Determining Authentication Strength for Smart Card-based Authentication Use Cases

Ramaswamy Chandramouli
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology
Gaithersburg, MD, USA
mouli@nist.gov

Abstract - Smart cards are now being extensively deployed for identity verification(smart identity tokens) for controlling access to Information Technology (IT) resources as well as physical resources. Depending upon the sensitivity of the resources and the risk of wrong identification, different authentication use cases are being deployed. Assignment of authentication strength for each of the use cases is often based on: (a) the total number of three common orthogonal authentication factors – What You Know, What You Have and What You are – used in the particular use case and (b) the entropy associated with each factor chosen. The objective of this paper is to analyze the limitation of this approach and present a new methodology for assigning authentication strengths based on the strength of pair wise bindings between the five entities involved in smart card based authentications – the card (token), the token secret, the card holder, the card issuer and the person identifier stored in the card The use of the methodology for developing an authentication assurance level taxonomy for a real world smart identity token deployment is also illustrated.

Keywords - Identity Verification; Smart Identity Token; Authentication Strength

I. INTRODUCTION

Smart cards are now being extensively deployed for identity verification for controlling access to Information Technology (IT) resources as well as physical resources [1,2,3]. We refer to them as Smart Identity Tokens and use the two terms interchangeably throughout this paper. These types of smart cards generally carry: (a) A Person Identifier (PI), (b) A Secret (TS) usually in the form of a cryptographic key [4], and (c) A Credential linking the Secret and the Identifier (CR). Along with these data, a PIN (a combination of numbers) is often used for: (a) Activating the card (token) and for (b) Restricting access to certain data objects and operations. In some instances, presentation of a live biometric data (such as a fingerprint) is used to enable the above functions instead of a PIN. In any enterprise deploying smart cards, there may be different types of resources that may have to be protected by restricting access to only those whose identity is verified through a smart card based authentication mechanism. Depending upon the sensitivity of the resource and the risk associated with wrong identification of the entity requesting access to those resources, authentication mechanisms using different combinations of the three data types enumerated above (PI, TS or CR) along with/without an activation data may be used. A set of authentication mechanisms used by an enterprise for controlling access to different types of resources (or stated differently- different applications of smart identity token) are called Authentication Use Cases.

In general (irrespective of whether a smart identity token is used or not), the choice of an Authentication Use Case in the context of an access control to a resource is often made based on authentication strength or assurance level associated with the token artifact used in the Authentication Use Case. These artifacts are: (a) an identifier specific to a domain and (b) a credential that is a combination of an identifier and a secret – examples for the latter being: (a) a PIN (b) a one-time password and (c) a cryptographic key. The usage of a token by a claimant during an authentication event results in a value called Authenticator that is generated by the token and is transmitted from the token to the authentication module or the verifier. The basis for designating an authentication strength associated with a token is a fundamental unit called "Authentication Factor". There are three main authentication factors [5]:

- What the Entity Knows (e.g., Password, PIN, etc)
- What the Entity Has (e.g., possession of a token that generates one-time passwords)
- What the Entity Is (e.g., inherent physiological characteristic such as a Fingerprint)

A token that uses one of the above three factors is called a single factor token (e.g., a password that belongs to " What the Entity Knows" factor). A token that uses a combination of two or more of the above factors is called a multi-factor token. A smart card that contains an embedded private cryptographic key (thus using What the Entity Has authentication factor) that can be used to generate an authenticator when it is activated by a PIN (using the What the Entity Knows authentication factor) is deemed a multi-factor token. An authentication use case may use one or more tokens and hence may involve the use of one or more authentication factors. In general, the authentication strength associated with an authentication use case is determined based on the combination of the following metrics:

 ISBN: 978-1-61208-176-2

- The number of authentication factors used in the authentication use case
- The Entropy associated with each of the authenticator factor used

In this paper, we argue that the logic for assigning authentication strength based on the number of authentication factors in an authentication use case is valid only under certain limiting conditions and that these conditions do not hold in the case of authentication use cases using smart cards as identity tokens. This is the rationale for proposing a new methodology for assigning authentication strengths for various authentication use cases involving smart identity tokens.

The description of the conditions under which the number of authentication factors can be used as a reliable metric for authentication strength and an illustration of how those conditions do not hold in the case of smart cards are given in Section II. Section III discusses the basis vector that is applicable for smart card based identity verification approaches. The development of our methodology for determining authentication strengths for various smart card-based authentication use cases based on the basis vector referred to above is the topic of Section IV. The application of this methodology for assigning authentication strengths for building a taxonomy of authentication assurance levels for the set of authentication use cases specified for a major government smart card-based identity verification deployment is done in Section V. Section VI presents the benefits of our methodology and provides the conclusions.

II. LIMITATIONS OF AUTHENTICATION FACTOR-BASED APPROACH FOR DETERMINING AUTHENTICATION STRENGTHS

In order that the number of authentication factors is a valid metric for determining the authentication strength of an authentication use case, it must satisfy the following properties:

- AF-AS-P1: The authentication factors must be mutually independent. If there is any mutual dependency between any two authentication factors, then assuming the additive property is not valid for computing the metric indicating the authentication strength. This is not an issue as the three authentication factors – What You Know, What you Have and What you Are do not have any pair wise mutual dependency.
- AF-AS-P2: All authenticators used in the authentication use case must flow directly from the claimant to the verifier in the resulting authentication message protocol. This property must hold since any authentication decision by the verifier is based entirely on the outcome of the process of verifying one or more authenticators received from the claimant. Hence any authentication decision based on a lesser number of authenticators is certainly of lower authentication strength than an authentication decision using a higher number of authenticators.

We illustrate through an example that the second property is not satisfied in many smart card based authentication use cases deployed in real-world implementations [3,8]. For example, in an authentication use case called Challenge-Response, the smart card responds to a random challenge string sent by the authentication system by encrypting the string with its private key and sending the encrypted string back. Some cards are programmed to require the card holder to provide a PIN to perform this private key operation. This authentication use case is classified as a two factor authentication (since it involves demonstrating the presence of a secret cryptographic key (one factor) and the PIN (second factor)) although the only authenticator that flows to the authentication system (verifier) is the encrypted challenge. Thus, we see that, in order to truly assess the authentication strength associated with smart card based authentication use cases, we need a basis vector other than just the number of authentication factors. To identify and derive such a basis vector, we find that there is a need to look at the various basic entities that participate in authentication protocols using smart cards and the nature of pair-wise binding that exists among them. The logic for development of these pair wise bindings is described in the next section.

III. DEVELOPMENT OF BASIS VECTOR FOR SMART CARD-BASED AUTHENTICATION USE CASES

Before we start using the pair-wise binding as components of a basis vector used for determining authentication strengths, we need to make a comprehensive list of the basic entities involved in them. These basic entities, building on the smart card contents we saw in the last section are: the physical token (smart card), the card holder, the token secret, card issuer and the person identifier. Please note that we do not term the credential as a basic entity since credential is a derived artifact providing the binding of the two basic entities – Person Identifier and the Token Secret. Before we start listing the pair-wise bindings, we find that any authentication use case is itself built from some primitive authentication usage modes each of which uses one or more of three categories of smart card data – Person Identifier, Token Secret and Credential. Hence every pair-wise binding should trace its link to a primitive authentication usage mode and the associated smart card data used in that mode. This link is provided through the data in Table I. Table I, in addition to providing the bindings, also provides the strength associated with each binding based on the nature of the primitive authentication usage mode and the associated data used in it. Out of the six possible valid bindings, the person identifier participates in three of them being associated with card issuer (through digital signature), token secret (being used in digital certificate) and card holder (being used in biometric object).

 ISBN: 978-1-61208-176-2

TABLE I. SMART IDENTITY CARD – PRIMITIVE AUTHENTICATION USAGE MODES & BINDINGS

Smart Card Data	Primitive Authentication Usage Mode	Pair-wise Bindings with associated strength
Embedded Cryptographic Key (private key of an asymmetric Key Pair) – Token Secret	PUM-1: Verifying Presence of embedded token secret (tested by sending an input data from the Verifier and receiving an associated Authenticator)	Token- Token Secret Binding (Strong)
Embedded Cryptographic Key (private key of an asymmetric Key Pair) – Token Secret that requires an activation data to demonstrate its presence	PUM-2: Same as previous + card holder providing a PIN for generating the authenticator	1.Token – Token Secret Binding (Strong) 2.Card Holder – Token Binding (Strong or Weak depending upon entropy of activation data)
Person Identifier	PUM-3: Person Identifier's origin and integrity checked using its associated digital signature	Person Identifier- Card Issuer Binding (Strong)
Credential (A Public Key Certificate) linking the token secret to the Person Identifier	PUM-4: Trust in the certificate established through Certificate Validation	Token Secret – Person Identifier Binding (Strong)
Credential (A digitally signed Biometric Object) linking a Card Holder Trait (biometric) to the Person Identifier	PUM-5: The digital signature associated with biometric data object is verified. Live biometric sample sent to the card for matching with the stored biometric data	Card Holder – Person Identifier Binding (Strong or Weak depending upon how live sample is collected)

IV. METHODOLOGY FOR ASSIGNING AUTHENTICATION STRENGTHS FOR AUTHENTICATION USE CASES

In the previous section, we identified the primitive authentication usage modes and the bindings (along with their associated strength) enabled by those modes. An authentication use case that is used in a smart identity token deployment will be a combination of one or more of the primitive authentication usage modes. Now our final goal is the determination of authentication strength for a given authentication use case. In order to compute this value, we need to know the security properties satisfied and the weakness in each of the primitive authentication usage modes that constitute that authentication use case. The derivation of these security properties satisfied and weaknesses from the bindings (and their associated strengths) provided by each of the five primitive authentication usage modes (taking into consideration the state of smart card technology) is shown in Table II.

Now, based on the observation that the primitive authentication modes are independent of each other (except for PUM-2 which is a superset of PUM-1), the security properties associated with the set of primitive authentication usage modes constituting an authentication use case can all be added up to obtain the total set of security properties satisfied in an authentication use case.

Let us consider the following Authentication use case which we shall call as BIO-A:

1. The Authentication Module (Verifier) reads the signed biometric object on the card.
2. The digital signature of the biometric object is verified.
3. The Authentication station is attended by a guard under whose watch the claimant provides his /her fingerprint through a scanner present in the station.
4. The Live sample of the biometric is compared with the stored biometric data on the card.
5. When the match is successful, the person identifier extracted from the signed biometric object is compared with identifier stored in the identifier object on the card. The digital signature associated with identifier object is verified.
6. If the verification is successful, the identifier is sent to the Physical Access Control Server which in turn sends a signal to open the door leading to the facility controlled by the authentication station.

From the description of the above steps in our example Authentication Use Case BIO-A, we find that steps 1-4 map to our primitive authentication usage mode PUM-5. Step 5 maps to our usage mode PUM-3. Hence adding the properties associated with these primitive authentication usage modes, we find that the authentication use case BIO-A satisfies the following total set of properties:

1. Card Holder is authenticated (Strong – since the live sample is collected under a supervised condition ensuring freshness and hence no replay using duplicated fingerprints possible)
2. Validity of the Identifier is established

The security property set associated with an authentication use case can be used as a metric for establishing a partial order among the various authentication use cases specified for a smart card based identity verification deployment scenario. This partial order can then be used to construct an authentication assurance level taxonomy for that deployment instance.

 ISBN: 978-1-61208-176-2

TABLE II. SECURITY PROPERTIES OF AUTHENTICATION USAGE MODES

Primitive Authentication Usage Mode	Bindings Established with associated strength	Security Properties Satisfied (WEAKNESS in CAPS)
PUM-1: Verifying Presence of embedded token secret (tested by sending an input data from the Verifier and receiving an associated Authenticator)	Token- Token Secret Binding (Strong)	1.Card is Authenticated 1.STOLEN CARD 2. CARD HOLDER IS NOT AUTHENTICATED 3. NO LINK FROM TOKEN SECRET TO PERSON IDENTIFIER
PUM-2: Same as previous + sending an activation data to the token	(a)Token – Token Secret Binding (Strong) (b)Card Holder – Token Binding (Strong or Weak depending upon activation data)	1. Card is Authenticated 2. Card Holder is Authenticated (Strength based on Activation Data) 1.NO LINK FROM TOKEN SECRET TO PERSON IDENTIFIER
PUM-3: Person Identifier's origin and integrity checked using its associated digital signature	Person Identifier – Card Issuer Binding (Strong)	1.Validity of the Identifier is established 1.STOLEN CARD 2. CLONED CARD 3. CARD IS NOT AUTHENTICATED 4. CARD HOLDER IS NOT AUTHENTICATED 5. NO LINK FROM TOKEN SECRET TO PERSON IDENTIFIER
PUM-4: Trust is established on a credential (a public key certificate) linking embedded token secret and the person identifier through certificate validation	Token Secret – Person Identifier Binding (Strong)	1.Link from Token Secret to Person Identifier established 1.STOLEN CARD 2. CLONED CARD 3. CARD IS NOT AUTHENTICATED 4. CARD HOLDER IS NOT AUTHENTICATED
PUM-5: Trust is established on a credential (signed biometric object containing the identifier in addition to biometric data) by verifying the digital signature. Live biometric sample sent to the card for matching with the stored biometric data	Card Holder – Person Identifier Binding (Strong or Weak depending upon how live sample is collected)	1. Card Holder is Authenticated (Strength based on how live biometric sample is collected) 1.CLONED CARD 2. CARD IS NOT AUTHENTICATED

V. ILLUSTRATION OF METHODOLOGY FOR A REAL WORLD SMART IDENTITY TOKEN DEPLOYMENT

In this section, we illustrate the application of our methodology for assignment of authentication strengths for authentication use cases used in a real world smart identity token deployment scenario. The first step of our methodology is to express each authentication use case specified for the deployment in terms of our primitive authentication usage mode. This will automatically provide us the total set of security properties associated with that authentication use case. We then use the property set containment to derive a partial order among the authentication use cases and to finally derive an authentication assurance level taxonomy for the entire smart identity token deployment. The real world smart identity token deployment we have chosen for our illustration is the Implementation of Personal Identity Verification (PIV) smart card for controlling physical access to federal facilities and logical access to U.S government IT systems [7,8]. For the sake of space and brevity, we do not describe each of the authentication use cases in the PIV deployment scenario. We also do not illustrate the process by which our primitive authentication usage modes can be composed to obtain a PIV authentication use case. These liberties have been taken since our final goal is just to illustrate the use of our methodology for developing an authentication assurance level taxonomy. Table III below provides a compilation of all the PIV Authentication uses [8], the list of primitive authentication usage modes that comprise each authentication use case and total set of security properties satisfied by each authentication use case specified in a PIV deployment instance.

 ISBN: 978-1-61208-176-2

TABLE III. PROPERTIES SATISFIED BY PIV AUTHENTICATION USE CASES

PIV Authentication Use Case	Set of Primitive Authentication Usage Modes involved	Properties Satisfied
Authentication using PIV CHUID (CHUID)	PUM-3: Identifier's origin and integrity checked using its associated digital signature	1.Validity of the Identifier is established
Unattended Authentication using PIV Biometric (BIO)	PUM-5: Trust is established on a credential (signed biometric object containing the identifier in addition to biometric data) by verifying the digital signature. Live biometric sample sent to the card for matching with the stored biometric data PUM-3: Identifier's origin and integrity checked using its associated digital signature	1. Card Holder is authenticated (Weak) 2.Validity of the Identifier is established
Attended Authentication using PIV Biometric (BIO-A)	PUM-5: Trust is established on a credential (signed biometric object containing the identifier in addition to biometric data) by verifying the digital signature. Live biometric sample sent to the card for matching with the stored biometric data PUM-3: Identifier's origin and integrity checked using its associated digital signature	1. Card Holder is authenticated (Strong) 2.Validity of the Identifier is established
Authentication using PIV Asymmetric Cryptography (PKI-AUTH)	PUM-4: Trust is established on a credential (a public key certificate) linking embedded token secret and the person identifier through certificate validation PUM-2: Verifying Presence of embedded token secret (tested by sending an input data from the Verifier and receiving an associated Authenticator) (derived from PUM-1) + sending a activation data of robust strength to the token PUM-3: Identifier's origin and integrity checked using its associated digital signature	1.Link from Token Secret to Identifier established 2. Card Holder is authenticated (Strong) 3. Card is Authenticated 4.Validity of the Identifier is established
Authentication using Card Authentication Certificate Credential (PKI-CAK)	PUM-4: Trust is established on a credential (a public key certificate) linking embedded token secret and the person identifier through certificate validation PUM-1: Verifying Presence of embedded token secret (tested by sending an input data from the Verifier and receiving an associated Authenticator) PUM-3: Identifier's origin and integrity checked using its associated digital signature	1.Link from Token Secret to Identifier established 2. Card is Authenticated 3.Validity of the Identifier is established

Based on the property containment relationship between the various PIV authentication use cases, we derive a partial order and use that partial order to develop a complete authentication assurance level taxonomy. The taxonomy thus derived in shown in Figure 1 below:

 ISBN: 978-1-61208-176-2

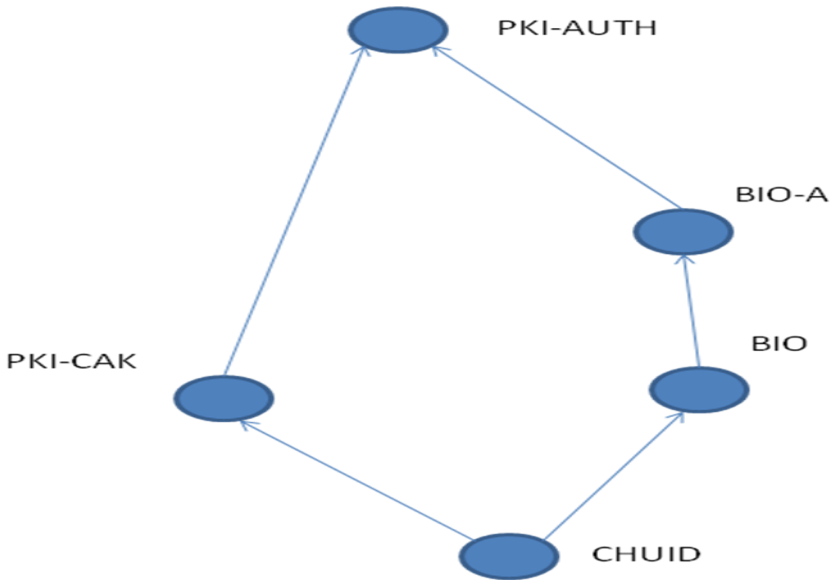

Figure 1. Authentication Assurance Level Taxonomy for a Smart Identity Token Deployment

VI. CONCLUSIONS AND BENEFITS

The observation that not all authenticators flow between the smart identity token and the authentication module (verifier) has driven the need for a new basis vector other than just the number of authentication factors and an associated methodology for assigning authentication strengths for various authentication use cases involving smart cards. In this paper, we developed such a methodology which uses pair wise bindings between the five entities involved in smart identity token authentication use cases –i.e., token (the card), the token secret, the card holder, the card issuer and the person identifier - as the basis for deriving a set of properties satisfied for each primitive authentication usage mode. The primitive authentication usage modes are in turn identified based on the types of data a smart identity token usually holds. Next, we illustrated the process of expressing an authentication use case in terms of the combination of primitive authentication usage modes and using the additive properties associated with each usage mode, derived the total set of properties satisfied by an authentication use case. Finally the property set associated with an authentication use case is used to derive a partial order among the use cases. This partial order was then used to derive an entire authentication assurance level taxonomy for a smart identity token deployment scenario. The advantages of this approach are: (a) It takes into account all entities participating in the authentication protocol (the five that we referred to earlier) and the pair wise bindings between them and (b) considers technology-specific weaknesses (e.g., token can be stolen and cloned) that may affect the security properties satisfied in each primitive authentication usage mode and by extension in an authentication use case.

REFERENCES

[1] Securing e-business applications using Smart Cards, IBM Systems Journal, Vol 40, Number 3, 2001, (Oct, 2011), http://www.research.ibm.com/journal/sj/403/hamann.html

[2] Kumar, M.: New Remote User Authentication Scheme Using Smart Cards, *IEEE Transactions on Consumer Electronics.* Volume 50, Issue 2, 597 – 600 (2004)

[3] TWIC Reader Hardware And Card Application Specification, May 30, 2008, (Nov, 2011) http://www.tsa.gov/assets/pdf/twic_reader_card_app_spec.pdf

[4] NIST SP 800-63-1 Recommendation for Electronic Authentication, Dec 2008, (Oct, 2011) http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf

[5] OMB M04-04 – E-Authentication Guidance for Federal Agencies, Dec 16, 2003, (Oct, 2011) http://www.whitehouse.gov/omb/memoranda/fu04/m04-04.pdf

[6] Internet X.509 PKI Certificate & CRL Profile, (Nov, 2011) http://www.ietf.org/rfc/rfc5280.txt

[7] Identity Management Task Force Report, National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, 2008, (Oct, 2011) http://www.biometrics.gov/documents/idmreport_22sep08_final.pdf

[8] FIPS 201 – Personal Identity Verification of Federal Employees and Contractors**,** (Oct, 2011) http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf

 ISBN: 978-1-61208-176-2