Journal of
Information Technology & Software Engineering

Palmateer, J Inform Tech Softw Eng 2017, 7:5
DOI: 10.4172/2165-7866.1000214

Review Article Open Access

Defining Security in Primary Key Infrastructures

Kurtis B Palmateer*

College of Information Systems and Technology, Colorado Technical University Online, United States

Abstract

Smart card authentication is a methodology used for security across various network infrastructures that demand multiple factors in user authentication. The present existence of smart card authentication thrives in our mobile and payment card networks; but can be applied to the average organization's local area network (LAN) and remote connectivity mediums for a baseline of multiple factor authentication. Moreover, this paper looks into implementing network-wide smart card authentication on enterprise systems in an attempt to alleviate those systems of password-based authentication schemes. Much emphasis and research will be provided on the detailed characteristics of smart card authentication and its implementation on modern network appliances, key distribution servers and endpoint configurations.

Keywords: Public key infrastructure; Smart card authentication; X.509 certificate objectives

Introduction

Advances in Information Assurance Security (IAS)

Smart card technology: The smart card authentication schema is an advancement in network security that the Department of Defense (DoD) and contractors use to authenticate with defense systems via X.509 certification. This method of identification, authentication and authorization can be implemented into any enterprise network infrastructure as a more reasonable way of protecting the network from intrusions with the help of smart card readers and middleware software designed to utilize two-factor authentication via encrypted certificates and access PINs for network logins.

Smart card compatibility: This advancement is compatible with network-based firewalls and virtual private network (VPN) implementations for remote employees that experience days of work from home. The goal behind the security implementation of smart card access is to alleviate the password usage on the computer-based network since hackers are already familiar with password cracking techniques; hence a more secure method of authentication demands digital certification and public key encryption that can be managed via a public key infrastructure (PKI).

Future research with smart cards: The research produced in the following sections will apply this technology to the different realms of a networked architecture (e.g., endpoint authentication, remote identity management, middleware implementations, media access control, certification standards, and network protocols) compatible with public key infrastructure administration [1]. The goal is to provide enough research for one to make an educated decision about whether smart card technology and public key encryption proves to be a viable direction for their organization or if the default password-based authentication schema is indeed reliable enough for tomorrow (Figure 1).

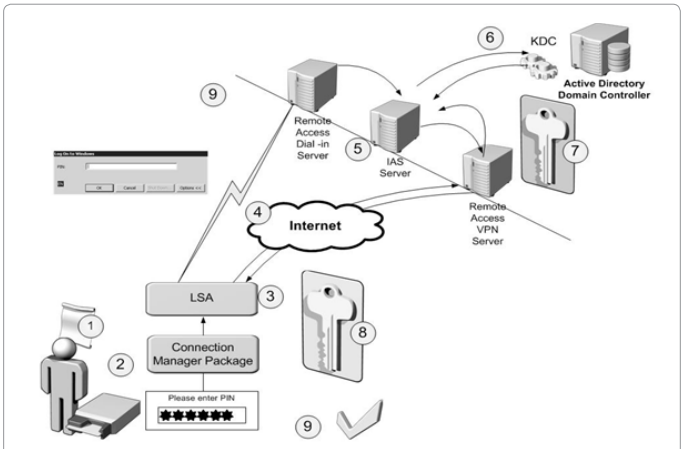

Figure 1: Public key infrastructure (pki) with smart card authentication.

Systems and Software Security Integration Topics

Historical perspective

The historical presence of smart card authentication began in the late seventies by Michel Ugon who invented the highly reliable and portable security device that was physically drafted and developed in the early eighties [2]. Once the physical draft and standardization of the contact location was completed, application development for cryptographic capabilities began on the technology [3]. Nowadays, smart card authentication is used in several applications including payment card and cellular phone technology. The future of smart card technology should begin to emphasize on the average organization's authentication schema on the backend of our networks; a perspective that would reduce the commonality of intrusions on network resources.

Topic applicability

The topic of smart card authentication is applicable to the concept of replacing/eliminating password usage on backend networked resources. Adversaries have been exploiting and compromising password authentication methods for decades; a practice that will only advance in complexity over the coming years. Among their methods includes keystroke grabbing, shoulder surfing, malware injection, local and remote privilege escalation, and software exploitation techniques that discover, retrieve, and decrypt our passwords much faster with the help of cloud services and powerful hardware. It is an organization's decision to implement digitally encrypted certificates in their authentication schema and enforce acceptable usage amongst

***Corresponding author:** Kurtis B Palmateer, College of Information Systems and Technology, Colorado Technical University Online, United States, Tel: +1(623)299-5955; E-mail: kurtis@sqldriven.com

Received November 03, 2017; **Accepted** November 13, 2017; **Published** November 20, 2017

Citation: Palmateer KB (2017) Defining Security in Primary Key Infrastructures. J Inform Tech Softw Eng 7: 214. doi: 10.4172/2165-7866.1000214

distributable smart card technologies as an effort to protect themselves against weak password authentication schemes. One shouldn't question the viability in the technology as it is implemented in our mobile phones, payment cards and common access cards (CAC) for telephony, payments, and facility accessible resources on a regular basis. Given that track record of reliability, why wouldn't an organization use the same concept to protect themselves from password theft?

The reliability of a smart card and its application to public key infrastructure is dependent on the distribution of digitally encrypted certificates stored on the card and key distribution server.

Implementation applicability

Design: This process covers the steps taken to implement smart card authentication across the security infrastructure of your organization. Questions arise such as, "Should we use a one-key methodology that grants access to facility resources (e.g., doors, rooms) and logical resources (e.g., active directories) on the network?".

Acquisition: The step that requires the acquisition of hardware (e.g., card readers) and software for the organizations door entries and computers. Additionally, the smart card media themselves are acquired at this stage. This is an important process that should not be overlooked by upper-management during a budgetary evaluation.

Implementation: The transformation of the information infrastructure occurs depending on the intensity of your solution. For instance, the one-key methodology is going to require more legwork in installing hardware components and middleware software on the doors, servers, and endpoint computers of the organization.

Risk Assessment

Defining the risk

The probability of a user's credentials (e.g., digital certificates, personal identification number, smart card) being compromised is reduced to several factors: a combination of a lost smart card and disclosure of personal identification number (PIN) or a traffic capture that exploits encryption, furthermore allowing a malicious actor to craft and/or compromise credentials on the network. The following section will cover the risks surrounding a public key infrastructure's implementation and describe the steps taken to (1) analyze (2) identify (3) describe (4) estimate and (5) evaluate such risks.

Addressing the risk

Steps to address risk is shown in Table 1.

Risk assessment

Smart Card Authentication Implementation is shown in Table 2.

Security risk

Figure 2 displays the concept of credential theft via password-sharing, session hijacking, password brute-forcing (dictionary or character-based attacks) or any other means illegal authentication through password-based login.

Infrastructure Topics

Change plan

The implementation of new technologies always impacts the organization in a positive or negative manner. Despite the chances of end users disliking new systems and technologies on an increase of work load(s) baseline, changes to the current system oftentimes introduce standards that aid compliance across the information infrastructure. Additionally, newly introduced systems and networks typically provide opportunities for technological advances like new services, increased network architecture complexities and expansion. The following sections will discuss the impact smart card authentication technologies

Gathering Information	Involves discovering, identifying, and describing the risk before (and after) the incident
Assessing the Risk	Determines the potential (or actual) impact the risk has on the organization
Recommending Controls	Specifies the countermeasures that must be taken to circumvent such risk
Determining Residual Risk	Identifies the side-effects of the risk or any long-term damage that may occur (e.g., reputation loss)

Table 1: Steps to address risk.

Title of project Smart Card Authentication Implementation			
Location of activity Computer Security Division		**Start and end dates** 08/25/16 – 09/20/16	
Brief description (or attach procedure/protocol) The installation of smart card readers, software components (middleware), and public key infrastructure will propose the following securities to our information systems: confidentiality, accountability, and complexity. This new technology demands a detailed risk assessment on the assets introduced to this new solution. Updates to the current system convey a new set of risks and effects along with their respective countermeasures and residual components.			
Hazard	**Effect**	**Control measures**	**Residual risk**
Compromised Smart Card / PIN	Potential Intrusion / Identity Theft	Mandatory reporting of lost or stolen smart access cards within 24 hours of discovery.	Compromised Electronic Resources / Data Leak and Reputation Loss
Traffic Sniffing / Session Hijacking	Arbitrary Access to Unauthorized Resources / Temporal Privilege Escalation	Monitor the network for abnormalities in network resource requests. Always use encrypted communication mediums (including the PKI authentication technology proposed in this research) on the network.	Undetectable Data Capture / Information Disclosure or Resource Access
Denial of Service (DoS) / Service Interruption	Interruption of Network Resources, Communications, or Business-critical Processes	Frequently update the attack signatures on the DoS attack signatures via the firewall vendor service subscription. Maintain whitelist on security appliances and ensure the throughput of such devices.	Resource Slowdown or Downtime / Loss of Reputation
Malware Detection / Computer or Network Infection	Loss of Computer System Operability / Unauthorized Control and Disclosure of Data	Respond immediately to reports of malware detection and quarantine systems per occurrence for investigation and malware analysis.	Violations to the Acceptable Use Policy (AUP) / Data Loss or Information Disclosure
Phishing / Blackmail Attempts on Human Assets	Compromised User Credentials / Unauthorized Control of Information Systems or Data Disclosure	Mandatory reporting of suspicious communications to the computer security division. Follow-up investigations of potential dangers regarding malicious actors. Documentation of each report instance.	Data Theft / Unrecoverable Information Disclosure

Table 2: Details of smart card authentication implementation.

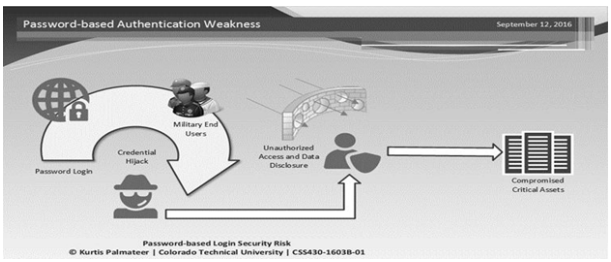

Figure 2: Password-based login security risk.

have on the organization.

Impact on the people and organization

A client and server authentication solution around a complex public key infrastructure mandating smart card authentication across each user is an ideal solution for out-phasing password-based logins without investing in biometrics. Since organizations that require federal information processing standards (FIPS) conform to stricter methods of encrypted communication and endpoint network authentication for access to networked storage, smart card authentication becomes reasonable for resource accessibility. Can this level of security be applied to the average corporation as well? How must one measure the need for a public key infrastructure with smart card authentication? The answer relies on one's trust in password-based authentication.

Technological implementation

A smart card solution for authentication in the most common business environments yields great results for the datacenters and endpoints across the security realm of each technological infrastructure because of the core values it is built upon: confidentiality, accountability, accessibility, and authorization. These core concepts establish the current evolution we are experiencing in the payment industry and information age. The active migration from passwords and personal identification numbers to encrypted certificates (X.509) on the storage of smart card technologies is today's new standard. Such technology protects an organization from the vulnerabilities associated with hash captures of login credentials and subsequently the disclosure of unencrypted employee login information.

Technological auditing and monitoring

Overall, the impact smart card authentication and public key infrastructure has on an organization is positive with the correct implementation of a (1) Kerberos Distribution Center (2) lightweight directory access protocol for an updated certificate revocation list (3) pluggable authentication modules requiring two-factor authentication for common access cards and pin system logins. Such system provides the ability to revoke credentials for resigned employees, lost or stolen cards, and unacceptable use cases. These security configurations provide the changes we need to create a strong audit trail of information we need to recognize exactly what occurs before and after an instance of unauthorized data access and/or usage.

Communication plan

The implementation of strong authentication measures oftentimes includes periodically training personnel of their acceptable usage rights and duties of such technology. In most cases, technologies are not cheap and require the proper training to use responsibly. It is upper-management's duty to oversee that the security media used in this implementation is carefully handled by appointing supervisory managers to enforce strict regulations on acceptable use and care for such technology with the assistance of the security team and information technology department(s).

Training details

Table 3 contains the training details.

Training frequency

- Quarterly - Reponsibilities and Acceptable Usage.
- Annually - Cyber Security Challenges and Responsiblities (Figure 3).

Communication distribution

Training meetings should occur in-house and remotely on scheduled dates in conference rooms and are mandatory each team subjected to using information technology owned by the organization. Remote meetings will occur via networked conferencing software. These meetings occur weekly, quarterly, and annually depending on the topic and urgency of the meeting. A typical cyber security meeting is held by all personnel that uphold a responsibility on information technology equipment. Otherwise, financial advisors and project managers meet separately on a separately running schedule.

Emerging Threats to IAS

Payment card industry data security standard

Smart card authentication has been implemented into the payment card industry standards for its reasonably secure authentication, accountability, authorization, and availability standards because of the troubles the industry has encountered with fraudulent transactions, credit card cloning, and identity theft on payment gateways [4]. Any software or system that interacts (or communicates) with a payment gateway is subject to the Payment Card Industry Data Security Standard (PCI-DSS).

Payment system information supporting smart cards

Figure 3: Training frequency.

The payment gateway is application-based; and its software is written in various system-level programming languages. Oftentimes, the subjected units of code for such software system is responsible for the payment form interface, secure payment transmission, and third-party API of the payment gateway [5]. The following classes and interfaces will be tested individually (Table 4).

The most important part about accepting payments on a payment gateway is securing the data being transmitted. Since this product serves third-party e-commerce websites, the primary protocol used for transmission is HTTPS; hence the use of SSL/TLS is an important factor on the frontend. Any data being transmitted over external or untrusted networks needs strong encryption over this protocol [6]. In addition, the following requirements need met:

1. Only trusted keys and certificates will be used.
2. Secure versions of SSL/TLS and configurations are to be used.
3. Strong encryption strength is to be used.

These units of the system will be tested by certified penetration testers quarterly.

System testing

When testing the payment gateway for errors, samples of the data transmissions will be collected and examined. These samples will allow us to determine the quality of service (QoS) of our product. In addition, the data samples will be used to examine the security of the transmissions. Both the integrity and confidentiality of the payment transactions our gateway processes are top priorities (PCI Security Standards Council, 2013). The following connections will be sampled and examined:

1. Inbound Connections (SSL/TLS) – These connection requests contain cardholder information, and are to be strongly encrypted.

2. Outbound Connections (SSL/TLS) – These connections contain sensitive responses to our client's requests, and are to be encrypted as well.

During system testing, the process of identifying system vulnerabilities is imperative to keeping a payment gateway alive. The information systems security officer (ISSO) should be responsible for identifying, patching, and rating the potential vulnerabilities of the system. Only reputable outside sources should be used to identify vulnerabilities in the system [6]. Additionally, the ISSO will be overseeing the security controls implemented in the system. Counteractive plans will be created in the case the system is compromised. The errors or vulnerabilities in the system should be reported to the software developers and information systems security officer (ISSO) for changes. The ISSO is always involved in these reports because many system crashes and/or errors can be vulnerabilities black hats use to exploit systems. It's imperative that this system is secured because it is a high-profile target for hackers.

Department	Training
Information Technology Department(s)	• Install, configure, and maintain the smart card authentication implementation for all organization personnel. • Host presentations and training meetings for personnel on acceptable use and responsibilities for smart card technology.
Project Management Department(s)	• Oversee that the technology is properly implemented and used for the well-being of the company. • Ensure that strict policies are enforced for unacceptable usage.

Table 3: Training details.

User acceptance testing

The payment gateway should be tested during its beta phase by third-party clients that are interested in purchasing our product. There isn't much scope for an end-user in this system; hence the developers should be doing the majority of the testing in the earliest of stages. This includes the web developers responsible for creating secure forms for the payments on the frontend. Most of the backend testing will be conducted by system developers and senior network engineers. Issues found in the system will be recorded by latency tests, packet analysis, and source code examination. Our web services will be tested by our users during the user acceptance test (UAT) to gain feedback of the friendliness and usability of the payment form.

Quality assurance plan

The quality assurance plan relies heavily on the security of our system(s). The plan is to develop and maintain a secure network of systems with strong access controls, firewall configurations, and data encryption. The confidentiality, integrity, and availability (CIA) of our system is what keeps our product in demand. This entails the following:

1. Firewalls installed between each Internet connection or any demilitarized zone (DMZ).

2. Certificate revocation list rotations between onboarding and offloading human assets.

3. Least privilege principles for analysts including walled-garden authentication for compartmentalized systems.

4. Default passwords are replaced with strong passwords.

5. Router configurations managing to restrict incoming and outgoing connections.

6. A process for testing and approving network routes and changes to the firewall and router configurations.

Overall, the quality assurance (QA) plan is to process payment transactions securely. This is done through diagramming the network, examining each unit of the system for flaws, and complying with the standards set by the Payment Card Industry (PCI).

Note: This section of coursework about the Payment Card Industry was repurposed from IT425-1404B-07, Systems Analysis, Design, and Integration with Prof. Ihssan Alkadi at Colorado Technical University.

Federal regulations

This section of coursework about the federal regulations was reused from CSS441-1602A-01 [7], Security Compliance, with Prof. Tavon Reid at Colorado Technical University (Table 5).

Physical security regarding smart cards

Table 6 contains the details of Smart Card Door Locks.

Conclusion

Ultimately, the security of smart card identification, authentication,

Class/Interface	Description
Web-based Payment Form (API)	• Sends form-data as a HTTPS post transaction • Initiates communication with the transaction processing system (TPS) • Handles sensitive cardholder information via the web browser
Payment Gateway	• Processes remote requests from the Payment Form API • Works as a remote transaction processing system (TPS) • Communicates with payment processors, consumer bank, and merchant bank
Secure Payment Protocols	• Provides security via secure electronic transaction (SET) standard • Uses the 3-D Secure payment protocol as an extra authentication step for online payments • Works with handshakes containing secure shell (SSH) and secure socket layer (SSL) certificates.

Table 4: The description of class/interface.

Regulation	Description
Sarbanes-Oxley (SOX)	• Requires that we maintain our integrity and accountability as a corporation. • Prohibits the destruction of evidence to imped a Federal investigation. • Mandates that our CEO and CFO take responsibility for quarterly financial reports under Section 302. • Protects our company from whistle-blowers and describes criminal penalties (white collar crimes and conspiracy) for the manipulation, destruction, or alteration of financial reports.
National Institute of Standards and Technology (NIST)	• Contains many publications regarding computer security in its 800- XX series. • Includes guidelines for protecting personally identifiable information (PII). • Sets federal standards for an organization to adhere to at the minimal security level. • Applies to our Information Security Continuous Monitoring (ISCM) for Federal Systems and Organizations guidebook.
Federal Information Security Management Act (FISMA)	• Protects governmental information from reaching the public. • Ensures information systems inventory is accounted for. • Requires information systems are categorized by risk level by FIPS 199 and establish security controls on FIPS 200 at the minimum. • Instills the required security plan of high risk systems. • Mandates continuous monitoring on accredited systems.
Homeland Security Presidential Directive (HSPD)	• Demands that unauthorized access on secure federal information systems be eliminated. • Requires that secure forms of identification (ID) is utilized for computer system access.

Table 5: Federal regulations supporting smart cards.

Component	Description
Smart Card Door Locks	• High-cost network components that unlock doors via contactless smart card technologies. • Effective with physical security guards or front-desk clerks watching over door entries.

Table 6: Security component description.

and authorization technology is now implemented in the Department of Defense (DoD) and Payment Card Industry (PCI) because of the portability, availability, accountability and sub-sequential authorization validation that it offers its vendors and consumers. Since the early eighties, the technology has grown well out of prototype and can be applied to almost any networked security appliance across the information technology realm. Its advancing pace and nature of pocket-sized authentication abilities will only grow as we adopt a cheaper form of authentication measures over passwords; without investing in expensive biometrics.

References

1. Mavrogiannopoulos N, Pashalidis A, Preneel B (2012) Security implications in Kerberos by the introduction of smart cards. Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. pp: 59-60.
2. Glisic S (2016) Advanced wireless networks: Technology and business models. John Wiley & Sons, Indianapolis IN. p. 864.
3. Gordon A, Hernandez S (2016) The Official (ISC) 2 guide to the SSCP CBK.
4. Kleinman C (2012) Understanding the role of payment gateways. Response 20: 74.
5. Wang B, Zhu Y, Cai C (2016) A novel smart-card based authentication scheme using proactive secret sharing. IJCCE 5: 196-205.
6. PCI Security Standards Council L (2013) Data security standard requirements and security assessment procedures.
7. Woland AT, Redmon K (2015) CCNP security SISAS 300-208 official cert guide. Cisco Pre, Indianapolis, IN.