UNIVERSITI PUTRA MALAYSIA

IMPROVED TLS PROTOCOL FOR PLATFORM INTEGRITY ASSURANCE USING MUTUAL ATTESTATION

NORAZAH BINTI ABD AZIZ

FSKTM 2014 4

IMPROVED TLS PROTOCOL FOR PLATFORM INTEGRITY ASSURANCE USING MUTUAL ATTESTATION

By

NORAZAH BINTI ABD AZIZ

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

July 2014

DEDICATIONS

To my beloved husband, Mohd Iskandar bin Idris,

To my lovely mother, Jamiah binti Bero,

And to the memory of my late father, Abd Aziz bin Hassan,

passed away peacefully on 3 December 2012.

May Allah bless his soul, and grant him the highest level of paradise...Ameen.

Al-Fatihah.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science.

IMPROVED TLS PROTOCOL FOR PLATFORM INTEGRITY ASSURANCE USING MUTUAL ATTESTATION

By

NORAZAH BINTI ABD AZIZ

July 2014

Chair: Associate Professor Nur Izura Udzir, PhD

Faculty: Computer Science and Information Technology

Normally, secure communication between client-server applications is established using secure channel technologies such as Transport Layer Security (TLS). TLS is a cryptographic protocol which ensures secure transmission of data and authenticity of communication at each endpoint platform. However, the protocol does not provide any trustworthiness assurance of the involved endpoint. So, they are not able to handle the security risks due to potential malicious software or any third parties who may penetrate the platform. Furthermore, there is no mechanism for a computing platform to address the trustworthiness of platform integrity such as free from any malware or spyware.

Remote attestation is an authentication technique proposed by the Trusted Computing Group (TCG) which enables the verification of the trusted environment of platforms and assuring the information is accurate. To incorporate this method in web services framework in order to guarantee the trustworthiness and security of web-based applications, a new framework called TrustWeb is proposed. The TrustWeb framework integrates the remote attestation into TLS protocol to provide integrity information of the involved endpoint platforms. The framework improves TLS protocol with mutual attestation (MA) mechanism, named TLS+MA which can help to address the weaknesses of transferring sensitive computations, and a practical way to solve the remote trust issue at the client-server environment.

In this thesis, we study the foundations of the credibility of the TLS+MA protocol and TrustWeb approach before we describe the work of designing and building a framework prototype in which attestation mechanism is integrated into the Mozilla Firefox browser and Apache web server. We analyse the security of our protocol using Automated Validation of Internet Security Protocols and Applications (AVISPA) to show that it meets the security goals. Analysis on TLS+MA protocol shows that it is resistant against replay and collusion attacks. For performance analysis, we also compared the TLS+MA with previous protocol. The results show that our protocol only incurs 11.2% of performance overhead in secure connection, which lower than the previous protocol. Despite that, our protocol is 50% more efficient.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Sarjana Sains.

PENAMBAHBAIKAN PROTOKOL TLS MENGGUNAKAN PENGAKUSAKSIAN BERSAMA BAGI JAMINAN INTEGRITI PLATFORM

Oleh

NORAZAH BINTI ABD AZIZ

Julai 2014

Pengerusi: Profesor Madya Nur Izura Udzir, PhD

Fakulti: Sains Komputer dan Teknologi Maklumat

Kebiasaannya, keselamatan komunikasi antara perisian pelayan-pelanggan dibangunkan dengan menggunakan teknologi keselamatan rangkaian seperti Keselamatan Lapisan Pengangkutan (*Transport Layer Security (TLS)*). TLS adalah protokol kriptografi yang memastikan keselamatan data dan komunikasi yang sah di setiap destinasi platform. Namun, protokol ini tidak menawarkan sebarang jaminan kebolehpercayaan bagi setiap platform titik hujung yang terlibat. Dengan itu, protokol ini tidak berupaya menangani sebarang risiko keselamatan yang diakibatkan oleh serangan perisian hasad atau pihak ketiga yang mungkin telah menembusi platform. Tambahan pula tiada mekanisma untuk sesebuah platform pengkomputan menentukan kebolehpercayaan integriti platform sama ada ia bebas daripada sebarang perisian hasad atau perisian perisikan.

Pengakusaksian jauh adalah satu teknik pengesahan yang dicadangkan oleh Trusted Computing Group (TCG) yang membolehkan pengesahan persekitaran yang boleh dipercayai bagi sesebuah platform dilakukan dan memastikan maklumat yang diperolehi adalah tepat. Untuk menggabungkan kaedah ini dalam rangka kerja perkhidmatan web bagi menjamin kebolehpercayaan dan keselamatan aplikasi berasaskan web, satu rangka kerja baharu yang dipanggil TrustWeb telah dicadangkan. Rangka kerja TrustWeb ini mengintegrasi komponen pengakusaksian jauh ke dalam protokol TLS bagi menyediakan maklumat integriti bagi sesebuah platform titik hujung yang terlibat. Rangka kerja ini menambahbaik protokol TLS dengan mekanisma pengakusaksian bersama yang dinamakan TLS+MA yang mana dapat membantu menangani masalah kelemahan dalam memindahkan maklumat pengiraan yang sulit dan merupakan cara yang praktikal untuk menyelesaikan isu kebolehpercayaan jauh

dalam persekitaran pelanggan-pelayan.

Dalam tesis ini, kami mengkaji asas-asas kredibiliti protokol TLS+MA dan pendekatan TrustWeb sebelum kami menerangkan mengenai reka bentuk dan pembinaan prototaip rangka kerja di mana mekanisma pengakusaksian disepadukan ke dalam pelayar Mozilla Firefox dan pelayan web Apache. Kami membuat analisa keselamatan pada protokol kami menggunakan Automated Validation of Internet Security Protocols and Applications (AVISPA) untuk menunjukkan bahawa ia memenuhi matlamat keselamatan. Analisa pada protokol TLS+MA itu juga kebal daripada serangan Replay dan Collusion. Bagi analisa prestasi, kami membuat perbandingan penyelesaian rangka kerja diantara TLS+MA dengan protokol terdahulu. Keputusan menunjukkan bahawa protokol kami hanya mengalami penurunan prestasi dalam keselamatan rangkaian sebanyak 11.2% sahaja. Sehubungan dengan itu, menunjukkan bahawa protocol kami 50% lebih efisien.

ACKNOWLEDGEMENTS

Alhamdulillah, with Allah's blessing, I have completed my research and thesis. Firstly, I thank my employee Mimos Berhad for providing financial support and equipment to assist me in my studies.

I am grateful to my supervisor, Associate Professor Nur Izura Udzir and co-supervisor, Professor Ramlan Mahmod whose guidance on secure applications and information security research methods had enabled me to complete this thesis. Their patience were most valuable whenever I was confused and stuck. Without them to pull me through, I would not have been able to finish this study.

I would like to thank my colleagues, Dr. Poh Geong Sen and Moesfa Soeheila, for the fruitful discussions on cryptographic protocols and for proofreading this thesis. Also, thanks to my superior Mr. Azhar Abu Talib and team members at the workplace for their technical help and for allowing me the time to work on this thesis.

My heartfelt gratitude goes to my beloved husband for giving me the confidence to strive, for lending his strong shoulder during trying times, and for his understanding while being second to my studies sometimes.

Last but not least, I dedicate special thanks to my mother, siblings and friends who had encouraged me throughout my journey in pursuing this master degree.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree Master of Science.

The members of the Supervisory Committee were as follows:

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Ramlan bin Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____	Signature: _____
Name of Chairman of Supervisory Committee: _____	Name of Member of Supervisory Committee: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIK	Attestation Identity Key
BIOS	Basic Input/Output System
CA	Certificate Authority
CGI	Common Gateway Interface
COT	Chain of Trust
CPU	Central Processing Unit
CRTM	Core Root of Trust for Measurement
cURL	Client URL Request Library
DAA	Direct Anonymous Attestation
EK	Endorsement Key
HTML	Hypertext Markup Language
HLPSL	High Level Protocol Specification Language
HTTPS	Hyper Text Transfer Protocol Security
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMA	Integrity Measurement Attestation
IPsec	Internet Protocol Security
MA	Mutual Attestation
MITM	Man-in-the-Middle
NAT	Network Address Translation
NSS	Network Security Service
OASIS	Organization for the Advancement of Structured Information Standards

PCA	Privacy CA
PCR	Platform Configuration Register
RA	Remote Attestation
RSA	Cryptosystem (Ron Rivest, Adi Shamir, Leonard Adleman)
RTM	Root of Trust for Measurement
SOAP	Simple Object Access Protocol
SML	Storage Measurement List
SSL	Secure Socket Layer
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TLS	Trusted Layer Security
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSS	TCG Software Stack
TTP	Trusted Third Party
URL	Uniform Resource Locator
VPN	Virtual Private Network
WSDL	Web Service Definition Language
XACML	EXtensible Access Control Markup Language

CHAPTER 1

INTRODUCTION

This chapter presents as an overview of the authenticated key exchange with platform integrity assurances framework which comprises of extended Secure Socket Layer (SSL) or TLS protocol with mutual attestation. In this chapter, we describe the motivation of the framework in Section 1.1. Section 1.2 states the problem being solved followed by Section 1.3 which lists thesis objective. The scope of the research is defined in Section 1.4. In Section 1.6, we summarize the main thesis contribution. Finally, Section 1.7 outlines the organization of the thesis.

1.1 Motivation

With the rapid increase in remote services such as e-commerce and online systems usage, online transactions security becomes more crucial. In order to protect data communication on the network, many remote services are dependent on the deployment of SSL/TLS protocol. SSL/TLS supports security schemes with authentication, data integrity and confidentiality between two networking applications. Most SSL/TLS implementations utilize remote authentication scheme to validate the host's identity across the network by using public-key certificate mechanism. However, improper key exchange mechanism and unknown integrity status of the host's platform might expose sensitive information to an attacker. So, SSL/TLS is still vulnerable to remote attacks because the protocol is unable to provide integrity of remote system platform. The famous remote attack is phishing attack.

Phishing is a semantic attack which can be categorized into different types of attacks. These attacks' behaviour depends on the diverse type of proliferation including man-in-the middle (MITM) and malware. Man-in-the-middle attack is a class of phishing attack which spoof a browser using phishing email or bogus web sites to lure user into unknowingly produce user information such as usernames, passwords and account details. All the information can be used for criminal purposes by impersonating the user. This attack exploits weaknesses in client-server authentication schemes such as password authentication and SSL/TLS implementation. In contrast, malware-based attacks using malicious pieces of software installed on the host platform to steal confidential information. The malware is installed through drive-by installations technique. The techniques use online advertising spaces or faulty websites to publish hidden malicious HTML code by exploiting popular website vulnerabilities. The malware is automatically installed on the platform when users browse to the website.

In order to protect against these attacks, there are a number of security solutions for phishing defences have been introduced. The famous security solutions are using end-system security product such as malware scanners and personal firewall [33]. The installation, maintenance and correct usage of these security products rely on end user capability. It may require extensive configuration effort and high

technical skill. However, the configuration process will confuse non-technical users and can cause insufficient configuration that lead to reduce product functionalities. Furthermore, most of these security products are costly. Other well-known security solutions are password authentication scheme and SSL/TLS protocol. As discussed earlier, there are also weaknesses in these solutions due to the lack of a proper mechanism to establish the integrity and non-repudiation requirements of the information involved in online transactions [33].

As a result, existing computing platforms are exposed to various security problems due to the weaknesses of the hardware architecture and software configuration complexity. So, in order to guarantee authenticity, integrity, privacy, anonymity or availability of the computing platform, there are initiatives proposed by [25, 61] to use Trusted Platform Module (TPM) functionalities to verify the security of the platform. TPM is a hardware security chip introduced by the Trusted Computing Group (TCG). TCG is a non-profit industry standardization organization that aims to develop and promote an open industry standard to enhance the security of the trusted computing hardware and software building blocks. TCG has produced the specification for TPM (TPM specification 1.2). In the specification, clear guideline and explanation are given, so that developers can easily develop a system which uses the TPM [76]. In accordance with other security hardware extensions [17, 18], the TPM is embedded with cryptographic mechanisms that can be used to remotely certify the integrity of the application or system running on the platform. This functionality adopts attestation method to establish integrity assurance of the state of the hardware and software running on the computing device.

Remote attestation is a method which a client authenticates its hardware and software configuration to a remote host. Remote attestation enables a client to verify the identity and platform integrity of a remote host and vice versa. Moreover, the remote attestation's purpose is to ensure the trustworthiness of a platform without revealing the actual properties and configuration of the platform. Hence, this method provides confidence to client and remote host to communicate across a network through web services.

1.2 Problem Statement

Web services are the most established mechanism to support interaction between host platforms over a network. So, it is important to provide better security solutions on the web service applications platform. Although TLS protocol is widely used to secure network communication, normal TLS protocol does not handle the endpoint integrity issue. Hence, it is necessary to enhance the security of TLS communication by platform integrity assurance between client and remote host to ensure no malware or spyware is installed.

As mentioned earlier, even with security provided by TLS on the web services environment, web client have no assurance about the integrity of server platforms and

vice versa. Due to that, mechanisms are needed to provide the web server with trusted features which promises high security assurance. But how about in the situation wherein the web server has been compromised and consequently violates the integrity of clients information? The feasible solutions to this issue require Trusted Third Party (TTP) involvement to verify the integrity status of the web client and server.

Trusted computing techniques introduce a security mechanism via the TPM, a tamper-resistant hardware to provide integrity protection functionalities for web services platform. Other than securing cryptographic key in a protected storage, the TPM is also utilized to attest the web services platforms configuration. The mechanism is known as Remote Attestation (RA). An attestation technique is an essential mechanism to ensure a particular platform of endpoint has not been tampered with and is in a trusted state. Hence, this mechanism will be used to guarantee the hosts trust level before transmitting any sensitive information to remote host. Then, to assure the communication partner of web services environment, the RA requires verification method such as the TTP.

However, the RA mechanism which transfers the clients system components measurements to the remote host faces some challenges [27, 72, 71]. The challenges include on how to establish and secure the attestation channel between the client and remote host without neglecting scalability issues [71]. So, it is important to establish the attestation communication in a well-defined security protocol, otherwise, the attacker might be able to relay attestation challenge of compromised host to another host and masquerade the host as a trusted one [72].

In view of the issues above, this thesis proposes an integrated security solution for web services that extend SSL/TLS with remote attestation protocol. The idea is to develop a framework of dynamic software-oriented and fine-grained attestation in web environment called "TrustWeb" which leverages on TCG and web security technologies. Furthermore, all the proposed protocols embed the attestation protocol in the TLS extension resulting in modification of TLS library and hence changes plug-ins in users browser or application. Our protocol is designed in such a way that the TLS library does not have to be modified.

1.3 Research Objective

The main objective of the research is **to propose an improved TLS protocol to achieve platform security assurance and trustworthiness of the platform in client server environment** whilst considering the following requirements.

1. Security

   The major motivation of TrustWeb is to enhance web security by utilizing the capability of mutual remote attestation in isolated web environment. This approach which integrates TLS protocol with attestation mechanism will allow web server to verify the integrity of a requesting web client before permitting an access to a protected object based on integrity evidence and information of the web client. The web client can also verify the integrity of the web server before performing any transaction. The TrustWeb protocol will achieve some of the existing TLS security goals which are:

   - Confidentiality
   - Entity and data origin authentication
   - Data integrity
   - Privacy
   - Unlinkability

   and new security goal which is:

   - Platform Integrity

2. Performance

   The TrustWeb approach enhances the current web communication model by introducing extra entities and extra steps into the authentication phase. As a result, this approach is expected to degrade Web servers' performance level. Furthermore, SSL-enabled host is generally slower than non-SSL host. This approach is expected to achieve more security at the cost of performance degradation since adding more security inevitably incurs overhead. However, the approach must minimize the performance degradation to be widely accepted by the industrial world.

1.4 Scope

The scope of this research work is outlined in the following points:

1. The framework and implementation being discussed in this research work focus on web-services platform because it is most commonly used in client-server environment. However, major component of the framework can be implemented in any other client-server applications.

2. The security goals focused in this research work are confidentiality, entity authentication, data origin authentication, privacy, unlinkability, data and platform integrity. This can be achieved with existing TLS version and mutual attestation mechanism. Hence, other security goal such as client anonymity is beyond the scope of this thesis.

3. Security analysis of the protocols is performed using Automated Validation of Internet Security Protocols and Applications (AVISPA) with Dolev-Yao security model. The strength of the protocols against replay and collusion attack is also investigated through informal analysis.

4. The certification authorities mechanism used in this work is assumed secure and trusted. The discussion of this mechanism limitation is beyond the scope of this thesis.

5. The implementation of TrustWeb framework were developed for Mozilla Firefox and Apache as client and server applications, respectively. The solution framework is compared against other protocols to measure it time efficiency.

1.5 Significance of Study

The significance of this research work is outlined in the following points:

1. Provides **security protection** for secret information inside web client or server host from being revealed to any adversary.

2. Provides **integrity check** within SSL/TLS protocol so that it is resistant from being attack by adversary or untrusted system.

3. Provides **integrity measurement** for web applications running on SSL/TLS protocol so that it can detect any compromised application.

4. Provides **end-point integrity assurance** in web services environment.

1.6 Contributions

This thesis makes the following contributions:

1. **Extended TLS protocol, TLS+MA to achieve the endpoint integrity of client and server platform.**
   The TLS authenticated key exchange is extend with mutual attestation mechanism which provides protection against major active attacks such as replay attack, malicious code attacks and man-in-the-middle attacks.

2. **Another protocol, TLS+CA sets up secure communication with unilateral attestation.**
   In this protocol only client's platform integrity is verified. The advantage of this protocol is that the client achieves anonymity against the server.

3. **An implementation of TrustWeb framework that involves the TLS+MA protocol between web browser and web server.**
   The implementation consist of :

- A novel pluggable interfaces used to perform remote attestation which can be customized either to embed with or integrate with TLS protocol in client-server environment.
- Additional module for Certificate Authority (CA) which provide Endorsement Key (EK) credential as authoritative certificate of TPM.

1.7 Organization of Thesis

This thesis is organized in accordance with the standard structure of thesis at Universiti Putra Malaysia:

Chapter 2 Literature Review provides relevant information about Trusted Computing technology in order to create a basis of understanding for the rest of the thesis. This chapter also summarize methods used in related work which the design structures and security strengths are compared as well as the necessity of combining the TLS with attestation in a client-server environment.

Chapter 3 Research Methodology describes the research methodology on how to conduct this research including method of verification that will be used to analyze the security of the proposed protocol.

Chapter 4 Extending TLS Protocol briefs about attestation protocol design and component that are directly related to our proposed protocol.

Chapter 5 Security Analysis of Protocol presents the security analysis of the proposed protocol in Chapter 4.

Chapter 6 Implementation of TrustWeb contains the detail of TrustWeb framework and implementation based on the proposed protocol.

Chapter 7 Performance Analysis of TrustWeb presents the performance result analysis of TrustWeb framework implementation in Chapter 6.

Chapter 8 Conclusions and Future Works concludes the thesis and presents possible directions for future work.

BIBLIOGRAPHY

[1] Nagarajan. Aarthi, Varadharajan. Vijay, Hitchens. Michael, and Saurabh Arora. On the applicability of trusted computing in distributed authorization using web services. In Vijay Atluri, editor, *Data and Applications Security XXII*, volume 5094 of *Lecture Notes in Computer Science*, pages 222–237. Springer Berlin / Heidelberg, 2008.

[2] W A Arbaugh, D J Farber, and J M Smith. A secure and reliable bootstrap architecture. In *Proceedings 1997 IEEE Symposium on Security and Privacy Cat No97CB36097*, pages 65–71. IEEE Comput. Soc. Press, 1997.

[3] Frederik Armknecht, Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin, Martin Unger, Gianluca Ramunno, and Davide Vernizzi. An efficient implementation of trusted channels based on openssl. In *Proceedings of the 3rd ACM workshop on Scalable trusted computing*, STC '08, pages 41–50, New York, NY, USA, 2008. ACM.

[4] Seshadri. Arvind, Perrig. Adrian, van Doorn. Leendart, and Khosla. Pradeep. Swatt:software-based attestation for embedded devices. In *IEEE Symposium on Security and Privacy*, 2004.

[5] AVISPA. *AVISPA v1.1 User Manual (Automated Validation of Internet Security Protocols and Applications)*. Information Society Technologies Programme (IST-2001-39252), www.avispa-project.org, document version: 1.1 edition, June 2006.

[6] Shane Balfe, Amit D. Lakhani, and Kenneth G. Paterson. Trusted computing: Providing security for peer-to-peer networks. In *Peer-to-Peer Computing, IEEE International Conference on*, volume 0, pages 117–124, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[7] Roger Bass, Kenneth Bengtson, and Timothy Bennett. *OASIS, Advancing open standards for the information society*. OASIS, January 2013.

[8] Andrea Bottoni, Gianluca Dini, and Evangelos Kranakis. Credentials and beliefs in remote trusted platforms attestation. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, WOWMOM '06, pages 662–667, Washington, DC, USA, 2006. IEEE Computer Society.

[9] Don Box, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Frystyk Nielsen, Staish Thatte, and Dave Winer. Simple object access protocol (soap) 1.1. www.w3.org/TR/2000/NOTE-SOAP-20000508, 2000.

[10] Colin A. Boyd and Anish Mathuria. *Protocols for Key Establishment and Authentication*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[11] Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 132–145, New York, NY, USA, 2004. ACM.

[12] Michiel Broekman. End-to-end application security using trusted computing. Master's thesis, Software Engineering Programme, Oxford University Computing Laboratory, 2005.

[13] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Trans. Computer System*, 8(1):18–36, February 1990.

[14] Jan Camenisch. Better privacy for trusted computing platforms. Technical report, IBM Research, Zurich Research Laboratory, 2005.

[15] Liqun Chen, Rainer Landfermann, Hans Löhr, Markus Rohe, Ahmad-Reza Sadeghi, and Christian Stueble. A protocol for property-based attestation. In *Proceedings of the first ACM workshop on Scalable trusted computing*, STC '06, pages 7–16, New York, NY, USA, 2006. ACM.

[16] Erik Christensen, Francisco Curbera, Greg Meredith, and Sanjiva Weerawarana. Web services description language (wsdl) 1.1. http://www.w3.org/TR/wsdl, 2007.

[17] Grawrock David. The intel safer computing initiative building blocks for trusted computing. http://www.intel.com/intelpress/sum secc.htm, 2005.

[18] Advanced Micro Devices. *AMD Secure Virtual Machine Architecture Reference Manual*. AMD, 2005.

[19] Kurt. Dietrich. A secure and reliable platform configuration change reporting mechanism for trusted computing enhanced secure channels. In *Institute for Applied Information Processing and Communication (IAIK), IEEE*, 2008.

[20] David L. Dill, Andreas J. Drexler, Alan J. Hu, and C. Han Yang. Protocol verification as a hardware design aid. In *Proceedings of the 1991 IEEE International Conference on Computer Design on VLSI in Computer &Amp; Processors*, ICCD '92, pages 522–525, Washington, DC, USA, 1992. IEEE Computer Society.

[21] Danny Dolev and Andrew C. Yao. On the security of public key protocols. In *IEEE 22nd Annual Symposium on Foundations of Computer Science*, pages 350–357, Stanford, CA, USA, 1981. Stanford University.

[22] J. G. Dyer, M. Lindemann, R. Perer, R. Sailer, L. van Doorn, S.W. Smith, and S.Weingart. Building the ibm 4758 secure coprocessor. *Computer*, 34(10):5766, 2001.

[23] Ralf S. Engelschall. Mod_ssl combines the flexibility of apache with the security of openssl. http://www.modssl.org/, July 2013.

[24] P. England, B. Lampson, J. Manferdelli, and B. Willman. A trusted open platform. *Computer*, 36(7)(7):55–62, 2003.

[25] Jeff Farris. Remote attestation. http://www.math.uiuc.edu/ dursma/Math595CR/FarJ.pdf, 2005.

[26] H. Ge and L. Liu. A method to implement direct anonymous attestation. *eprint.iacr.org*, eprint.iacr.org/2006/023.ps, 2006.

[27] Kenneth Goldman, Ronald Perez, and Reiner Sailer. Linking remote attestation to secure tunnel endpoints. In *Proceedings of the First ACM Workshop on Scalable Trusted Computing*, STC '06, pages 21–24, New York, NY, USA, 2006. ACM.

[28] Li Gong, R. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*, pages 234–248, 1990.

[29] Alan Grosskurth and Michael Godfrey. Architecture and evolution of the modern web browser. Elsevier Science, June 2006.

[30] Alan Grosskurth and Michael W. Godfrey. A case study in architectural analysis: The evolution of the modern web browser. emse. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.68.52, 2007.

[31] Sigrid Gurgens, Peter Ochsenschlager, and Carsten Rudolph. Role based specification and security analysis of cryptographic protocols using asynchronous product automata. In *International Workshop on Trust and Privacy in Digital Business*. DEXA 2002, 2002.

[32] Vivek Haldar, Deepak Chandra, and Michael Franz. Semantic remote attestation: A virtual machine directed approach to trusted computing. In *USENIX Virtual Machine Research and Technology Symposium*, 2004.

[33] Stan Hegt. Analysis of current and future phishing attacks on internet banking services. Master's thesis, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, May 2008.

[34] HLPSL. *HLPSL Tutorial - Beginners Guide to Modelling and Analysing Internet Security Protocols*. European Community under the Information Society Technologies Programme (1998-2002), www.avispa-project.org, 1.1 (ist-2001-39252) edition, June 30 2006.

[35] Trent Jaeger, Reiner Sailer, and Umesh Shankar. Prima: Policy-reduced integrity measurement architecture. In *Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, SACMAT '06, pages 19–28, New York, NY, USA, 2006. ACM.

[36] Camenisch Jan. Direct anonymous attestation: Achieving privacy in remote authentication. Technical report, Information Security Colloquium, IBM Research, Zurich Research Laboratory, 15 June 2004.

[37] Reid. Jason, M. Gonzalez Nieto. Juan, and Dawson Ed. Privacy and tusted computing. In *Proceeding of the 14th International Workshop on Database and Expert Systems Application (DEXA03), IEEE*, 2003.

[38] Steven Kinney. *Trusted Platform Module Basics Using TPM in Embedded Systems*. Elsevier, 2006.

[39] Adrian Leung, Liqun Chen, and Chris J. Mitchell. On a possible privacy flaw in direct anonymous attestation (daa). In *Proceedings of the 1st International Conference on Trusted Computing and Trust in Information Technologies: Trusted Computing - Challenges and Applications*, Trust '08, pages 179–190, Berlin, Heidelberg, 2008. Springer-Verlag.

[40] Gavin Lowe. Breaking and fixing the needham-schroeder public-key protocol using fdr. In *Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems*, TACAs '96, pages 147–166, London, UK, UK, 1996. Springer-Verlag.

[41] Vigano Luca. Automated security protocol analysis with the avispa tool. In *Proceedings of the XXI Mathematical Foundations of Programming Semantics (MFPS'05)*, volume 155, pages 61–86. Elservier, ENTCS, 2005.

[42] John Marchesini, Sean W. Smith, Omen Wild, and Rich MacDonald. Experimenting with tcpa/tcg hardware, or: How i learned to stop worrying and love the bear. Technical Report TR2003-476, Department of Computer Science, Dartmouth College, December 2003.

[43] Alam Masoom, Zhang Xinwen, Nauman Mohammad, and Ali Tamleek. Behavioral attestation for web services (ba4ws). In *Proceedings of the 2008 ACM workshop on Secure Web Services*, SWS 08, pages 21–28, New York, NY, USA, 2008. ACM.

[44] Microsoft. Ssl/tls in detail. http://technet.microsoft.com/en-us/library/cc7858112003.

[45] Mozilla. Introduction to network security services. https://developer.mozilla.org/en-US/docs/NSS, January 2013.

[46] Seiji Munetoh, Megumi Nakamura, Sachiko Yoshihama, and Michiharu Kudo. Integrity management infrastructure for trusted computing. *IEICE - Transactions on Information and Systems*, E91-D(5):1242–1251, May 2008.

[47] Andreas Nilsson. Key management with trusted platform modules. Master's thesis, Computer Science and Communication, Royal Institute of Technology, Stockholm, Sweeden, 2006.

[48] OpenSSL. Openssl cryptography and ssl/tls toolkit. http://www.openssl.org/, July 2013.

[49] Oracle. Oracle vm virtualbox user manual. https://www.virtualbox.org/manual/UserManual.html, 2013.

[50] Michael P. Papazoglou and Jean-Jacques Dubray. A survey of web service technologies. Technical report, Informaticae Telecomunicazioni, University of Trento, June 2004.

[51] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Computer Security*, 6(3):85–198, 1998.

[52] Siani Pearson. *Trusted Computing Platforms: TCPA Technology in Context*. Prentice Hall PTR, Upper Saddle River, NJ US, 2002.

[53] Paul D. Robertson, Matt Curtin, and Marcus J. Ranu. *Internet firewalls: Frequently asked questions*, revision: 10.9 edition, 2009.

[54] D. Robinson and K. Coar. Common gateway interface (cgi). http://www.ietf.org/rfc/rfc3875, October 2004. a Network Working Group, The Apache Software Foundation.

[55] C. Rudolph. Covert identity information in direct anonymous attestation. *In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, editors, 22nd IFIP TC-11 International Information Security Conference (SEC2007) on New Approaches for Security, Privacy and Trust in Complex Environments, Sandton, South Africa, May 14- 16, 2007. Proceedings, Springer, Boston, 2007*, Volume 232 of IFIP International Federation for Information Processing:pp. 443–448, 2007.

[56] Ahmad Reza Sadeghi. Trusted computing – special aspects and challenges. Horst Gortz Institute for IT Security, Ruhr University Bochum, Germany, 2007.

[57] Ahmad-Reza Sadeghi and Christian Stüble. Property-based attestation for computing platforms: Caring about properties, not mechanisms. In *Proceedings of the 2004 Workshop on New Security Paradigms*, NSPW '04, pages 67–77, New York, NY, USA, 2004. ACM.

[58] Reiner Sailer, Trent Jaeger, Xiaolan Zhang, and Leendert van Doorn. Attestation-based policy enforcement for remote access. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 308–317, New York, NY, USA, 2004. ACM.

[59] Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn. Design and implementation of a tcg-based integrity measurement architecture. In *13th USENIX Security Symposium*. IBM T. J. Watson Research Center, August 2004.

[60] Joe Salowey and Eric Rescorla. Transport layer security (tls) renegotiation indication extension. http://www.ietf.org/rfc/rfc5746.txt, Februrary 2010. a Internet Engineering Task Force (IETF).

[61] Dries Schellekens, Brecht Wyseur, and Bart Preneel. Remote attestation on legacy operating systems with trusted platform modules. *Sci. Comput. Program.*, 74(1-2):13–22, December 2008.

[62] Smith Sean. *Trusted Computing Platforms, Design and Applications*. Springer, 2005.

[63] Marcel Selhorst, Christian Stüble, and Felix Teerkorn. Tss study - introduction and analysis of the open source tcg software stack trousers and tools in its environment. German federal office for information security (bsi), Sirrix AG Security Technologies, 2010.

[64] S.Goldwasser, S. Micali, and C. Racko. The knowledge complexity of interactive proofs. *SIAM J. Comput*, 18(1):186–208, 1989.

[65] Elaine Shi, Adrian Perrig, and Leendert Van Doorn. Bind: A fine-grained attestation service for secure distributed systems. In *IEEE Symposium on Security and Privacy,*, volume IEEE Computer Society., pages 154–168, Washington, DC, USA, 2005. SP '05, IEEE Computer Society.

[66] S. W. Smith. Webalps: A survey of e-commerce privacy and security applications. *ACM SIGecom Exchanges*, Volume 2, 2001.

[67] S.W. Smith. Outbound authentication for programmable secure coprocessors. In *Proceedings of the 7th European Symposium on Research in Computer Security*, page 7289 ., London, UK, 2002. ESORICS 02, Springer-Verlag.

[68] B. Smyth, M. Ryan, and L. Chen. Direct anonymous attestation (daa): Ensuring privacy with corrupt administrators. *Proceedings of the Fourth European Workshop on Security and Privacy in Ad Hoc and Sensor Networks, Lecture Notes in Computer Science, Springer-Verlag*, Volume 4572:pp. 218–23, 2007.

[69] Lincoln Stein and Doug MacEachern. *Writing Apache Modules with Perl and C*. ISBN: 1-56592-567-X. O'Reilly, first edition, March 1999.

[70] Frederic Stump, Lars Fischer, and Claudia Eckert. A multilayered security architecture for c2c-communication. In *Trust, Security and Privacy in VANETs*. VDI/VW-Gemeinschaftstagung: Automotive Security, Wolfsburg, Germany, November 2007.

[71] Frederic Stumpf. *Leveraging Attestation Techniques for Trust Establishment in Distributed Systems*. PhD thesis, Department of Computer Science, Technische Universitat Darmstadt, 2010.

[72] Frederic Stumpf, Omid Tafreschi, Patrick Roder, and Claudia Eckert. A robust integrity reporting protocol for remote attestation. Technical Report D-64289, Darmstadt University of Technology, Department of Computer Science, 2010.

[73] TCG. Tcg specification architecture overview specification, revision 1.3, March 2007.

[74] TCPA. Trusted computing platform alliance main specification, version 1.1b, Feb 2002.

[75] TNC. Trusted network connect – specification. www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications, 01 2014.

[76] TPM. Tpm main part 1 design principles, specification version 1.2, 29 March 2006.

[77] Trousers. Trousers manpages. trousers.sourceforge.net/man.html, 2012.

[78] TSS. Tcg software stack (tss) specification version 1.2 level 1 errata a, March 2007.

[79] Jon Viega, Pravir Chandra, and Matt Messier. *Network Security with Openssl*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1st edition, 2002.

[80] W3Techs. Usage statistics and market share of apache for websites, July 2013.

[81] Gasmi Yacine, Sadeghi Ahmad-Reza, Stewin Patrick, Unger Martin, and N. Asokan. Beyond secure channels. In *ACM STC 07 Proceedings*, 2007.

[82] Thomas GENET Yann GLOUCHE and IRISA/Universite de Rennes 1 Erwan HOUSSAY. *SPAN a Security Protocol ANimator for AVISPA*. INRIA/IRISA LANDE Project, version 1.8 edition, Septermber 2008.

[83] S. Yoshihama, T. Ebringer, M. Nakamura, S. Munetoh, and H. Maruyama. Ws-attestation: efficient and fine-grained remote attestation on web services. *IEEE Journal on Selected Areas in Communications*, pages 2 vol. (xxxiii+856), july 2005.

[84] Yue Yu, Sun Hao, and Kong Yanan. Expand the ssl/tls protocol on trusted platform module. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, volume 11, pages V11–48–V11–51, 2010.

[85] Xiaofei Zhang. Trust extended dynamic security model and its application in network. *Springer-Verlag Berlin Heidelberg.*, 2006.

[86] Lingli Zhou and Zhenfeng Zhang. Trusted channels with password-based authentication and tpm-based attestation. In *Communications and Mobile Computing (CMC), 2010 International Conference on*, volume 1, pages 223 –227, april 2010.