Many researchers have examined the classification flows of the encrypted traffic and methods of encryption protocols such as Secure Shell (SSH), and Secure Sockets Layer/Transport Layer Security (SSL/TLS) [13], [14], [15]. Bissias et al. presented a traffic analysis attack against encrypted HTTP streams to identify the source of the traffic by analyzing distributions of packet sizes and inter-arrival times of web requests from interesting sites [12]. In our work, however, we show that it is conceivable to effectively control the encrypted flows by inspecting each Kerberos components' parameters in FTP.

Levillain et al. evaluated the practices of SSL/TLS servers by inspecting server replies [16]. They considered the details of the encryption parameters, for instance, cipher suites, session's key sizes, and protocol characteristics such as modernized versions and their extensions. Our work is an advance step in this direction.

Korczynski et al. presented stochastic fingerprints for several applications in Secure Socket Layer/Transport Layer Security (SSL/TLS) sessions based on the homogenous Markov Chains for effective network classifying traffic tunneled through SSL/TLS [1], [2]. Their datasets consist of only SSL/TLS encrypted traffic produced by standard services such as Web, while our work is to enhance the traditional way.

3. METHODOLOGY

In this section, we describe methodology approaches used in this paper including the conceptual analysis.

3.1 Kerberos

In this section, we describe Kerberos method and its operational objectives. To define what Kerberos is, it is a powerful authentication protocol comparable to Secure Sockets Layers (SSL) with a slight difference. Kerberos utilizes the mediator to both authenticate the credibility of the client(s) and the server [7], as shown in Figure 1.

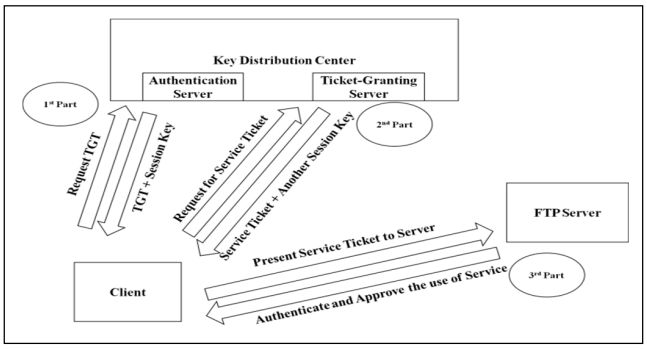

Figure 1 Kerberos Diagram

Figure 1 illustrates the structure of Kerberos and its three main parts. The detailed description of the operational flow of each three components is shown below:

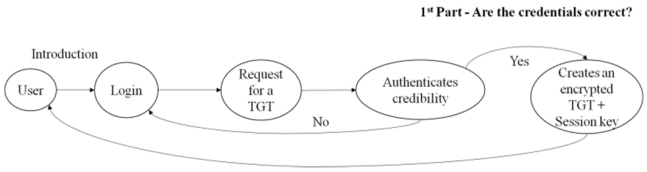

Figure 1.1 Credentials Diagram (1st Part)

In Kerberos, the client first sends a greeting to the Key Distribution Center (KDC) with its username to request a Ticket Granting Ticket (TGT) from the KDC, tickets do expire as a result tickets have a time stamp on them. The KDC searches for the desirable username of the client in the database and confirms it. Once confirmed, it produces the requested ticket and sends it back to the requesting client. The produced ticket consists of the client ID, name, IP address, and session key. The session key is a time stamps generated encrypted key assigned for. The requested ticket is encrypted and can only be read by the KDC.

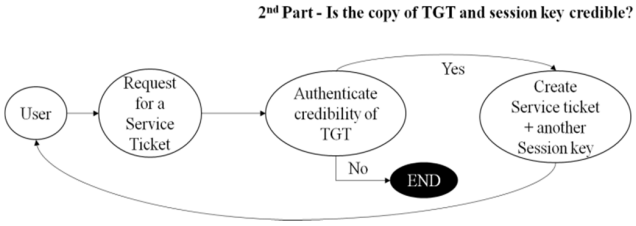

Figure 1.2 Credibility of TGT Diagram (2nd Part)

Once the client sends a request to use a service, the client sends the KDC an authenticator that consists of the client's ID, name, client's IP address, and timestamps. After that, it encrypts the authenticator with the session key produced by the KDC. Once the packet for request to use a service that has been sent to the KDC, the KDC then reads the ticket produced for that client to authenticate its credibility and if it's legit,

approves the request and sends the service ticket to permit the client to use the service.

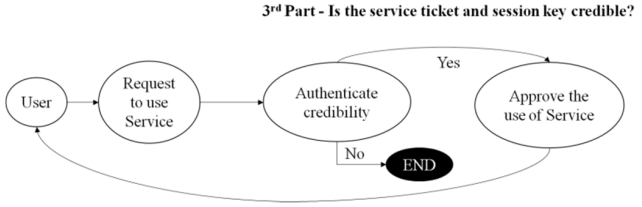

Figure 1.3 Service Ticket & Session Key Credible Diagram (3rd Part)

Kerberos generates a strong secure authentication, handles password management, and the convenience of a single sign-on feature that allows the clients to sign-in to use any services. Therefore, it is noticeable that there is no chance in time that the client's password and services can be obtained by anyone else, since everything has been maintained and handled by the Key Distribution Center (KDC).

3.2 Markov Model

Markov model uses a sequence of possible states that the probability of each state transition will only depend on the previously chosen state [5]. The idea is that a Markov model decision capable to detect intrusion because of the sequencing of possible states. These states are representing the parameters of the Kerberos as shown in figure 1. For instance, relying on the correct transition of the states if one does not know or made a mistake towards the correct state path, an alert will be issued and a termination action will be occurred. The system is also capable to identify the connection as a non-trusted connection and will be treated as unsecured and be dropped off. However, Markov model consists of the initial probability, transition probability matrix, and termination probability distribution.

Markov Property: Assume that discrete-time random variable X_t, for any $t = t_0, t_1, ..., t_n \in T$. It takes the observed values in the Kerberos parameters per state. Consider that $P_{i,j} \geq 0$ for all i, then

$$\sum_{j=1}^{n} Pij = \sum_{j=1}^{n} P\,(Xt + 1 = j \mid Xt = i) \qquad (1)$$
$$= 1$$

Based on the formula (1), in state *i,* the next state transition is most likely be one of the possible state probabilities. So when adding all possible values *j*, which should be one of the many possible states that the rows of any state is equal to one [10].

The state transition matrix $P = (P_{i,j})$ is shown below:

$$P = \begin{pmatrix} P11 & P12 & \cdots & P1n \\ P21 & P22 & \cdots & P2n \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ Pn1 & Pn2 & \cdots & Pnn \end{pmatrix} \qquad (2)$$

Markov Notation: The Markov can be divided into three categories: input, process, and output as shown in Figure 2.

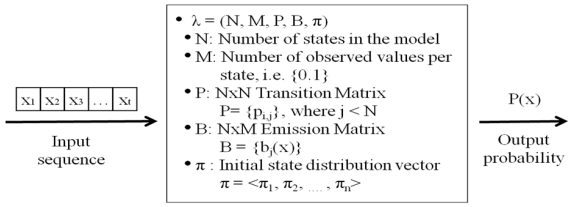

Figure 2 Markov Notation

First step is to create the state transition matrix by inputting the values of the Kerberos parameters for each state. After identifying the values for each state, substitute the values to the formula in order to get the percentage [11]. To calculate the percentage in each states transition, utilize the state transition matrix or transition probability matrix, which calculates the probability of each state transitioning [2], [10].

However, the parameters of the Markov model would be based on the Kerberos that consists of a sequence of states. The identification of the six parameters of the Kerberos requests flow can be presented as the following table 1:

SID	Description
11:	Request for TGT
12:	TGT + Session Key
13:	Request for Service Ticket
14:	Service Ticket + Another Session Key
15:	Present Service Ticket to Server
16:	Authenticate and Approve the use of Service

Table 1 Parameters Identification of the Kerberos

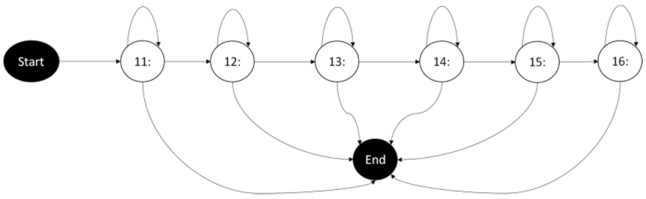

Figure 2.1 Fundamental Model of Kerberos Architecture

As shown in above Figure 2.1, Start state is the initial state and End state is termination state. Each state can be terminated if a problem occurs while performing the authenticating process of Kerberos such as connection breakdown, and users' wrong operations and it stays on itself only waiting for confirmation of the next request validity. The relationship per transition from itself to either moving forward (verification being successful) or just terminated (verification being unsuccessful). However, all users' activities are recorded into the log file and Markov transition values are obtained from the log file of many users.

4. DISCUSSION

Secure Sockets Layer (SSL) structure contains of a Record Protocol, Handshake Protocol, Application Data Protocol, Change Cipher Spec Protocol, and Alert Protocol [1]. Over the century, however, attackers yet keep on attempting to find ways to bypass security protocols. In Secure Sockets Layers (SSL), hackers have developed several ways to break the SSL Protocol. One of the classic trick that they use to gain access is tricking a user to accept a fake certificate, a SSL certificate is used to start a secure connection with a browser. Other ways include, obtaining valid certificates, using a tool to act as a proxy that removes the security, using tools to crack the encrypted key, and eavesdropping or sniffing, making independent connection with the victim and acts like a mediator between the client and the server [8].

To prevent and detect, one way is to regularly monitor the logs or records in order to detect any malicious activities within the server system. Another way to detect and prevent future attacks is to study how the attackers operate, by figuring out the method they are using; then must configure the machine with the necessary counter for the attacks. This allows the users to detect incoming attacks that uses the same configuration in the future [9]. Talking about applying Kerberos method [7] with Markov chain [2] in detecting intrusion attacks, using Kerberos method protocol will allow the possibility to detect and stop the attack completely.

What makes Kerberos more powerful than SSL is the fact that the only way for an attacker to bypass Kerberos protocol is to have access to the main Kerberos Server (KDC) as shown below by the Figure 3.

Kerberos versus SSL/TLS

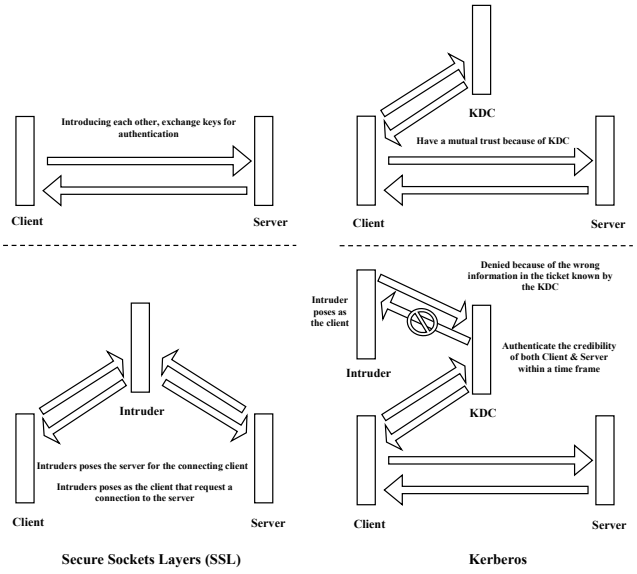

Figure 3 SSL vs. Kerberos Diagram

In the diagram above, we have shown that the possibility of an intruder to bypass the security in Kerberos is almost unlikely to succeed. In Secure Sockets Layers (SSL), intruders trick the client(s) and server by pretending to be one of each. Intruders pretend to be the server the client is trying to have access to, and intruders pretend to be the client trying to connect to the server. Thus, having access with the shared key for both client(s) and server.

5. CONCLUSION AND FUTURE WORK

In this paper, we have presented the concept for applying the Kerberos to improve the security in FTP using Markov model. The standard security protocol for FTP is using Secure Sockets Layers (SSL) which have found that it has weaknesses that is prone to sniffing attacks that can bypass the security.

On the other hand, Kerberos uses a server that encrypts and sends ticket that neither the client(s) nor the server knew about the content of authenticating each ticket created for the legitimate client(s) and server. Therefore, blocking the possibility of a sniffing attack and all kinds of fraudulent attacks from an intruder. Therefore, instead of having the client(s) and the server share a set of encrypted keys both of them know in SSL. Thus, using Kerberos authentication protocol, it improves the security between the FTP server and the client(s).

For future work, we plan to investigate further on a wider range of the security of Kerberos KDC server to further strengthen the effectiveness of using Kerberos rather than SSL for a security protocol and preventing the likelihood of being compromised by intruders. We also aim at analyzing the Kerberos protocol to prove its consistency and best security practice.

6. REFERENCES

[1] M. Korczynski and A. Duda, "Markov Chain Fingerprinting to Classify Encrypted Traffic," IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 2014, doi:10.1109/infocom.2014.6848005.

[2] M. Korczynski and A. Duda, "Classifying Application Flows and Intrusion Detection in Internet Traffic", University of Grenoble, France, 2012. http://mkorczynski.com/Thesis_Maciej_Korczynski.pdf

[3] ELDOS "Kerberos vs. SSL/TLS. What's the Buzz?" Software Components for Data Protection, Secure Storage and Transfer. Accessed July, 2016.

[4] V. Beal, "FTP – file transfer protocol", Accessed August, 2016.

[5] "Markov Chains: Explained Visually", Accessed August, 2016. http://setosa.io/ev/markov-chains/

[6] V. Alex "An Overview of a Kerberos Infrastructure", Accessed August, 2016.

[7] M. Cregg, "Six Ways Hackers Try to Break Secure Sockets Layer-encrypted Data." Accessed August, 2016.

[8] DFT Software "Immediate Intrusion Detection: Catching Hackers Red-handed on Your Web Server!" January 23, 2013. Accessed August, 2016.

[9] Introduction to Probability, Statistics and Random Processes "State Transition Matrix and Diagram", Accessed September, 2016. https://www.probabilitycourse.com/chapter11/11_2_2_state_transition_matrix_and_diagram.php

[10] "Probability Distribution", Accessed September, 2016. https://www.probabilitycourse.com/chapter11/11_2_3_probability_distributions.php

[11] G. D. Bissias, M. Liberatore, D. Jensen, and B. N. Levine, "Privacy Vulnerabilities in Encrypted HTTP Streams," in *Proc. of the Int. Conference on Privacy Enhancing Technologies*, 2006, pp. 1-11.

[12] L. Bernaille and R. Teixeira, "Early Recognition of Encrypted Application," *Proc. of the PAM Conference*, vol. 4427, pp. 165-175, 2007.

[13] G. Sen, Y. xue, Y. Dong, D. Wang, and C. Li. "An Novel Hybrid Method for Effectively Classifying Encrypted Traffic," Proc. of IEEE GLOBECOM, pp. 1-5, 2010.

[14] M. Korczy´nski and A. Duda, "Classifying Service Flows in the Encrypted Skype Traffic," *Proc. of IEEE ICC*, pp. 1–5, 2012.

[15] O. Levillain, A. Ébalard, B. Morin, and H. Debar, "One Year of SSL Internet Measurement," *Proc. of ACM ACSAC*, 2012, pp. 11–20.