

# Identity Protection Factor (IPF)

Arshad Noor  
StrongAuth, Inc.  
550 Lakeside Drive, Suite 10  
Sunnyvale CA 94085  
arshad.noor@strongauth.com

## ABSTRACT

Since the dawn of computing, operating systems and applications have used many schemes to identify and authenticate entities accessing resources within computers. While the technologies and schemes have varied, there appears to have been little attempt to classify them based on their ability to resist attacks from unauthorized entities.

With the proliferation of identity management technologies in the market today, it is becoming increasingly difficult to assess and compare them with each other. As the threat level continues to rise on the internet, and regulations governing information technology continue to grow, risk managers need more objective mechanisms to assign risk to their systems so they may apply appropriate mitigating controls.

This paper attempts to describe a classification scheme that will permit the comparison of seemingly different identification and authentication (I&A) technologies on the basis of their vulnerability to attacks. With a better understanding of related authentication technologies, companies can determine the appropriate technology to use for mitigating authentication risks.

## Categories and Subject Descriptors

D.4.6 [Operating Systems]: Security and protection – *authentication*.

## General Terms

Management, Security, Standardization.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IDtrust '08, March 4-6, 2008 Gaithersburg, MD  
Copyright 2008 ACM 978-1-60558-066-1...\$5.00

## Keywords

Access Control  
Asymmetric key  
Authentication  
Identification & Authentication  
Identity Protection Factor (IPF)  
Identity Management  
Shared-secret  
Symmetric key

## 1. INTRODUCTION

User ID/Passwords, One-Time Password (OTP) tokens, biometrics, smartcards, Network Information Services (NIS) aka Yellow Pages, Kerberos, Secure Socket Layer (SSL), Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), OpenID, CardSpace - these are just a small sample of the dizzying array of identification and authentication (I&A) technologies the computer industry has created to address varying business and security requirements in the Identity Management (IdM) space.

However, except for the rather simplistic “what-you-know, what-you-have and what-you-are” method of classification, there has been little attempt to create a formal classification scheme for I&A technologies on the basis of their resistance to attack. While most technologists have an intuitive understanding of the relative merits of each I&A technology, and security practitioners are more than likely to have a deeper understanding of it, the lack of a formal classification method is indicative of the immaturity of the profession.

This paper attempts to introduce such a classification scheme. It is intended to be a first step within a process that will, hopefully, lead to more research and consequently, a validation of this scheme or the creation of a better one. Besides bringing clarity to this segment of security management, the benefits of such a classification will lead to better risk-management of systems.

### 1.1 Organization of Paper

This paper begins by describing some of the problems in the area of authentication technologies in Section 2. In Section 3, an overview of the IPF Scale and the technologies that make up the scale is provided. It also explains why this particular model makes sense. In Section 4, the characteristics, strengths and vulnerabilities of each level of the IPF Scale are presented. Section 5 compares this concept with some well-known frameworks and papers on the subject. Section 6 identifies where more research needs to be conducted in this area and the paper finally concludes in Section 7.

## 1.2 Some Definitions

Before delving into the problems of authentication technologies, it is useful to establish this paper's definition of identification and authentication, so that the proper context is established for discussion.

Within the context of computerized information systems, **Access Control** – the discipline of restricting access to computer resources – is defined to consist of three distinct processes[1]:

- i. **Identification** – where a resource claims (or is identified through other means) a specific and unique identifier. Depending on the resource making the claim, the identifier may be a User ID, a Distinguished Name of a digital certificate, a Fully-qualified Domain Name, an Internet Protocol address, etc. *NIST Special Publication 800-63*[2] refers to this resource as “Claimant”, which this paper will use from time-to-time.
- ii. **Authentication** – where the claimed identifier is verified by the access control mechanism, through some means. Depending on the resource, the verification process may consist of using technologies such as Passwords, Digital Signatures, Reverse DNS lookups, etc. A successful verification deems the resource to be “authenticated”.
- iii. **Authorization** – where the privileges associated with an authenticated identity are determined. This is the final step of determining whether the claimant may be granted access to another restricted resource.

Similar definitions of Identification and Authentication are presented by the authors of “*Who goes there?: Authentication Through the Lens of Privacy*”[3].

When discussing identity protection, this paper restricts itself only to the Authentication process part of Access Control.

## 2. PROBLEMS IN AUTHENTICATION

With the introduction of time-shared computers in large corporations and government sectors in the latter part of the

20<sup>th</sup> century, the use of the User ID/Passwords as the basis of authentication in restricting access to computerized resources, was a very reasonable control mechanism. Given the controlled physical access to computing devices and the closed architectures of computers of the time, it was fairly difficult for attackers to compromise computing resources.

With the explosive growth of the personal computer and Local Area Network (LAN) based computing since the late eighties, and of the internet and the World Wide Web since the mid-nineties, computing resources are now available at even the remotest corners of the planet. Simultaneously, in an attempt to take advantage of the internet and the WWW, companies are racing to transform their business practices - and as a consequence, their computing infrastructure - to deliver personal and business services to their customers over the internet.

As a result, not only are hitherto closed computing systems opening up to the internet, but an unprecedented number of users are now connecting to these computing systems through web-portals from all parts of the globe.

Even though there have been many advances in the field of Identification & Authentication (I&A) technology in the intervening period, most companies - including banks and other firms providing financial services - web-enabling their service delivery have chosen to rely on the ubiquitous User ID/Password as the means of identifying and authenticating users.

This has resulted in a multitude of problems:

- i. Consumers of services are forced to register with a multitude of web-sites and acquire new User IDs and Passwords to avail these services. As a result, the average consumer now has more than a dozen credentials, if not more. Most users tend to reuse passwords for multiple credentials, thereby increasing the risk to more valuable accounts;
- ii. In order to achieve the quickest and widest adoption of their web-enabled service, businesses use the path of least resistance and require users to only choose a User ID and Password to register for availing the service. While this has the desired effect in the short-term, the long-term problems are just now starting to surface as businesses grapple with the problems of identity-theft;
- iii. Knowledgeable, but unethical, computer professionals have recognized opportunities to gain financially by stealing User ID/Passwords and taking advantage of the products and services available over the internet in the name of legitimate users;
- iv. The number and types of attacks that attempt to compromise end-user computers and their accounts have grown tremendously over the last ten years – phishing, pharming, key-stroke loggers, root-kits, cross-site

scripting (XSS), SQL injection – these are just a small sample of the types of attacks that have surfaced since the advent of the WWW;

The availability of more sophisticated authentication mechanisms have not made a huge difference towards managing risk in most companies. In an attempt to cut costs and to ease the process of registration, businesses have avoided using the more resilient authentication mechanisms in favor of the User ID/Password.

To make matters worse, in an attempt to simplify the process of authenticating to web-sites, new schemes for authentication are being hatched by the technology industry. The Liberty framework[4], OpenID[5], CardSpace[6] are some examples of “federation” where a single, or a small group of identity-service providers (IdSP) manage the I&A processes, while service web-sites - also called “Relying Parties” in this context - are provided assertions by the IdSP about user-identities. While this has the benefit of off-loading the I&A process to IdSP from the service-provider's point-of-view, unless the underlying authentication technology used by the IdSP was strong, the consolidation of user-credentials at the IdSP could lead to a larger compromise for service-providers.

Finally, in another example of the immaturity of the computing industry, the fact that companies that have suffered a breach are not required to report compromises in a technical manner to some authority, similar to the National Highway Traffic Safety Administration (NHTSA) for automobiles, or the Federal Aviation Administration (FAA) for airlines, makes it impossible for the industry to compile statistical data that would provide insights to risk and mitigation techniques that work. In a telling example of the failure of legislation, the “Breach Disclosure” laws of 37+ US states do not require compromised companies to provide *any technical information* about the compromised infrastructure or the mechanics of the compromise, thus disabling the entire industry from learning from another company's misfortune.

### 3. IDENTITY PROTECTION FACTOR

Just as the medical industry has coined the term “Sun Protection Factor (SPF)” as a measure of the ability of sun-screen lotions to block the sun's harmful rays from burning human skin[7], this author introduces the term **Identity Protection Factor (IPF) as a measure of the ability of an I&A technology to resist attack from unauthorized entities.**

The IPF uses a numerical scale ranging from zero (0) to ten (10) to indicate the relative effectiveness of the I&A technology to protect credentials, with higher numbers indicating a greater ability to resist attack.

*Note: One assumption this paper makes is that the risk of compromise to an I&A technology is based on the client-server architecture using a network for the transport of credentials. This is the typical scenario for the vast majority of systems in use today. However, the IPF can also be used to rate I&A technologies where no network is used for authentication. Examples of the latter are computer operating systems authenticating users against a local database of credentials, or an application authenticating users locally against its own credential database.*

*A second assumption this paper makes about secret-based authentication is that the shared secret between the human user and the system is not maintained in plaintext on the system.*

#### 3.1 IPF Scale

The eleven (11) layers of the IPF Scale are:

IPF	Description
0	No identification or authentication
1	<b>Shared-secret</b> based authentication on a local system, or a network <b>without</b> any network encryption
2	<b>Shared-secret</b> based authentication <b>with</b> network encryption
3	<b>Multiple shared-secret</b> based authentication <b>without</b> an external token, but with network encryption
4	<b>Asymmetric-key</b> based authentication with <b>Private Key in a file</b>
5	<b>Multiple shared-secret</b> based authentication with <b>external token</b> and network encryption
6	Asymmetric-key based authentication with <b>Private Key</b> generated and stored on <b>cryptographic hardware token</b> and using <b>keyboard</b> for authentication to token
7	Asymmetric-key based authentication with <b>Private Key</b> generated and stored on cryptographic hardware token and using an <b>external PIN-pad</b> for authentication to token
8	Asymmetric-key based authentication with <b>Private Key</b> generated and stored on cryptographic hardware token using an external PIN-pad and <b>being physically present at the machine</b> where the resource exists and where authentication is performed

<b>9</b>	Asymmetric-key based authentication with Private Key generated and stored on hardware cryptographic token, using an external PIN-pad, being physically present at the machine where authentication is performed and using <b>M of N control</b> for authentication to token
<b>10</b>	Non-existent/Unknown

### 3.2 A one-dimensional linear scale?

Given the diversity of business, security, operational and user requirements, the IPF Scale begs the question – why a linear scale on a single dimension? Risk-management decisions are a lot more complex than can be plotted on a one-dimensional scale, so how can security professionals and business managers be expected to make a complex decision on authentication technology based on a one-dimensional scale? Chung and Neuman identify multiple dimensions in establishing the *Strength of Security* of network protocols[26]. However, the current paper has chosen to focus on only a single dimension for the reason explained below.

It is the contention of this author, that while it is true that many variables determine the final outcome of computing infrastructures - cost, ease-of-use, operational complexity, availability, ubiquity, etc. - authentication technologies have only one single over-riding factor that truly matters: their ability to resist attacks! If an authentication technology is compromised, nothing else matters to the business at that point. (*Note: At the time of writing this paper, news reports have appeared in the computing press about the \$7.9B loss of Societe' Generale to have been caused by poor password management of internal trading systems at this bank[8]*).

An analogy in the field of civil engineering serves as a telling example: while civil engineers do pay attention to factors such as cost, operational complexity and aesthetics, only a single feature truly matters when constructing a bridge – structural integrity of the design and materials used to construct the bridge, and the ability of the bridge to carry its load given the adverse conditions the bridge may be exposed to in its environment. The collapse of the Tacoma Narrows Bridge (“Galloping Gertie”) in November 1940[9] is still used as a case-study in the field of Civil Engineering, to teach engineering students the importance of focusing on design. The more recent collapse of the interstate bridge on 35W, in Minneapolis in the state of Minnesota, US in August 2007[10] serves as another example of what truly matters when all is said and done.

It is the position of this paper, that regardless of what factors a company might take into account when determining

the authentication technology to use for a computer system, the only factor that truly matters, at the end of the day, is the authentication technology's ability to resist attacks. If an authentication technology with a given IPF rating is not matched appropriately with the risk that a business wishes to assume in a given computer system, it is only the randomness of attacks that prevents the computer system from being certainly compromised.

## 4. CHARACTERISTICS OF THE IPF

Following are the technological characteristics of each layer of the IPF Scale, with examples of real-world technologies, and potential attacks against them.

### 4.1 IPF 0

There are business situations where a computing device does not require human users to identify and authenticate themselves to avail services from the device. Kiosks in public facilities, such as airports and museums, are common examples of these business situations.

While the application providing services to the public does operate with the privileges of a User ID known to the underlying operating system, for the purposes of our classification system, we assume this application has an IPF of Zero (IPF 0) because it does not prompt the human user - within the context of the application - to identify and/or authenticate themselves. Such applications are typically built without any credential databases for authentication.

*Note: However, within the context of the operating system in which this application executes, I&A technology with a higher IPF rating is assumed to be in force.*

I&A technologies with a rating of IPF 0 are assumed to provide no credential risk-mitigation benefits.

### 4.2 IPF 1

I&A technologies with an IPF of One (IPF 1) are defined as those using a shared-secret based authentication mechanism *without* any network encryption, such as SSL, TLS, IPsec or message-level security, to protect the credential.

IPF 1 technologies are different from IPF 0 in that they add an authentication mechanism to IPF 0 technologies to increase their degree of resistance to attacks. All other characteristics of the application and/or system remain the same as IPF 0.

The primary example of an I&A technology with IPF 1 is the ubiquitous User ID and Password being transported to the server over a protocol such as the Hyper-text Transfer Protocol (HTTP), or a User ID and Password being authen-

ticated against a local file or database on the machine where the credential is presented.

I&A technologies with a rating of IPF 1 are capable of being compromised by any of the following forms of attacks:

- Dictionary attacks against the password file;
- Attacks on the password using Rainbow tables;
- Snooping of network traffic for credentials;
- Keystroke loggers to capture the credentials;
- Phishing attacks that prompt the legitimate user to provide their credentials to the attacker;

Given the nature of IPF 1 I&A technologies – the use of a shared secret to authenticate the user - an attacker can compromise a credential without the knowledge of the credential-owner or server, and usurp the identity of the legitimate user. So, a compromise to IPF 1 I&A technologies can go undetected for long durations after the compromise itself has occurred. This paper identifies this characteristic feature of I&A technologies as being “**compromise-blind**”.

#### 4.3 IPF 2

I&A technologies with an IPF of Two (IPF 2) are defined as those using a shared-secret based authentication mechanism with some form of network encryption, such as SSL, TLS, IPsec or message-level security, to protect the credential.

IPF 2 technologies are different from the prior level in that they add network and/or message-level security to increase their degree of resistance to attacks. All other characteristics of the application and/or system remain the same as IPF 1.

I&A technologies with a rating of IPF 2 are identical to I&A technologies with ratings of IPF 1, with one exception: they are not susceptible to compromise through snooping of network traffic, thus giving them a higher IPF rating. Otherwise, all other characteristics and vulnerabilities remain the same.

Other examples of I&A technologies with a rating of IPF 2 would be those based on biometrics alone. On the surface, while biometric I&A technologies appear to use an external authenticator – fingerprint, iris scan, etc. - the reading is ultimately translated into a shared-secret - the template. Biometrics-based I&A technologies also have their own unique attacks that render them susceptible to compromise[11], [12], [13].

IPF 2 I&A technologies, like IPF 1 technologies, are compromise-blind.

#### 4.4 IPF 3

I&A technologies with an IPF of Three (IPF 3) are defined as those combining multiple shared-secret based authentication mechanisms. Because multiple shared-secrets are used to authenticate an identity, this allows such I&A schemes to have a higher IPF rating.

IPF 3 technologies are different from the prior level in that they add a second shared-secret credential to increase their degree of resistance to attacks. All other characteristics of the application and/or system remain the same as IPF 2.

Examples of I&A technologies with IPF 3 are those that combine a User ID and Password with:

- Non-electronic One-Time Password (OTP) tokens – such as from a sheet of paper with predesignated OTPs;
- The selection of a predesignated graphic from an array of graphics;
- Predesignated answers to specific questions;
- Biometrics-based technology;

In all cases, the second authentication credential is also a shared secret that must be sent to the authenticator as part of the authentication process.

From a vulnerability point of view, IPF 3 I&A technologies need to be compromised by multiple types of attacks. The User ID/Password part of the authentication set is capable of being compromised by the same attack techniques as IPF 1 or IPF 2 technologies, while the second shared-secret of IPF 3 I&A technologies is susceptible to phishing attacks[14].

IPF 3 I&A technologies – regardless of the number of shared-secrets used to authenticate the identity - are compromise-blind.

#### 4.5 IPF 4

I&A technologies with an IPF of Four (IPF 4) do not use shared secrets for authentication. They use a form of authentication based on asymmetric cryptographic keys – more popularly known as Public Key cryptography.

IPF 4 technologies are drastically different from the prior level in their use of public-key cryptography to increase their degree of resistance to attacks. All other characteristics of the application and/or system remain the same as IPF 3.

An example of an I&A technology with IPF 4 is the X.509 digital certificate using the Client Authentication protocol

from SSL or TLS[15]. Another example is the Secure Shell (SSH) Protocol when using public-keys[16].

Given the nature of public-key cryptography, the network communication between the client, where the credential is presented, and the server where it is authenticated, is encrypted or cryptographically transformed to prevent replay-attacks; this also eliminates attacks from network-snooping. Public-key cryptography also makes it possible to authenticate a user without having to send the Private Key to the authenticator; merely proof of possession of the Private Key is sufficient to authenticate the user.

The defining characteristic of this IPF 4 technology is that the Private Key of the client's asymmetric key-pair is stored in a file. This file is on the client machine's file-system or an external drive accessible as part of the client machine's file-system with standard ownership privileges.

While the Client Authentication protocol of SSL/TLS and the Public Key Authentication protocol of SSH is robust, the primary vulnerability in this technology is that the file containing the Private Key – typically called a **Cryptographic Keystore** - can be compromised by malware through:

- Dictionary attacks that guess the password/PIN protecting the Cryptographic Keystore; and/or
- Keystroke loggers that capture the password/PIN protecting the Cryptographic Keystore;

Once compromised, the attacker can establish a new SSL/TLS session with the server – either from the legitimate user's PC or from the attacker's own PC if they have copied the Cryptographic Keystore file to their machine - while assuming the identity of the legitimate user. Neither the legitimate user, nor the server would know that the credential had been compromised. Thus, this I&A technology using this specific implementation at IPF 4 is compromise-blind.

#### 4.6 IPF 5

I&A technologies with an IPF of Five (IPF 5) are identical to IPF 3 - i.e. authentication is based on multiple shared secrets – with one exception: in addition to the User ID/Password credential, they use an *external* electronic One-Time Password (OTP) token to generate a shared-secret which is valid for a very short duration[17].

While IPF 5 technologies drop back to shared-secrets for authentication, they are different from prior levels in that they add an external hardware token to increase their degree of resistance to attacks. All other characteristics of the application and/or system remain the same as IPF 4.

While public-key cryptographic authentication systems are generally considered to be superior to shared-secret based authentication systems (because no secrets are shared between the client and the server), I&A technologies with a rating of IPF 4 are easier to attack than systems with a rating of IPF 5.

Nonetheless, external OTP tokens are susceptible to a phishing attack where the attacker can setup a website that mimics the legitimate server site, and then prompts the legitimate user for their User ID, Password and the OTP secret. Upon receiving these, the attacker uses these values to immediately authenticate to the legitimate server site while displaying an error message to the legitimate user. Thus, an attacker can compromise IPF 5 I&A technologies without direct access to the token, and without compromising the client or server machines.

However, because the window of opportunity is extremely short, and the legitimate user must succumb to a phishing attack first, the attacker will have a harder time compromising an IPF 5 technology than ones with lower IPF ratings.

IPF 5 I&A technologies are partially compromise-blind. If the external OTP token is stolen or missing, the legitimate user can suspect their credential may get compromised unless they notify appropriate authorities to take corrective action. However, until an Administrator disables that specific OTP credential, the server remains compromise-blind.

#### 4.7 IPF 6

I&A technologies with an IPF of Six (IPF 6) is the first level on the IPF Scale that provides a significant ability to resist attacks against compromise of the credential. Not only does it use X.509 digital certificates with the SSL/TLS protocol (or Public Key with the SSH protocol), but it also uses a cryptographic hardware token – rated at **FIPS 140-2 Level 2** (or above). The token is used to generate and store the asymmetric key-pair on, thus eliminating an attacker's ability to copy the Private Key from the client machine[18].

In this implementation of an IPF 6 technology, there is little scope for an attacker to compromise the credential from a remote location:

- A dictionary attack (or a Rainbow table attack) is not feasible since there is no password database on the server to attack;
- A keystroke logging attack does not serve much purpose, since the the physical hardware token is necessary to complete the Client Authentication protocol in SSL/TLS or the Public Key Authentication protocol in SSH;

- Network traffic is encrypted by the nature of this protocol, so an attacker would not learn anything from snooping the network;
- Even if the attacker managed to steal the physical token, launching an attack on the token to access the Private Key will be useless, since most token implementations lock up the token after a small number – typically 3-5 - of incorrect attempts, thus rendering the token useless until the token is unlocked by a Security Officer of the legitimate user's company;

However, there is a possibility that an attacker – once having gained access to the legitimate user's client machine, and with significant knowledge of the client and server applications, could launch a social-engineering attack with software of his/her creation. The attack software could prompt the legitimate user for the password/PIN to the token; and if the legitimate user typed in his/her password or PIN – assuming this to be a legitimate request from an application on their PC – this would give the attacker access to the token.

For this attack to work, the attacker must have more than the average attacker's knowledge about hardware tokens, the SSL, TLS or SSH protocols, the look & feel of the client application that interacts with the hardware token, and finally, a great deal of knowledge of the server application to be able to manipulate it remotely.

Slightly less complex – but equally compromising - attacks might result in the legitimate user signing objects that he/she did not intend to sign.

IPF 6 I&A technologies are not compromise-blind, since the legitimate user would be aware of the loss of a hardware token (if it is external), or would be prompted for a PIN to the token. However, until an Administrator disables a specific cryptographic hardware token's credential, the server remains compromise-blind.

#### 4.8 IPF 7

In an IPF 6 I&A technology, if the cryptographic hardware token that stored the Private Key were embedded on the motherboard of the client machine as in a Trusted Platform Module (TPM)[19], or when an external cryptographic token is inserted into the client machine through some port, the Private Key to the legitimate user's credential would become accessible to software on the machine.

Should the attacker, using a keystroke-logger, capture the PIN or pass-phrase to the cryptographic hardware token, they would be able to compromise the legitimate user's credential and establish an authenticated session to the server.

I&A technologies with an IPF of Seven (IPF 7) differ from IPF 6 in that they use external PIN pads - or other physical authentication devices - that are hard-wired to the cryptographic hardware token. This allows the legitimate user to authenticate to the token directly without using the keyboard of the client machine for the authentication process, thereby increasing technologies at this level to resist attacks better than technologies at IPF 6.

IPF 7 I&A technologies are not compromise-blind, since an attacker would not only have to have physical access to the cryptographic hardware token, but also manipulate the hard-wired connections between the authentication input device and the cryptographic token. Servers continue to remain compromise-blind until an Administrator disables a specific credential.

#### 4.9 IPF 8

I&A technologies with an IPF of Eight (IPF 8) differ from IPF 7 in that they require the physical presence of the legitimate user at the machine where the protected resource is being accessed. This is the same machine where the user presents his/her credential and where the application performs the authentication.

By having the legitimate user be present at the machine that will perform the authentication, the machine operators can be assured that there has been no physical tampering of the connections between the cryptographic hardware token and the input device presenting the authentication credential. This difference distinguishes IPF 8 technologies from those at IPF 7 and adds to the technology's ability to resist attacks.

However, IPF 8 technologies are susceptible to compromise by a knowledgeable insider, someone who has unfettered access to the server.

IPF 8 I&A technologies are not compromise-blind.

#### 4.10 IPF 9

I&A technologies with an IPF of Nine (IPF 9) go above and beyond IPF 8 by adding the requirement that no single individual may gain access to the server individually, and that a quorum of legitimate users must be present and authenticated to gain access to the server resource.

This is typically implemented as an M of N control, where M is a subset of N, but represents a majority to establish a quorum. M and N are both odd numbers. Examples of an M of N control is when 3 of 5, 4 of 7, etc. legitimate users are required to authenticate to the server to access the resource.

By requiring such a control, implementers reduce the risk of a sole insider-attack on the resource. While it is still possible to compromise the resource through collusion of legitimate insiders, operators of such an infrastructure must manage that risk through adequate process controls.

IPF 9 I&A technologies are not compromise-blind.

#### 4.11 IPF 10

In keeping with typical scales, this author believes that I&A technologies with an IPF of Ten (IPF 10) - implying perfection - do not exist. There is no such thing as perfect security, and consequently there is no perfect identification and authentication technology.

### 5. COMPARISON WITH OTHER FRAMEWORKS

There are a number of frameworks and concepts that have been created in the field of identity management. The IPF is compared to some of these frameworks/concepts to place the IPF in perspective.

#### 5.1 The Liberty Alliance Framework

In response to an effort by Microsoft to consolidate User ID's and Passwords through a service called Passport, Sun Microsystems and 33 other companies created a consortium called the Liberty Alliance to provide an alternative to Microsoft's Passport technology[20].

The Liberty Alliance framework supports many authentication technologies - User ID/Password, OTP, X509 digital certificates, etc. - and uses Security Assertion Markup Language (SAML) to federate credentials through an identity service provider (IdSP). No matter how many web-service providers federate their identity management services to the IdSP, the end-user must still authenticate to the IdSP before a SAML assertion can be created to send to the web-service provider.

It is at the point of authentication at the IdSP that the IPF rating would come into play. The IdSP could offer different classes of identity management services based on the IPF ratings of the authentication technology used which would allow the web-service providers to manage the risk of their computer systems based on the IPF ratings they choose to accept in the SAML assertions.

So, the Liberty framework and the IPF Scale are complementary, each providing a different benefit to web-service providers and consumers.

#### 5.2 Oracle's Identity Governance Framework

Oracle and 7 other companies, in November 2006, founded the Identity Governance Framework (IGF) to address the governance of identity-related information across enterprise IT systems[21]. The project is now subsumed under the Liberty Alliance Identity Framework[22].

Most applications currently depend on tightly-coupled application programming interfaces (API) to repositories of information that includes the attributes of credential owners. For example, a Human Resource application has a need to lookup various attributes - such as Social Security Number, tax-related information, medical information, benefits information, etc. - of personnel whose credentials are stored in the HR database. The HR application may use one of many APIs - Java Database Connectivity (JDBC), Open Database Connectivity (ODBC), Lightweight Directory Access Protocol (LDAP), Simple Object Access Protocol (SOAP), etc. - to access this information depending on what type of repository holds the attributes. However, once the application is built to access a specific repository, they usually have little flexibility in dealing with the repository schema, or changes in policies with respect to the identity attributes.

The IGF allows the creation of loosely-coupled systems to reference such identity attributes without hard-coding them into applications, using XML-based protocols. Client applications use the *Client Attribute Requirements Markup Language (CARML)*[23] to specify their requirements for identity attributes, while the service providers use the *Attribute Authority Policy Markup Language (AAPML)*[24] to indicate the attributes they serve and the policies under which they serve up the attributes.

Even though the framework does provide a means to create loosely-couple applications, it still requires users to authenticate to some credential verifier before the user can use the application. While the IGF framework is not explicit in its documentation about what forms of authentication are required, given that the framework is now part of the Liberty Alliance, it can be safely assumed that the Liberty-supported authentication technologies will be supported by the IGF. Therefore, web-service providers can choose to define IGF policies, using AAPML, that serve up different levels of attribute data based on the IPF rating of the authentication technology used by the end-user.

So, once again, the IGF and the IPF Scale are complementary, providing two completely different benefits and services to web-service providers and consumers.

#### 5.3 NIST Special Publication 800-63

The National Institute of Standards and Technology (NIST) published Special Publication 800-63[2] that defines four *Levels of Assurance (LoA)* for electronic authentication

with Level 1 being the lowest and Level 4 the highest level of assurance. The NIST publication has some overlap with the IPF Scale.

Where they are similar is that they both focus on authentication technologies and their abilities to resist attacks. However, the NIST publication's authentication LoA becomes confusing because it combines secret sharing schemes with asymmetric key schemes within the same level. It is this paper's contention that due to the nature of asymmetric key-based authentication schemes at IPF-6 or above, they provide significantly better protection of credentials than secret sharing schemes. Thus, this author believes that the IPF Scale provides better clarity with respect to authentication technology than the NIST LoA framework.

Secondly, the NIST LoA framework is not sufficiently granular to distinguish between implementations of a specific authentication technology. As this paper described earlier, even when using an asymmetric key-based authentication technology (which is FIPS 140-2 Level 2/3 approved) it is possible to differentiate the protection factor rating into at least 4 factors - IPF-6 through IPF-9 - based on how the credential owner is authenticated to the cryptographic token. The NIST LoA collapses such differences into a single Level 4. It is this author's contention that the IPF Scale provides better risk-management with lesser ambiguity to implementers.

Where they differ are, the NIST publication factors in registration processes and identity proofing in addition to authentication technologies in determining the LoA, while the IPF focuses only on the authentication technology. The LoA is designed to provide a business-level assurance regarding claimants' identities and is broader in scope than the IPF Scale.

This author concedes that there is value in providing this level of business assurance regarding a claimants' identity, but believes that that a more useful scheme might be to create a quantitative *Identity Proofing Score* that assigns a quantitative value to various degrees of identity-proofing, and then combine it with a more granular IPF rating to arrive at a more granular Level of Assurance.

This author, additionally, believes that an LoA must take more factors into consideration when determining a level; some factors that need to be factored are:

- The operational practices of the verifier's infrastructure; a Relying Party can have little assurance in a Level 3 or 4 credential if the operations of the Registrar or the Verifier have weaknesses that are unknown until after a breach is discovered;

- The security state of the client machine from which the claimant is authenticating to the Verifier. Once again, a Relying Party can have little assurance in a claimants' credential if the machine from which they're using the token has been compromised;

More work needs to be done in this area to determine the optimal way to combine these factors.

#### 5.4 Microsoft's CardSpace

Microsoft introduced an identity meta-system, dubbed CardSpace, to simplify the management of computer-based identities[25]. Using standards such as WS-Security, WS-SecurityPolicy, WS-Trust, WS-MetadataExchange, SOAP, XML and SAML, CardSpace allows an end-user to submit a *Security Token* provided by an Identity Provider (IdP), to a Relying Party (RP) instead of a credential.

When an end-user needs to authenticate to an RP's site to access a secured resource, the user is presented with the option of submitting a security token in addition to other traditional forms of authentication supported by the RP. If the user chooses the option to submit a security token, they are given the choice of selecting a card from their local CardSpace environment on their client PC.

Unless the card they selected was created by a local "self-issued identity provider" on their PC, the user is redirected to make a request to a third-party IdP for the security token. The IdP, after having authenticated the requester, generates a security token - that is digitally signed and encrypted if there is sensitive information embedded in it - which is used by the end-user to submit to the RP. The RP after having verified the token, makes an authorization decision to allow/disallow access to the secured resource by the end-user.

CardSpace, in its first iteration, supports four methods of having end-users authenticate to the third-party IdP. These are:

- 1) User ID/Password;
- 2) Kerberos tickets;
- 3) X.509 digital certificates from either soft (file-based) or hard-tokens;
- 4) SAML security tokens created by the "self-issued identity provider"

The IPF Scale and CardSpace are complementary. CardSpace has effectively created four levels of authentication to the IdP, which is more coarse-grained than the IPF Scale. While this may be acceptable to many RP's, this author believes that it is not granular enough to manage risk effectively.

While more analysis is required to determine this, it should be possible to define an element in the WS-SecurityPolicy document created by RP's regarding the IPF rating of authentication that is acceptable to the RP. The IdP, upon receiving this security policy from the RP, can authenticate the end-user using an authentication credential with that IPF rating, and then assert if the end-user was successfully authenticated at that IPF rating in the security token generated by the IdP.

### 5.5 Higgins – Open source identity framework

Higgins is an open source identity framework from the Eclipse project, with a goal towards integrating identities and profile information across multiple sites and applications. Using standards such as WS-Trust, SAML, LDAP, OpenID, etc., it allows end-users to manage their identities and associated attributes using “*i-cards*”. On the surface, it appears to be the “open-source” equivalent to CardSpace, but Higgins inter-operates with CardSpace as one of the identity registries.

To a large degree, the mechanics of Higgins are similar to CardSpace. And to the same degree, the IPF Scale is complementary to Higgins too. Just as CardSpace redirects the end-user to an IdP for authentication and to acquire a security-token from a “*security token service*”, Higgins also supports a *Token Service* that allows end-users to authenticate to an IdP and generate a security token that can be handed to the RP. Since Higgins supports WS-SecurityPolicy, WS-Trust and WS-Security too, it is conceivable that the same element definitions for CardSpace that define an IPF rating, can be used within the Higgins framework.

### 5.6 Comparison summary

As can be seen from comparing IPF to various identity frameworks in this section, the IPF quantifies a unique aspect of authentication technology that makes it possible to complement and integrate with almost all identity management frameworks, while adding unique value to the field of risk management.

## 6. FURTHER RESEARCH

This is a first attempt at assigning a numerical rating to I&A technologies so they may be compared to each other in mitigating risks of compromise. There are many areas that this author believes requires further research:

- Validation of the assumptions of this model. Are there benefits and attacks that have been overlooked?
- Validation of the granularity of this model. Would a model that has more granularity – say from zero (0) to one-hundred (100) serve the community better?

- Identification of probabilities for compromises of I&A technologies with specific IPF ratings, based on historical breach data;
- Establishment of a repository with IPF values of known I&A technologies;
- Investigation about the possibility of creating an international database of breaches, with sufficient technical detail to assist researchers and practitioners on how to improve computer security;
- A methodology for assessing the risk of a given application system, and how implementers of the application may choose an I&A technology with a specific IPF to mitigate the credential risk.

## 7. CONCLUSION

There is a plethora of identification and authentication (I&A) technologies available to the information technology (IT) community today. With the exception of the “something-you-know, something-you-have and something-you-are” classification scheme, there has been no methodology based on the risk of compromise to credentials, to assist implementers of systems in choosing appropriate I&A technology to address their business risk. The Identity Protection Factor (IPF) rating is an attempt to create such a classification scheme.

Covering the gamut of shared-secret based I&A technologies and asymmetric-key cryptography based solutions that incorporate the use of cryptographic hardware tokens, this paper presents the IPF Scale and ranks known I&A technologies against this scale on the basis of their protection levels.

Using the IPF Scale and IPF ratings of individual I&A technology products, implementers of information systems will have a means to assess the relative strengths of I&A technologies and their ability to resist attacks to the credential.

The paper concludes that there is no perfect I&A technology, and that further research is necessary to validate the assumptions and granularity of this model, to create an IPF repository of products, and most importantly – to determine the probability of a compromise of each IPF layer based on historical breach data. This information will become crucial towards reducing identity-based risks in the future.

## REFERENCES

- [1] “Information Security for Lawyers and Law Firms” - Sharon Nelson, David Isom, John Simek, 2006, ISBN 1590316630
- [2] NIST Special Publication 800-63 – Electronic Authentication Guideline, William Burr, Donna Dodson, Tim Polk, April 2006 - [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

- [3] "Who goes there?: Authentication Through the Lens of Privacy" – Stephen Kent, Lynette Milett, 2003, ISBN-10: 0-309-08896-8
- [4] Liberty Alliance - [http://projectliberty.org/liberty/specifications\\_\\_1](http://projectliberty.org/liberty/specifications__1)
- [5] OpenID - <http://openid.net/>
- [6] Microsoft CardSpace - <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>
- [7] Sun Protection Factor (SPF) - [http://en.wikipedia.org/wiki/Sun-screen#Sun\\_protection\\_factor](http://en.wikipedia.org/wiki/Sun-screen#Sun_protection_factor)
- [8] Poor password Management may have led to bank meltdown – InfoWorld, February 2008 - [http://www.infoworld.com/article/08/02/04/Poor-password-management-may-have-led-to-bank-meltdown\\_1.html](http://www.infoworld.com/article/08/02/04/Poor-password-management-may-have-led-to-bank-meltdown_1.html)
- [9] "Galloping Gertie Collapses November 7, 1940" - <http://www.ws-dot.wa.gov/TNBhistory/Connections/connections3.htm>
- [10] Interstate 35W Bridge Collapse website - <http://www.dot.state.mn.us/i35wbridge/index.html>
- [11] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.
- [12] How to hack biometrics - <http://www.theinquirer.net/en/inquirer/news/2005/07/30/how-to-hack-biometrics>
- [13] Attacks on Biometric Systems: A Case Study in Fingerprints - [http://biometrics.cse.msu.edu/Publications/SecureBiometrics/UludagJain\\_BiometricAttacks\\_SPIE04.pdf](http://biometrics.cse.msu.edu/Publications/SecureBiometrics/UludagJain_BiometricAttacks_SPIE04.pdf)
- [14] Phishing attack targets one-time passwords - [http://www.theregister.co.uk/2005/10/12/outlaw\\_phishing/](http://www.theregister.co.uk/2005/10/12/outlaw_phishing/)
- [15] The TLS Protocol Version 1.0 - <http://www.ietf.org/rfc/rfc2246.txt>
- [16] SSH Authentication Protocol - <http://www.ietf.org/rfc/rfc4252.txt>
- [17] A One-Time Password System - <http://tools.ietf.org/html/rfc2289>
- [18] Security requirements for cryptographic modules - <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [19] Trusted Platform Module FAQ - <https://www.trustedcomputing-group.org/faq/TPMFAQ/>
- [20] Alliance forms against Microsoft Passport – USA Today, December 2001 - <http://www.usatoday.com/tech/news/2001/12/20/anti-passport-alliance.htm>
- [21] Oracle Identity Governance Framework (IGF) - <http://www.oracle.com/technology/tech/standards/idm/igf/index.html>
- [22] Liberty Alliance Identity Governance - [http://www.projectliberty.org/index.php/liberty/strategic\\_initiatives/identity\\_governance](http://www.projectliberty.org/index.php/liberty/strategic_initiatives/identity_governance)
- [23] Client Attribute Requirements Markup Language (CARML) - <http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-CARML-spec-03.pdf>
- [24] Attribute Authority Policy Markup Language (AAPML) - <http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-AAPML-spec-08.pdf>
- [25] Introducing Microsoft CardSpace - <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>
- [26] Modelling the Relative Strength of Security Protocols, 2nd Workshop on Quality of Protection, Oct 30, 2006, Alexandria, VA, USA - <http://www.scf.usc.edu/~hochung/papers/qop18-chungneuman.pdf>