Brewing Next Generation Identity

Kalman C. Toth

kalmanctoth@gmail.com

Abstract

The growing popularity of mobile apps, the "bring your own device" (BYOD) phenomenon, cloud computing, and big data, seem to have created the perfect storm for traditional identity technologies and solutions. Service providers - and certain users too - are increasingly aware that the features and benefits offered by an identity solution are worth nothing if a crafty attacker breaks through critical design elements, exposes secrets and private information, and thereby facilitates user impersonation and fraudulent transactions. This paper provides a synopsis of the identity problem (as I see it), discusses essential weaknesses of legacy identity technologies, and puts forward a plausible vision and operational concept for a next generation identity solution that overcomes many of weaknesses of these legacy technologies.

Biography

Kal Toth *has over 30 years of technical, consulting and management experience working for small, medium and large-sized technology companies including aTrust Inc., Hughes Aircraft, Datalink Systems Corp., the CGI Group Inc., the Software Productivity Centre (Vancouver, BC), and Intellitech Canada. He is past Executive Director of the Oregon Master of Software Engineering (OMSE) program at PSU and has delivered systems/software engineering and project management courses at PSU, OSU, TechBC, Simon Fraser, U of Alberta, and UBC. He completed his Ph.D. in systems engineering at Carleton University (Canada) and is a registered professional engineer with a software engineering designation in British Columbia.*

1 Introduction

For some time now I have advocated and refined a user-centric model (see refs.[21-24]) for personal identity to counter certain weaknesses of server-centric identity solutions. Rather than allocating the responsibility for storing and managing personal identities to service providers and applications in the cloud, I have suggested that next generation identity solutions enable individuals to embed their identifying information into their personal devices, for example, their smart phones, smart cards, tablet PCs, and laptops. Naturally, such an approach opens up many new challenges for the software quality engineer.

Although privacy laws oblige enterprises to safeguard private and identifying information of customers and employees, their record has not been stellar. 2014 was not a good year for big targets like Target, Home Depot, JPMorgan Chase, Athenahealth and others [1]. We have plenty of evidence that the server-side of the web is rapidly losing ground in its battle against hackers, malware and other types of electronic abuse.

I believe the root of the problem is that enterprise servers and server farms are, by definition, massively complex, collectively containing virtually all of the identities and private data of our global population. It is no wonder that servers are the primary targets for online hacking, breaches, and identity theft that enable fraudulent use of identities. In comparison, end-users, numbering 270M in the US alone [3], are collectively much more numerous, are widely dispersed, and are mostly low-yield targets. With the exception of notables like Bill Gates and Warren Buffet, the average return-on-hacking effort against individuals will be much less than that realized by attacking enterprise and service provider repositories. The tide should be shifted from a server-centric identity model to a user-centric one that strengthens user control over their identities, while reducing opportunities for exploit on the server-side. Such models have merit and should be widely discussed.

2 Elevated Identity Assurances Mitigate User Masquerade

Fraudulent web transactions arise by way of “user masquerade” (a.k.a. impersonation), such e-fraud damaging targeted victims, their associates, and their e-business providers.

For example:

- Scam artists register pseudonyms to obtain accounts and credentials to defraud victims
- “Dumpster-divers” acquire records and credentials of victims to obtain accounts in their names
- Hackers and phishers acquire electronic credentials of their victims to break into their accounts to mount various fraudulent transactions.

Recommended impersonation prevention measures include elevating identity assurances by:

- Conducting thorough due diligence/vetting of users and their asserted identities (a.k.a. “proofing”)
- Vetting in proportion to perceived transactional risks
- Deploying technologies, policies and administrative procedures specifically designed to collectively prevent fraud and exploits enabled by way of identity theft and server-side breeches.

3 Weaknesses of Traditional Password/PIN Authentication

Traditional schemes have long been demonstrated to present ample opportunity for user masquerade. Employing a number of fairly straight-forward exploits and/or readily available software tools, a malicious attacker can defeat traditional PIN/password authentication by acquiring the victim’s secrets and fraudulently using such private knowledge to access and tamper with their electronic accounts. At a minimum, it is essential to adopt best password management procedures which include appropriate procedures for creating sufficiently strong passwords and PINs; their safekeeping; augmenting them with

non-guessable security questions; safe account reset procedures; and elevated awareness of the risks of social engineering attacks and scams.

Of course, the routine reuse of the same and/or similar passwords/PINs greatly exacerbates the above risks. This is because the number of opportunities for a malicious attacker to acquire similar passwords/PINS increases together with the number of accounts protected by these similar passwords. Identity federation and single sign-on (SSO) together with multi-factor authentication (mFA) schemes can significantly reduce this password reuse risk.

4 Potential and Limitations of Single-Sign-On and Federation

Pioneered by Liberty Alliance and other players in the late 1990s and early 2000s, single-sign-on (SSO) consolidates identity management at a single point, a federated identity service, which enables the user to be authenticated in one place (or at least in a small number of places) while provided access to multiple web resources. This greatly reduces the number of PINs and passwords required. SSO and identity federation thereby reduce the need and motivation to reuse the same password or PIN for multiple purposes and reduces the opportunities for password/PIN compromise. OpenAM, an open source solution supported by RockForge, Oracle, PingIdentity and others, can be used to implement such identity federating solutions.

5 PKI and PGP: Positive Features and Shortcomings

Public Key Infrastructure (PKI), underpinned by digital certificate technology and extensively deployed across the Internet, automates the deployment of public-private encryption key pairs for secure communications, message transmission, and document safe-keeping. A digital certificate, conforming to the X.509 digital certificate standard, includes a public encryption key embedded in the certificate that is paired with a private key stored outside the context of the digital certificate. A remote party who does not have knowledge of the private key can perform tests to verify that the party claiming ownership of the certificate and contained public holds the matching private key. PKI implements a hierarchical trust model wherein certificate authorities successively distribute digital certificates to dependent certificate authorities, Internet servers, and end-user devices. Digital certificates and their corresponding private keys are distributed by certificate authorities to other certificate authorities, to servers, and to end-user devices. Certificate authorities have the option of employing qualified human agents for 3rd party identity proofing and verification.

I have observed the following deficiencies of PKI:

(a) Using qualified independent certificate authorities, effective for verifying and tracking the identity of service providers, does not scale for human beings who outnumber servers by orders of magnitude;
(b) Because public-private key pairs are generated by certificate authorities and subsequently distributed electronically, such key pairs are vulnerable to compromise during distribution;
(c) Because X.509 digital certificates only specify the certificate holder by a common name or identifier, identities of persons cannot be specified comprehensively for commercial and other such applications;
(d) Digital certificates do not readily bind with other personal identifying information of an owner such as digital photographs or personal identifying information (e.g. passport, driver's license, certifications);
(e) Although digital certificates enable relying parties to verify that the digital certificate owner has the private key that matches the public key of a digital certificate, PKI does not incorporate personal identifying information that reliably distinguishes the certificate owner from other users;
(f) PKI does not provide assurances that the private key is strongly bound to the certificate owner;
(g) PKI does not incorporate identity proofing and binding capabilities that provide objective evidence to relying parties that an independent party has attested to the identity of the digital certificate holder;

(h) Because X.509 certificates are associated with a single public-private key pair, typically multi-purposed (e.g. used for digital signing, encryption, email, FTP, etc.), the risks of encryption key compromise are elevated over other approaches.

Pretty Good Privacy (PGP), meanwhile, was introduced to automate the deployment of public-private key pairs among persons (peer-to-peer) to secure communication channels, transmitted messages, and documents among PGP users. In contrast to PKI, PGP implements a web of trust model wherein individuals issue digital certificates to each other. An end-user, having installed PGP software on their personal computer, creates an X.509 digital certificate containing a single public key with matching private key stored on the user's computer. PGP enables an informal process whereby a first user can send such a certificate to a second PGP user who digitally signs and returns the certificate to the first user. By retaining the single private key of a digital certificate within the owner's computing device, PGP reduces the risk of exposing and compromising this private key. This approach for creating and sharing digital certificates can be replicated among users with PGP software on their computing devices. PGP users can present one or more signed digital certificates to relying parties (users) which elevates identity assurances when presented to other parties.

PGP has the following deficiencies:

(a) Because X.509 digital certificates only specify the certificate holder by a common name or identifier, identities of persons cannot be specified comprehensively for commercial and other such applications;
(b) Digital certificates do not readily bind with other personal identifying information of an owner such as digital photographs or personal identifying information (e.g. passport, driver's license, certifications);
(c) Although digital certificates enable relying parties to verify that the digital certificate owner has the private key that matches the public key of a digital certificate, PGP does not incorporate personal identifying information that reliably distinguishes the certificate owner from other users;
(d) PGP does not provide assurances that the private key is strongly bound to the certificate owner;
(e) PGP does not incorporate a formal identity proofing process whereby relying parties are provided objective evidence of a user's identity;
(f) Because X.509 certificates are associated with a single public-private key pair, typically multi-purposed (e.g. used for digital signing, encryption, email, FTP, etc.), the risks of encryption key compromise are elevated over other approaches.

6 Role of Multifactor Authentication

Multiple factors can be applied jointly to reduce the probability of failed authentication due to the compromise of any one factor. For example, the following factors could be applied in various combinations to achieve more than one factor of authentication:

- What the user knows (like a PIN or password)
- What the user has or holds (for example, possession of their smart card, smart phone or tablet PC)
- What the user is (facial, iris, fingerprint, hand geometry, voice print, or key stroke biometric).

Probably the best known examples of 2-factor authentication are using a PIN together with a banking debit card, and using a hardware token that generates a one-time-password (OTP) for remote terminal logon. Another possibility is 3-factor authentication using one of the above biometrics together with knowledge (a PIN or password), and possession of the access device (say a smart phone).

When used together, MFA and SSO/federation have the potential of significantly scaling back the need to manage large numbers of passwords/PINs by decreasing the motivation for specifying and using many passwords. Next generation identity should closely integrate multi-factor authentication schemes with federated SSO frameworks to reduce the risks of reused, weakly specified, and poorly managed password/PIN systems.

7 Role of Biometric Authentication

Biometric authentication is an increasingly critical ingredient for preventing user masquerade and elevating authentication assurances. Fingerprint, facial, signature, voice, iris and other biometric authentication schemes are commercially viable for deployment on user platforms (e.g. PCs and smart phones). Ma in [20] reports the relative accuracy of available biometrics in terms of false positive rates with facial recognition at 43%, fingerprint at 30%, signature at 28%, voice at 20%, and iris recognition at only 0.47% (which explains the growing interest in iris biometrics). Meanwhile, emerging biometric schemes leveraging the body's venous, nervous and DNA systems are being researched.

Relevant Observation: User preferences for each biometric scheme, matching accuracy, matching performance, human risks factors, and compatibility with the individual circumstances can vary. This implies that:

- Next generation solution architectures should be designed specifically to accommodate a range of biometric options for remote user authentication;
- Biometric scanning/matching should be embedded in the user's personally held and controlled platform;
- The user's platform should be resistant to tampering to protect the user's internally stored biometric minutia (a.k.a. biometric templates);
- The identity service should acquire objective evidence that the user is in control of their platform;
- The system architecture should be extensible, accommodating add-on biometrics in a modular fashion as they become available.

8 Browser Vulnerabilities

Well-documented by the Open Web Application Security Project (OWASP) [4], browser vulnerabilities can be mitigated by implementing best programming, configuration, and usage practices. However, in the face of constant feature creep and fixes, externally mounted browser exploits are unlikely to abate any time soon rendering browser-based user authentication to be of unacceptably high risk in many business contexts. This has stimulated considerable interest in a variety of "out-of-band" authentication schemes that avoid in-browser authentication risks.

9 Benefits of Out-of-Band Authentication Schemes

Out-of-Band (OOB) Authentication over an alternate channel between the user's platform and the identity service provides the user an independent path for user authentication, reserving the browser channel for transaction flow. A compelling risk mitigation strategy is to re-authenticate the user immediately prior to committing a critical transaction (e.g. high value electronic funds transaction). For successful compromise, the attacker must be able to simultaneously penetrate both the OOB authentication channel and the browser channel.

Certain SMS-based OOB schemes using smart phones have been shown to be vulnerable primarily because SMS text messaging typically runs in the clear [15]. To take advantage of operating as an independent authentication channel, messages running over the OOB channel must be encrypted and digitally signed, and the communications protocol must be resident to Man-in-the-Middle (MITM) attacks.

10 Benefits and Limitations of Fast-Identity Online (FIDO)

Fast Identity Online [29] was launched by a consortium of technology companies providing hardware-oriented authenticators (e.g. OTP and smart card tokens) designed to positively authenticate the device

holder. FIDO has been developing a standard set of methods and protocols by which such devices can integrate with online web services, the aim being, to replace existing password usage.

FIDO authenticators generate public-private key-pairs on the client where the public key and an associated “handle” is registered with the online service/application during initial password-based authentication. Subsequently, login access is accomplished by way of a public/private key protocol and challenge that, in effect, substitutes the public/private key pair for the password being currently used (private key is the user’s secret; the public key and challenge are used to verify proof-of-possession). While FIDO reduces dependence on passwords, their authenticators do not support the specification or proliferation of user identities characterizing the user’s attributes and/or life events. The proofing of users remains the responsibility of the service/application, and personally identifying information continues to be held in server-side identity repositories which are vulnerable to large-scale breaches.

11 Relevance of Identity Assurance

While authentication assurances can be elevated by deploying multiple authentication factors, they do not identify other attributes that characterize the individual being authenticated. They only confirm that the person being authenticated is, indeed, the same person. In contrast, identity assurance involves life events, observations and endorsement made by independent parties who can attest to such aspects of the person’s identity. For example, birth date and place, contact information, education, citizenship, skills, financial instruments, business affiliates and so forth are attributes of a given individual that cannot be captured by biometrics, and are (or should be) independent of their secret knowledge (PINs/passwords).

Note that many of these attributes can be found in existing physical credentials such as birth certificates, citizenship certificates, driver’s licenses, passports, diplomas, credit cards, and business cards.

When communicating with a remotely located persons or services, collaborating parties need assurances as to the true identity of the parties. To support this requirement, the identifiers and attributes of a person (a subject), including legal, common, and pseudonyms, should be independently attested by other persons who may elect to issue an identity artifact to that person. The level of identity assurances achieved by such an issuer depends on the extent to which the subject person is known by the issuer (familiarity), and the vetting and proofing competencies of the issuer. Relevant competencies for an issuer include proofing and vetting skills, objectivity, questioning skills, professional oversight by a governing body, and applicable code of conduct possibly sworn by oath - notary publics are exemplars. Identity assurances increase as the number of years that an issuer has personally known a subject, though not necessarily linearly. Identity assurance levels are also proportional to the above listed range of vetting and proofing competencies. Because objectivity and independence may conflict with familiarity, certain professionals, such as notaries and agents of credential issuing organizations, may be obliged to decline proofing and vetting a person who is too closely related to the issuer by way of family and employment.

NIST and Kantara in [8] and [9] respectively recommend implementing progressively increasing levels of identity proofing and verification thereby significantly and prudently reducing the risk of bogus identity issuance.

Although, document proofing and in-person verification procedures are time-consuming activities, there is little doubt that they significantly reduce the risk of fraudulent credential issuance and consequential transactional risk. Such procedures should be an integral part of any identity solution mandated to govern value transactions in the banking, finance, healthcare and similar industry sectors. Solutions should bind the level of identity assurances performed to the credentials issued, and then use this information to mediate high value transactions and access to critical information.

12 Role of Trusted Execution Environments and Modules

User Authentication can be performed by a software component (an “app”) running on the user’s platform that runs independently, but in cooperation with, the browser. Such a component could be designed to implement biometric and/or multi-factor authentication schemes independent of the browsing channel thereby avoiding in-browser authentication vulnerabilities. Nonetheless, such a component would be vulnerable to malware running on the user’s platform leaving open the possibility of remote hackers, phishing attacks, man-in-the-middle (MITM) attacks, and BOTs breaking the embedded authentication mechanisms. For example, malware could lurk within the run-time operating system of the user’s platform waiting for an opportunity to activate and tamper with authentication software thereby exposing private and secret user information.

A trusted user platform capable of isolating the authentication logic and the user’s sensitive information store from malware injected into the platform’s operating system would greatly mitigate such risks.

13 Characterizing Next Generation Identity Solutions

Next Generation Identity Architectures must overcome the range of vulnerabilities and technology challenges with which today’s legacy solutions are barely able to cope. They must support the highly complex interplay between multi-faceted applications running in various run-time contexts, multiple identity repositories from different vendors, and disparate user platforms including PCs, tablets, smart phones (e.g. Android, I-phone, Blackberry) … all exacerbated by today’s “bring-your-own-device-to-work” trend.

The critical design attributes that must be incorporated into the identity architecture should include the following functions and features:

- Multi-factor authentication of the user on their computing platform that includes PIN/password knowledge, proof of platform possession, and at least one biometric authentication factor. This mitigates the risks associated with single-factor authentication schemes and elevates identity assurances for both e-business providers and users;
- Hardware and/or software mechanisms that isolate user authentication processes and private user data from malware that may penetrate the user’s run-time environment executing on their computing platform;
- Procedures that vet users by way of document proofing and verification, and mechanisms that bind users’ physical credentials to their identities and electronic credentials. These credentials are locally available on the user’s platform, and also remotely to authorized identity and service providers;
- Architectural elements that isolate remote user authentication schemes and processing from primary application access and transaction flows;
- Components and mechanisms that federate user authentication for the benefit of multiple service provider applications, centralizing, hardening, and off-loading critical authentication processing from core information processing services;
- Provisioning the appropriate mechanisms and protocols needed to ensure that the communication channels connecting users to service provider applications and identity services, and application services to identity services, are reliable and highly resistant to MITM, MITB, and malware exploits mounted by phishers, hackers, BOTs and others.

The total risk posture of an identity solution is only as strong as the system architecture’s binding strength. For example, a reliable biometric authentication technology is not very useful if an attack can be mounted that bypasses this functionality. It is therefore essential that the software components and protocols implementing the architecture’s binding mechanisms also be highly trusted - resisting

determined Man-In-The-Middle (MITM), Man-In-The-Browser (MITB), and malware attacks by phishers, hackers, BOTs and other attack agents.

In the final analysis, the identity solution's architecture is the essential glue that binds distinct roles and responsibilities of each technology element into a cohesive whole, mitigating the baseline risk of electronic fraud by way of the various user masquerade/impersonation scenarios.

14 Vision and Operational Concept

The above-articulated analysis has led me to formulate the following identity vision and operational concept which I offer to the reader. Your constructive feedback is invited.

a) Users own personal identity devices that contain their electronic identities with associated encryption keys which they use to (a) identify themselves and (b) secure collaboration with other parties.
b) Users (e.g. consumers, employees, admins, and managers) install trustworthy identity applications (apps) on their personal identity devices and servers to safeguard and manage their identities.
c) Users can exchange electronic identities with other users and servers having an identity application.
d) Identities are specified by electronic artifacts (I call them "e-credentials"). Each e-credential of an owner includes personally identifying information chosen by the owner including identifiers, attributes and images associated with the owner. The identifiers may be pre-existing (e.g. social security number) or may be created by the owner. Attributes can be physical characteristics and life events. Images selected by the owner may depict the user themselves or physical artifacts with which the user openly or secretly identifies (e.g. an article of clothing, a favorite object, or a super-hero).
e) The identity device owner can specify "true", pseudo-anonymous and anonymous identities. A "true" identity could be a driver's license, a credit card, or a business card; a pseudo-anonymous identity is one that is known only to selected friends and associates; an anonymous identity is a secret handle known only to the owner (e.g. for web blogging purposes).
f) After installing their identity app, the owner enrolls their authentication data (e.g. PIN and/or a biometric) and defines their personal profile including their identifying images and contact info.
g) Subsequently, the owner submits already specified e-credentials to collaborating parties requesting them to proof and attest to their identities including accompanying personally identifying information. The owner's identity app cryptographically binds their identity to requests such that the owner cannot repudiate having submitted the request. Both application servers and users can attest identities.
h) In response to receiving an e-credential request, an owner uses their identity app to inspect and proof the provided e-credential and personally identifying information. If satisfied, the recipient uses their identity app to attest to the requester's identity, cryptographically bind their identity and attestation to the e-credential subsequently issued to the requester. The issuer cannot repudiate this action.
i) Once e-credentials are exchanged, identity apps can use the cryptographic properties of e-credentials to establish mutually trusted channels for transactions and document notarization.
j) When initially exchanging e-credentials, the identity apps can generate and exchange one-time-passwords (OTPs) over alternate channels (e.g. in-person, phone, texting, email, etc.).

15 Why this Operational Concept is Promising

a) Given the identity app controls both the owner's enrolled authentication data and the owner's e-credentials, the app strongly binds owners to their identities and, in turn, enables the identity app to employ the encryption keys associated with each e-credential to remotely bind collaborating owners.
b) As suggested by Asokan [6], identities should have multiple public/private crypto key pairs, each pair designated to perform distinct cryptographic functions. For example, cryptographic functions

designed to achieve confidentiality, integrity, originator authentication, and non-repudiation should use distinct key pairs. Breaking of one cryptographic key does not break the others.

c) Private keys associated with any given e-credential are “secrets” of the owner and must not be revealed by the identity device and app. This ensures that an owner’s identity acquired by way of identity theft or a server-side breach cannot be used to impersonate the owner. Remote parties (users and servers) will be able to conduct tests to verify proof-of-possession of these private keys.
d) Ideally, a given owner’s e-credential should be proofed and attested by multiple parties. Such a strategy elevates assurances that the e-credentials actually represent the person specified. Furthermore, the likelihood that an identity thief could conspire to issue such multiply-attested e-credentials, each of which cannot be repudiated without detection, would be significantly reduced.
e) Once e-credentials have been successfully exchanged between collaborators, man-in-the-middle (MITM) and phishing attacks are prevented because the attacker does not possess either collaborating party’s private keys. Exchanging an OTP out-of-band to bootstrap e-credential exchange similarly thwarts MITM and phishing attacks.
f) An e-credential, attested to using an e-credential of the owner and stored on a backup device/server of the owner, or held in escrow, can be used to create a “poison-pill” that only the owner can activate, for example, to disable or wipe their device if lost or stolen.
g) Of course, identity app must be trustworthy and isolated from tampering by unintentionally hosted malware and faulty software. This should be achieved by employing a trusted operating system and platform (e.g. trusted execution environment, trusted platform module (TPM) or trust zone). The identity device should also safeguard the user’s private information, authentication data, and secret keys in a protected memory store that can only be accessed by the identity app.

16 How this Approach Compares to Other Solutions

In contrast to Public Key Infrastructure (PKI) [13], e-credentials can be specified richly (suitable for consumer identities); have multiple public/private key pairs, each for well-specified purposes (hence less vulnerable), and e-credential can be attested and issued by multiple collaborating parties (other users as well as service providers/applications). This significantly elevates identity assurances by reducing the risk that a compromised identity will proliferate across the web.

Like PGP [14], I have proposed that private keys associated with an owner’s e-credentials be strongly protected by the identity app and not revealed to other parties. I also advocate that other parties be obliged to routinely execute remote proof-of-possession tests that verify that the e-credential owner controls the associated private encryption keys. In contrast to PGP I have also advocated that both ordinary users and designated identity authorities be capable of proofing, attesting and issuing identities to other users as well as to service providers.

While FIDO [29] reduces dependence on passwords, their authenticators do not support the specification or proliferation of user identities. Personally identifying information continues to be stored on servers where they remain vulnerable to server-side breaches. The approach I have advocated specifies e-credentials that, if stolen, cannot be used to easily create fraudulent identities because the private keys are controlled by owners and collaborating parties are obliged to conduct proof-of-possession tests. This strategy would prevent identity thieves employing stolen identities because they would not be in possession of users’ private keys.

17 Role of Software Quality Engineering

It is reasonable to argue that experienced software quality engineering practitioners are ideally placed to implement such a mission-critical identity vision and concept. Certainly, information security expertise, including experience with the application of cryptographic components and related security protocols will

be essential. However, we should not forget that other software quality engineering skills and processes will also be critical success factors, including: functional and operational requirements analysis and specification, architectural design know-how, reviews and walkthroughs, static code analysis and inspections, multiple levels of testing, penetration testing, independent quality assurance, and independent (3rd party) verification and validation (IV&V).

References

[1] Lt. Dan, A 'Perfect Storm' for Data Breaches, Experian, Dec. 17, 2014
[2] Draft NIST Special Pub. 800-157, Guidelines for Derived PIV Credentials, March 2014
[3] Miniwatts Marketing Group, 2014
[4] Open Web Application Security Project (OWASP) Top 10 Project, https://www.owasp.org, 2013
[5] National Institute of Standards and Technology SP-800-63-1, "Electronic Authentication Guideline", 2011
[6] Asokan et. al., "On the Usefulness of Proof of Possession", PKI workshop, 2013
[7] Zaker Soltani, "Improving PKI: Solution Analysis in Case of CA Compromisation", 2013
[8] NIST Special Pub. 800-63-2 Electronic Authentication Guideline, August 2013
[9] Kantara Initiative, "Identity Assurance Framework, Service Assessment Criteria", April 8, 2010
[10] Adeoye, A Survey of Emerging Biometric Technologies, Int'l Journal of Computer Appl, Nov. 2010
[11] ITU, X.1252, "Baseline Identity Management Terms & Definitions", April 2010
[12] RSA Laboratories, B. Kaliski, PKCS #5: Password-Based Cryptography Spec'n, V2.0, Sept 2000
[13] Internet X.509 PKI and CRL profile, Network Working Group, 2008
[14] Finnet, IETF, Open PGP Message Format, Network Working Group, Nov. 2007
[15] Gary Blair, SMS-delivered two-factor authentication will be dead in three years, 2007
[16] Kalman C. Toth, A Practical Identity Management Reference Implementation, CATA, Honolulu, Hawaii, 2007
[17] K. Toth, Identity Management Systems, tutorial for IEEE COMPSAC, Chicago, September 2006
[18] Toth, Persona Concept for Web-Based Identity Management, Int'l Conf on Privacy, Security & Trust, 2006
[19] Sarbanes – Oxley Act of 2002, top management accountable for financial accuracy of corporate information
[20] Ma, L., et.al., "Efficient iris recognition by characterizing key local variations". *IEEE Trans. Image Processing. 2004*
[21] K.C. Toth, M.Subramanium, Req'ts for the Persona Concept, RHAS'03 workshop, Monterey, 2003
[22] Toth, Subramanium, Persona Concept: MobEA, Budapest, 2003
[23] Toth, Subramanium, Persona Concept for Privacy and Authentication, In'l Bus & Eco Res. Jrn,2003
[24] Toth, Subramanium, Chen, Persona Concept for Privacy and Authentication, IABR Conf, 2003
[25] K. Toth, Information Security Architectures, AFCEA, Hawaii, 1990
[26] K. Toth, Towards an Improved Information Security Model, 1st Can. Comp. Security Conf, Jan'89
[27] K. Toth, Data Encryption Equipment Specification, Internal report specifying CryptoNet, 1986
[28] Implementing Mutual Authentication Using TLS/SSL: http://en.wikipedia.org/wiki/Transport_Layer_Security
[29] Fast Identity Online (FIDO) specification: www.fidoalliance.org
[30] FIPS PUB 201-2, Personal Identity Verification of Federal Employees and Contractors
[31] DoD Common Access Card Standards, http://www.cac.mil/common-access-card/
[32] Payment Card Industry Standards Site: https://www.pcisecuritystandards.org/
[33] RSA Encryption Standards: see http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29
[34] Elliptical Curve Encryption: see http://en.wikipedia.org/wiki/Elliptic_curve_cryptography