FILE INTEGRITY MONITORING USING CRYPTOGRAPHIC CHECKSUMS

(SURVEY PAPER ON SHA256 CHECKSUM MONITORING)

|  |  |
| --- | --- |
| *Tinashe Gondwa*  *Department of Information Security and Assurance*  *Harare Institute of Technology*  *h170192a@hit.ac.zw* | *Ms E Hukuimwe*  *Department of Information Security and Assurance*  *Harare Institute of Technology* |

***Abstract - HTTPS is rapidly rising alongside the need for Internet users to benefit from security and privacy when they log on to the Web, and it becomes an advanced online application. This migration to a secure Web using HTTPS comes with important challenges related to HTTPS traffic management to ensure basic network infrastructure such as security, QoS, reliability, etc. But cryptography undermines the effectiveness of customary observance techniques and makes it tough for ISPs and network directors to properly establish and manage the services behind HTTPS traffic. This paper aims to monitor the use of SSL/TLS Certificates so as to come up with a solution of how Zimbabwean domains can be able to keep up to date with their certificate renewals and use of the legit and authorised certificate issuers.***

***Keywords – SSL/TLS, Certificate, HTTPS, X509 Certificate, ISPs, Web, OSINT.***

1. **INTRODUCTION**

The Internet a global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) for communication between devices and networks. It is a community of networks that consists of private, public, business, government, and academic networks of local to world scope, linked via a huge array of electronic, wireless, and optical networking technologies. With the rapid growth of the Web additional security was essential for its success. This gave rise to the birth of SSL. Secure Socket Layer is cryptographic protocol created to provide secure communication over the computer networks. It makes use of SSL certificates that are data files bind by cryptographic keys to an organisation’s details. The SSL cert binds together (1) Domain Name or Server Name or Hostname and (2) an Organisational Identity and location. When these data files, also referred to as digital certificates, are installed on a web server, they provide a secure connection between the web server and the browser and makes use of the https (over port 443) protocol. Whenever the browser connects to the webserver through websites, all the data communicated will now be secure and encrypted. SSL secures data submitted over the Internet from being intercepted and viewed by unintended clients. This gives confidence to Internet users as there will be secure online credit card transactions, secure system logins and any sensitive information exchanged online and more. With all these advantages of the SSL certificates they come with a validity period reduced to no longer thirteen (13) months, leads to most webserver/domain owners not or delaying updating their digital certificates leaving clients and recipients vulnerable. The need for an information technology system that can monitor the validity of the X.509 Certificates and cut the risk of exposure, while maintaining trust and transparency.

1. **PROBLEM STATEMENT**

Ever since the introduction in 1994, the Secure Socket Layer (SSL) law (now Transport Layer Security (TLS)) has evolved into a de facto level of protection for the transport layer. SSL / TLS can be used to ensure data confidentiality, integrity, and authenticity during transit. A key feature of a protocol is its flexibility. Operating systems and security objectives can be easily adjusted by using various cipher suites. During its evolutionary process, a few errors were discovered. However, the flexible structure of the SSL / TLS has allowed for the right adjustment to address the issues. and Application Data Protocols, on TLS PKI infrastructure, and various other attacks. This gave the researcher the motive to look into Open-Source ways of collecting x509 certificates, reviewing and monitoring on their validity and usages so as to reduce the likelihood of the use of fake SSL certificates of Zimbabwean public domains.

1. **LITERATURE REVIEW**

The review carried out by the researcher has concluded the following on the literature that has been accessed:

1. ***Demystifying Service Discovery: Implementing an Internet-Wide Scanner***

***By : Derek Leonard and Dmitri Loguinov (Department of Computer Science and Engineering Texas A&M University)***

This paper addresses a high-performance internet-wide service discovery tool called IRLscanner. This tool’s objectives were mainly emphasizing on maximizing politeness at the remote networks, scanning rates that archive coverage of the Internet in minutes/hours rather than days/weeks, and reducing the administrator complaints. Assuming a fixed amount of bandwidth available for scanning, in this section we seek to alleviate these concerns by two ways. This ensures that checks are accomplished in time and improves lookup speed from 923 Kpps (balanced tree) to 11 Mpps (using a single core of a 2.2 GHz Opteron). Given that most commodity machines have at least 1 GB of RAM and the rest of the scanner requires only 2 MB of main memory, this trade off allows the tool to dedicate more computational power to sending packets and performing other processing as needed.

1. ***ZMAP - Fast Internet-Wide Scanning and its Security Applications***

***By : Zakir Durumeric, Eric Wustrow, J. Alex Halderman (University of Michigan)***

In this paper the researchers address how Internet-wide network scanning has numerous security applications, including exposing new vulnerabilities and tracking the adoption of defensive mechanisms, but probing the entire public address space with existing tools is both difficult and slow. They claim that ZMAP is an open-source tool that can port scan the entire IPv4 address space from just one machine in under 45 minutes with 98% coverage. They present the scanner architecture, experimentally characterize its performance and accuracy, and explore the security implications of high-speed Internet-scale network surveys, both offensive and defensive. The tool gives visibility into the distributed system. Their study led them to gaining a near real time perspective into the Certificate Authority ecosystem. As per the time of the publication of the paper they had managed to complete 110 scans of the HTTPS ecosystem in the previous year, collected more than 42 million unique certificates of which 6.9 million were browser trusted. Identified 2 sets of mis-issued CA certificates.

1. ***A Survey of Methods for Encrypted Traffic Classification and Analysis***

***By: Petr Velan∗†, MilanˇCerm ́ak, PavelˇCeleda, Martin Draˇsa (Institute of Computer Science, Masaryk University, Brno, Czech Republic)***

In this paper the researchers discovered that, with the widespread use of encrypted data encryption for data transmission it has become a common practice now. This poses a challenge to traffic measurement, especially in the analysis and discovery methods that are inconsistent based on the type of network traffic. In this paper, they explored the existing methods of planning and analysing encrypted traffic. First, they described the most widely used encryption methods used throughout the Internet. They show that the implementation of encrypted connections and the protocol structure provides more details of encrypted road planning and analysis. After that, they uploaded the surveyor and methods separated by the encrypted traffic feature and separate them using an inactive taxonomy. The advantage of one of the defined methods is the ability to know the protocol of a protocol through the encryption process. Finally, they made a complete comparison of the methods tested for segmentation and highlighted their weaknesses and strengths, with the most methods targeted encryption protocols being SSH,SSL/TLS and encrypted BitTorrent.

1. ***Classification of SSL Servers based on their SSLHandshake for Automated Security Assessment***

***By: Sirikarn Pukkawanna and Youki Kadobayashi Nara (Institute of Science and Technology)***

In this paper, they suggested three ways to break down the details of SSL / TLS security according to: (1) Alternative names, (2) proto-col version and encryption-based, and (3) combined risk factors -based methods. They also separated real-world SSL / TLS servers, which ran from July 2010 to May 2011, using the proposed methods. Finally, they proposed 45 features, which are considered to be consistent with security testing, in future SSL / TLS data integration. Partition results showed that the servers had bimodal distribution, especially good standards, and security. The results also show that most SSL / TLS servers had certificates appear to be malicious and use both malicious processes and encryption algorithms.

1. ***Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices***

***By: Homin K. Lee , Tal Malkin, Erich Nahum***

In this paper, they demonstrate the cryptographic capabilities of public servers using SSL / TLS on the Internet. They developed a tool for the purpose of the research, the ProbingSSLSecurityTool (PSST),and evaluated over 19,000 servers. Some of their disappointing results showed that many sites were still supporting the insecure SSL2.0, low encryption cipher scores, or weak RSA key strengths. They also observed the massive adoption of AES (with more than half of the servers that support the AES key as per its default option), and the use of RSA key sizes of 1024bits and above. Comparing their results of using their tool over the previous years indicates a positive trend that is going well, or perhaps not so fast.

1. ***Improving SNI-based HTTPS Security Monitoring***

***By: Wazen M. Shbair, Thibault Cholez, Jérôme François, Isabelle Chrisment***

Recent research shows that the number of encrypted web traffic is increasing rapidly. On the one hand, it provides users with important areas of security and privacy, but on the other hand, it raises important challenges and problems for organizations, related to monitoring the security of encrypted traffic (filtering, anomaly detection, etc.). This paper proposes to develop the latest HTTPS traffic monitoring system based on the TLS Server Name Indication (SNI) field and used in many firewall solutions. SNI value for new TLS connection. Their research shows that 92% of HTTPS websites tested in this paper can be accessed through fake-SNI. Their approach ensures a connection between the destination server and the required SNI value by relying on trust DNS service. The test results show the ability to overcome SNI-based surveillance by detecting SNI values ​​that were fraudulent while having a very low false alarm (1.7%). The title of their solution only adds a slight delay to accessing HTTPS websites. The proposed approach opens the door r to improve global HTTPS monitoring and firewall systems.

1. ***Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations***

***By: Chad Brubaker∗ † Suman Jana† Baishakhi Ray‡ Sarfraz Khurshid† Vitaly Shmatikov***

In this paper, they were developing, implementing, and implementing the first-of-its-kind certification testing system for SSL / TLS implementation certification. Their first ingredient is “frankencerters,” artificial certificates that are randomly modified from real certification components and thus include an unusual combination of extensions and subdivisions. Their second ingredient was a different test: if the SSL / TLS phone launcher receives a certificate while the other rejects the same certificate, they used the variation as oracle to detect errors in each operation. As OpenSSL, NSS, CyaSSL, GnuTLS, PolarSSL, MatrixSSL, etc. Most of them are caused by high security risks. For example Forex, any server with a valid X.509 version 1 certificate can act as a powerful certificate authority and issue illegal certificates of any domain, enabling attacks on people within the MatrixSSL and GnuTLS. Few implementations also accept certificate authorities made up of unauthorized providers, as well as certificates not intended for server verification. When presented with an express-issued, signed, NSS, Safari, and Chrome (on Linux) certificate it reports that the certificate has expired - a very serious, frequently signed error - but not that the connection is not protected from a man-in-the-middle the results show that auto-contradictory testing with frankencerts is a powerful way to detect security errors in SSL / TLS performance.

1. ***Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks***

***By: Md. Shohrab Hossain, Arnob Paul, Md. Hasanul Islam, Mohammed Atiquzzaman***

Web communication between server and client is widely used. However, the hijacking of the session has been a serious problem for many of the communications clients. Among the different session hijacking attacks, SSL hacking is the most dangerous attack. Several measures have been suggested to prevent SSL-based attacks. However, the present study did not summarize all methods of prevention in a holistic way (except for many illustrations and classifications). The purpose of this paper is to provide an in-depth study of existing measures to combat SSL hijacking attacks and to compare those measures. In this paper, they divided all the methods to prevent SSL-based hijacking session attacks into two categories: client-side measures and server-side measures. They outlined the proposed solutions in detail with useful drawings for clarification. They also compared the basics of different operating principles. This paper will help web security researchers to have a comparative analysis of all SSL solutions that attack based attacks, thus finding existing solutions to protect users from cyber hijacking attacks.

1. ***SoK: SSL and HTTPS:Revisiting past challenges and evaluating certificate trust model enhancements***

***By: Jeremy Clark and Paul C. van Oorschot***

Internet users nowadays swear daily on secure HTTPS connections with the sites they shall visit. Over the years, a lot of HTTPS attacks and sure credentials accustomed be thought of, enforced, and / or emerged. Their survey additionally identifies key security problems with HTTPS and provides systematic historical treatment and current challenges, aimed toward providing a context for future indicators.

1. **PROPOSED SYSTEM**

The aim is to have a dashboard to observe Zimbabwe IP and domain security exposure using Open Sources Intelligence. With the rapid increase of adoption and use of web technologies in Zimbabwe’s workspaces and businesses, there is a need to monitor the exposure to the technologies to reduce the risks associated. This solution upholds this by automating the process of enumerating domains, monitoring the x.509 certificates and triggering any necessary action whether the domains need certificate installation or updates.

This will serve as a great tool for the Cyber Security Researchers as it will be producing a full dashboard to observe Zimbabwe IP and Domain security exposure.

The scope of this project will be limited to Zimbabwean IPv4 addresses and domains (.zw domains). The SEMS will be focused on the http and https protocols for this project but in future there will be room for expansion into other protocols like S/MIME and others.

1. **DESIGN**

Access to IPinfo’s system is needed through the use of an API that can be called in the Django views for ASN Retriever module.

The system will be dependent on the access to the internet as the User will be interacting with public domain servers.

A central database system is needed as a repository to store the retrieved records of x509 certificates.

After development PCs are set up, installation and operation of IPinfo’s API is necessary and development of chain code for transaction execution is required. Below shows the architecture solution for the system.

Diagram

Description automatically generated

1. **IMPLEMENTATION**

The proposed system has the following modules which will allow it to successfully meet its functionality:

**Cert Retriever**

This module is a Django view that allows the user to create a search profile and then use the user passed information to lookup the x509 certificate of the related domain.

**ASN Retriever**

This is an IPinfo API used as a Django view to retrieve the domain passed ip address to lookup its organisation information linked to it.

The Use Case below describes the roles and responsibilities of each user.

A picture containing diagram

Description automatically generated

The User is the one that looks up the domains as desired.

The Admin is there to manage accounts and the database.

1. **CONCLUSION**

The purpose of these survey was to collect information on how Open-Source Intelligence can help in the management of security exposure and also to get to know on other projects and research done in the line of the use, abuse and forging of SSL/TLS, detailing possible attacks that could happen and how to cater for them. Based on the review it was found out that a web-based system provides convenience, efficiency, and security to the security researcher, system administrators and internet users.

1. **REFERENCES**

[1] RFC 5746: Transport layer security (TLS) renegotiation indication extension, 2010.

[2] RFC 6066: Transport layer security (TLS) extensions: Extension definitions, 2011.

[3] 2013 IEEE Symposium on Security and Privacy

[4] INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT: Int. J. Network Mgmt2014;00:1–24

[5] <https://arxiv.org/abs/2008.08339v1>

[6] URL: <http://dx.doi.org/10.5296/npa.v10i1.12478>

[7] Z. Cao, G. Xiong, Y. Zhao, Z. Li, and L. Guo, “A survey on encrypted traffic classification,” in Applications and Techniques in Information Security. Springer, 2014, pp. 73–81.

[8] M. Hus ́ak, M. Cermak, T. Jirsik, and P. Celeda, “Network-based HTTPSclient identification using SSL/TLS fingerprinting,” in10th Interna-tional Conference on Availability, Reliability and Security (ARES).IEEE, 2015, pp. 389–396.

[11] “Safety recommendations concerning the analysis HTTPS stream,”http://www.ssi.gouv.fr/uploads/IMG/pdf/NPTLSNoteTech.pdf,[InFrench], Accessed: 19/04/2015.