Identity Firewalls: An approach to overhauling the identity infrastructure

Version: 1.1

September 23, 2005

Arshad Noor

StrongAuth, Inc.

Abstract

The dramatic growth of computers on the Internet in the last decade, has placed inordinate pressure on structural controls governing trust in this environment. As a consequence, computers and computer users are under unprecedented attack - with identity theft and phishing ranking very high on the list. Despite commercial Public Key Infrastructure (PKI) technology being available for more than two decades, its use has been underwhelming in addressing these problems on a large scale. In this paper, a concept is presented to revamp the authentication infrastructure, using public key cryptography. Its anticipated benefits are a reduction in identity theft; the possible elimination of phishing; an improvement in the level of trust in the computing environment, and a lowering of overall costs to society in the long term.

Table of Contents

I. Background

Never in the history of computerization, have computer users had to deal with so many credentials for their day-to-day activities: Credentials from the bank, the brokerage, the insurance company and the credit card company. Credentials from local department store, specialty stores, grocery stores, airlines, hotels and car rental companies. Credentials for e-mail services, personal services, government procurement sites, alumni associations, local libraries, political organizations. And, of course, credentials for the company network, company e-mail, company VPN and company applications.

We are awash with credentials! While the goal of credentials - to prevent unauthorized users from accessing privileges granted to you – is laudable, the number of credentials possessed by average computer users has made the purpose counter-effective. Most people – including security-conscious professionals – resort to using similar passwords (or small set of passwords), or writing them on a piece of paper for the multitude of credentials in their possession.

Forces from the dot-com era have given companies the impetus to revamp business processes to take advantage of the Internet. However, access to sensitive information, which was controlled in the past, is now a mere login-screen away to anyone in the world with an Internet connection. This has given rise to new forms of attacks – most notably, phishing and keystroke-loggers - to siphon away credentials to valuable service accounts. As a result, Identity Theft has been designated the fastest growing crime in the US, with approximately, 9.9 million victims and approximately, US $5 Billion in losses in 2003[1].

II. Causes

There are many reasons for the present state of affairs. These are:

1. **An unprecedented number of naive computer users connecting to the Internet**. Without appropriate knowledge & security counter-measures, or with inadequate or non-existent security practices, these users became fodder for the scores of increasingly sophisticated criminals poaching the Internet.

2. **Inappropriate technology for the times**. User IDs and Passwords were created more than 40 years ago to deal with authentication issues inside closed, non-networked systems, housed within facilities that were reasonably well guarded (due to the cost of the machines, rather than the value of the data). It was only in the last 20 years that mere mortals could procure computers for themselves, enabling them to connect to some form of network. While this popular form of secret-key based credential was appropriate for a collegial, or budding network environment, it is no match for the more than ½ billion users connected to the “alway s on, high-speed” Internet.

3. **Inappropriate use of information in business processes**. Many years ago, programmers started using the Social Security number in the US, as a convenient method of identifying people in databases used by software. In addition, to make it convenient to provide services and support over the phone, businesses started programming “publ ic” information into their databases as secret identifiers. Mothers' maiden names, high school graduation year, high school attended, date of birth, etc. What began in convenience, is now the basis of offering individuals products and services over the phone. This is the reason why innocuous pieces of information from mailboxes and garbage cans have become so valuable to identity theives.

4. **Inadequate investment**. Security is a cost of doing business. It neither increases revenues, nor does it lower costs directly. As such, it is always difficult to justify spending more money on risk mitigation, unless the problem is obvious to everyone. Secondly, the culture of short-term thinking in US companies precludes making long-term risk-mitigation investments. As such, even when problems are obvious, most companies choose the path of least resistance, which are typically short-term solutions, serving as a panacea, but doing little to solve festering problems.

5. **Inertia**. User ID and Passwords have been around for more than 40 years. It exists on every modern operating system, database and multi-user application. System and application developers have been conditioned into thinking of secret-key based credentials for their new applications, simply because its out there already. As such, unless there is a strong impetus from the business users – as in military organizations – most IT organizations never think beyond secret-key based credentials.

III. Solution

Any solution to deal with the multitude of problems in this space must overcome the above-mentioned causes. This author proposes one that not only addresses the above, but also solves some other problems that are not directly related to the management of identity credentials.

Identity Firewalls is the term given to the concept of using consolidated X.509v3 compliant digital certificates along industry lines, in combination with external 2-factor cryptographic tokens, coupled with laws that protect the privacy of users.

Lets break this down component by component to see what it means.

Almost all transactions of a human being in industrialized nations such as the US, can be categorized into seven (7) industries. These are:

1. **Healthcare**. From the moment someone is born, till the day they die, a human must deal with either a doctor, a hospital, a pharmacy, a testing laboratory and potentially, some company/entity that serves their healthcare coverage needs financially.
2. **Education**. Almost all humans in industrialized nations will attend school. Many will attend college and some will go onto post-graduate Universities. Many will continue with some form of education even when fully employed and join professional associations based on their educational qualifications.
3. **Financial**. Almost all adults will deal with a bank at some point in their lives. Many will also deal with investment brokerages, mutual fund companies, insurance companies, credit unions, credit card companies and many other forms of financial service companies.
4. **Retail**. Given the Internet of the 21st century, there are millions who will purchase goods and services over the Internet. Books, clothes, music, airline tickets, hotel rooms, cars, groceries and many more things that are not easily categorized.
5. **Government**. Every human in every nation will deal with the government. Whether it is just with the registrar of births and deaths, the census, or with the tax authorities and the motor vehicle department, most citizens will interact with the government of their country for some transaction or the other.
6. **Employer**. Anyone that works in a company of any size, using computers, will require a credential that will permit them to interact with the computing resources of that company.
7. **Miscellaneous**. Any transaction that does not neatly fit into one of the above six categories, falls into this default bucket. These may be personal transactions between individuals – such as a client with his attorney or accountant, a social gathering of people with common interests, etc.

Given that our life's transactions neatly fit into one of these seven buckets, an identity infrastructure can be optimized along these seven “indu stries”, by issuing humans between two (2) and seven (7) cryptographic tokens with a distinct digital certificate on each. The two minimum credentials would serve the healthcare and government transaction needs – something that every person must deal with in industrialized nations even if they choose to forgo transacting with any other industry. Up to a maximum of seven (7) credentials may be issued to the individual to address all authentication needs of that user within his/her lifetime. This is rationalized in this paper.

Three items must be clarified, at the outset.

Firstly, these authentication credentials – the digital certificates on the cryptographic tokens – must not be confused with authorization to execute a given transaction. For example, as Arshad Noor, I will always remain Arshad Noor to any bank, brokerage or insurance company in the financial services industry. However, whether I am authorized to execute an options trade with my brokerage is a completely distinct issue that must be addressed by business rules within their applications and must not be encoded into my authentication credential. Similarly, just because I presented a valid credential to the company network, the authorization to use a specific color printer within a department should not be automatically assumed. Software controlling the submission of print jobs, which, while depending on my identity, must determine my authorization to submit jobs to that printer through some other mechanism – perhaps a group membership in a company directory. These credentials establish only identity, and relying parties may only depend on that upon a successful authentication.

Secondly, the concept primarily serves Business-to-Consumer or Government-to-Consumer transactions. Business-to-Business or Government-to-Business and Government-to-Government needs are not addressed here, although there is no reason why such a concept cannot be adapted to accommodate those special needs.

Finally, since this author lives in the US, some of the terms and concepts have been designed with the US system in mind. However, these are adaptable to any country that might choose to do so for their purposes.

IV. Mechanics

Non-profit organizations will be established to govern the business rules for identification and credential issuance within six of the above “industries” - private companies will determine their business rules for issuing credentials to their employees. We'll name the non-profit organizations “credentialing organizations” for want of a name. Governments will probably establish this through standards organizations representing the government - such as the National Institute of Standards and Technology (NIST) in the US.

Associations representing industries may assume the responsibility for that industry, or a working group may be created to address the needs of sub-industries within an industry. For example, there may be associations of banks that are distinct from associations serving credit unions or brokerages. Since no one association speaks for the entire financial industry, a working group within the financial sector may be created by representatives of each of these associations. The representatives will speak for their associations and will abide by the final rules established by the working group to serve their entire industry. Companies and sub-industries may choose to not participate in the effort, but will surely incur economic penalties, as described later in the section titled Economics.

These non-profit credentialing organizations will create the detailed business processes that establish the identity of customers within that industry, using guidelines that serves the entire sector and which conform to rules established by regulatory bodies for that industry. Where common rules cannot be distilled to serve the entire sector's needs, this will become an opportunity for streamlining those processes to establish the common rules. If conflicting regulations are the cause, it will present an opportunity to have the industry work with the regulatory bodies to streamline regulations to distill common rules that serve the entire sector. Businesses, government and consumers all benefit from the resulting efficiency due to the streamlining effort.

The rules for establishing identity and issuing credentials within a given industry, will be independent of rules established by any other industry. There will be no dependencies between industries for establishing identity, save for corroboration of specific facts. For example, today, most banks assume identity is firmly established when they see a government-issued credential – such as a Drivers License or Passport. However, it may well be that the credential presented by the individual is falsified. Rather than assume that another agency or industry has done its due diligence, each industry must strive to create its own strict rules for establishing identity before issuing credentials to the user.

The few facts that must be corroborated by other industries are:

- Date of Birth
- Educational Qualification
- Nationality (or Resident Status)
- Tax Identification Number

These facts must, by definition, be corroborated by other authoritative bodies. This can be accomplished by using digitally signed documents that are built into the identification & credential issuance process. None of these facts need be present in the digital certificate itself. These will be stored, encrypted, within the repositories of the credentialing organizations that perform the identification & credential issuance process. Should any company within an industry need this information directly for its business purpose, it must be requested by that company of the credentialing organization serving their industry. Protocols for the corroboration of the above facts, as well as the request-response of information between companies and the credentialing organizations serving their industry, will be defined by the working group representing the industry.

Upon concluding the identification process, the credentialing organization (or its agents) will issue the individual a 2-factor cryptographic token, generate a key-pair in the presence of the agent, and be issued a digital certificate for that specific industry. The certificate is published into an industry-specific repository that restricts access only to authenticated members of the industry. All companies that have chosen to participate in this effort within that industry will now honor that credential for authenticating that individual. Each company, must then use its own business rules to determine what transactions may be executed with that individual, independently.

As an example, if I were to approach a bank for the first time for a credential, an agent of the financial services industry's credentialing organization – potentially sitting at the bank - would verify my identity using guidelines established by the industry's credentialing organization, and issue me a cryptographic token with my financial services digital certificate.

Armed with this credential, I may now purchase banking services from that bank. However, using the same credential, I may enter into an agreement with a brokerage down the street to buy and sell equities through them, without having to undergo the identity verification process all over again. The brokerage would get all required information from the credentialing organization serving the financial services industry. Similarly, I may purchase a life insurance policy from an underwriter over the Internet, by entering into a business transaction with them, without undergoing the identity verification process again.

In this manner, an established credential may be re-used repeatedly within that industry, without the expense of executing the identity verification process again. One cryptographic token and digital certificate serves the needs of the consumer across the entire sector.

If companies chose to issue a secondary credential to a customer – for whatever business reason – they may do so. However, if the credentialing organizations' policies and practices are sound, there is little incentive for them to duplicate such infrastructure.

V. Economics

There are tremendous advantages to using a shared credentialing organization for industries. Currently, every company within an industry that deals with a customer, must independently identify the customer and issue them credentials for dealing with that specific organization. Considering that the identity of a customer rarely changes, the entire industry wastes a tremendous amount of money duplicating this process and infrastructure within each company in the industry. Ultimately, the consumer bears the cost of this inefficiency.

Secondly, this very same reason has prevented businesses from deploying 2-factor cryptographic tokens, or digital certificates across its customer base – the cost that must be borne by each company for the token, the digital certificate and the support infrastructure, can rarely be justified by individual companies.

By going to a consolidated credentialing organization that uses a shared process and a shared credential within the industry, companies, and thus consumers, save a huge amount of money through elimination of redundant processes & infrastructure. Where a 2-factor token and a digital certificate may have been too expensive for a single company for its million customers, the very same technology – issued and managed through a single credentialing organization for the sector – is more than justified for a thousand companies serving 200 million customers.

Applications and IT infrastructures built by companies to transact with their customers, will never have to execute the customer identification business process anymore; they never have to issue credentials anymore; they never have to secure and maintain authentication databases anymore. All they have to do is, validate the industry credential and determine the authorizations to transact with a customer. The savings over the long term would far exceed any initial cost that each company would have to pay to be part of that infrastructure.

While it will be pointed out that consolidating credential information with six credentialing organizations serving six industries, places too much risk in one place, it can also be conversely argued, that by consolidation, one can more efficiently protect & monitor the infrastructure than a thousand companies within an industry, can. The scale of economy afforded by consolidation will permit even the most onerous security process to become cost-effective.

Businesses will also see some tangential benefits. Firstly, with a customer base that has digital certificates, it will become easier to wipe out “phishing” and its associated losses. Businesses will start using certificate-based authentication on their websites, and digitally signed and encrypted e-mail when communicating with their customers. Businesses and customers will ignore unsigned, unencrypted e-mails, and there will be no User ID and Password to use at the website anymore. Even if customers were still duped into going to a “phishers” web-site instead of a legitimate business', the fact that the “phisher” does not have the 2-factor cryptographic token in their possession will eliminate the risk of stealing the legitimate customer's identity.

Consumers benefit significantly too. Even though they will wind up bearing the cost of the infrastructure, they will benefit from the reduced expenses at the companies they deal with (companies will be forced to pass on the savings to consumers, since it will become painless for consumers to switch service providers if they so desire); they will see improved security in the infrastructure as it moves towards asymmetric-key based authentication and communications; they will see improved productivity because they will never have to remember User ID's and Passwords to dozens of accounts; they will see small companies offer innovative services without sacrificing security; they may even be able to block spam by blocking all unsigned e-mails (while spammers can technically send digitally signed e-mails, this is a far more expensive operation considering the volumes of e-mails that spammers must send out).

Companies that choose not to participate within their industry's credentialing organization, will pay an economic penalty in increased costs for their "priva te" identity management process and infrastructure. While some organizations with very large customer bases could potentially find some economies of scale, it can never match the scale of economy of their entire industry.

VI. Privacy

Any infrastructure attempting the consolidation of identities at this scale is certain to raise concerns about how individuals can be protected from abuse. With tens of millions of identities being managed by each of the six credentialing organizations, the risk is significant. This author believes that the most effective way to solve this problem is through a combination of technology and law.

At the very outset, a federal law must be passed (for the US) with four primary goals:

1. It must mandate extremely harsh punitive measures for abuse by insiders, or theft of identity information by anyone. Employees of the credentialing organizations must recognize that carelessness or abuse of their responsibility will result in severe penalties to them. Law enforcement agencies may be provided access to this information upon the production of judicial orders.
2. It must prohibit the sharing of information between industries. Information may be shared by companies within an industry, if permitted by the consumer, but never across industries. This ensures that companies who are regulated by agencies within a specific industry, such as finance, do not have to concern themselves with regulations affecting other industries, such as healthcare. This element of the law establishes the "firewal l" between identities.
3. It must permit a credentialing organization that serves an industry to contract the operations to a service provider, if desired. However the service provider must not allow any of the information to leave the borders of the country. In addition, all personnel of the credentialing organization or its service providers, who have access to identity information, must reside within the borders of the country in which the information resides so they may be subject to this law. If a credentialing organization chooses to contract the service to a service provider, that service provider may not contract with any of the other credentialing organizations – in essence, a service provider must never operate the infrastructure for more than one credentialing organization.
4. Finally, it must establish regulatory oversight over the six credentialing organizations, and delegate it to the Consumer Division of the Federal Trade Commission (for the US). This agency must have the authority to ensure that credentialing organizations serve the privacy interests of consumers above the economic interests of the industries they serve. The agency must be allowed to establish guidelines for technology and operations, and to suspend a credentialing organization's operations if necessary. Funding for this oversight responsibility, must come from graduated fees levied on credentialing organizations. This has the advantage that if a credentialing organization takes the initiative to operate under more diligent conditions, and runs a secure infrastructure, the agency will only need to oversee that organization minimally, thereby lowering its oversight fee.

With a stringent law, and mandated security practices such as encrypting all customer information (at rest, or in transit) the risk of abuse can be minimized. It is almost certain that the credentialing organizations and their infrastructures will be subject to significant levels of technical attacks. However, as stated earlier, given the economies of scale, the credentialing organization can take extraordinary measures to protect its infrastructure, and yet be deemed cost-effective. The goal is to raise the bar for a successful attack so high, and the consequences of capture significantly painful, that they serve as strong deterrents to potential attackers.

VII. Seeding

One of the most challenging aspects of an effort of such scope is the first step. This author's contention is that the first step must come in the healthcare industry. When a new baby is born at a hospital, the baby should be issued its first digital certificate to serve its authentication needs in the healthcare industry.

The certificate will be unusual in that it will be the only one of the seven credentials that will have an otherName value in the SubjectAltName extension to store a one-way hash of the digital representation of the newborn child's DNA. (The digital representation of their DNA itself would never be available online to anyone outside the hospital; only the one-way hash would be hand-carried to the computer producing the baby's credential over an “air gap”).

The hash of the DNA is needed in case it becomes necessary to establish a person's identity with certainty, somewhere else. For example, if an individual ever lost all their digital credentials and needed to re-establish them, they would walk into any hospital that subscribed to this concept and provide some material from their body for a DNA analysis. Once analyzed, the hash of the digital representation of the DNA could be compared against the stored value in the extension of the originally issued digital certificate to that individual. Upon a successful match, the person will have established their identity with sufficient proof to the hospital, to authorize the creation of new credentials. The original hospital of birth need never be involved in the process.

The certificate and its keys will be issued in the name of the baby, to the mother (or legal guardian) on a cryptographic token. (If the token is a smartcard, the hospital may provide a reader too, in appreciation of having used their facilities). The guardian of the baby will be given provisional authority to use that credential on behalf of the child, until the child is a legal adult. The credential may be used for dozens of business applications - making appointments with the pediatrician; requesting that digitally signed “birth certificates” from the hospital be e-mailed to specific recipients; receiving digitally signed and encrypted lab results or prescriptions; securely accessing their medical history at a “medical warehouse” - the possibilities are endless.

When a child goes to enroll at a preschool or kindergarten, proof of residency and the date of birth can be provided to the school by having the hospital of birth e-mail a digitally signed birth certificate to the school admissions office (the guardian will actually request it through an application on the hospital's site, after authenticating him/herself with their own healthcare credential, or their child's credential). Schools may access the digital certificates of hospitals from well-known repositories, and use them to validate the digitally signed birth certificate. Once verified, the school would then issue the child's education credential (once again with provisional authority to use the credential on the child's behalf until the child entered high school, or became an adult).

Over a period of time, a new generation of credentials will become prevalent that will provide strong evidence of the possessor's identity. As these increase over time, applications and services over the Internet will become far more secure as they move away from single-factor, secret-key based authentication, heralding a new era of applications.

Registrars of births, or similar organizations, will also be a repository for the digital certificates issued in the healthcare industry, in case a hospital goes out of business.

VIII. Grandfathering

Given that business have already established millions of identities using processes that do not conform to the above recommendations, these identities must be “grandfathered” through a special one-time process.   It is necessary to grandfather them because, in the absence of a DNA record at the time of birth, it will be impossible to verify a person's identity with certainty, save for the sworn testimony of parents and witnesses.

As such, the one-time grandfathering process will consist of individuals providing sworn testimonies, attesting to their identity, and establishing a digital DNA hash at an approved healthcare institution to receive their healthcare industry digital credential. This credential in turn, will drive the remaining industry credentials, as necessary.

Where a person is not born in the country where the credential is being issued, sworn testimony of the individual, countersigned by their birth country's Embassy, as well as the establishment of the DNA hash, can initiate the process for issuing the healthcare credential.

IX. Conclusion

Public-key cryptography has been around for more than two decades. While most security practitioners recognize the value of PKI, they've been loath to forward it as a foundation solution, because of its complexity and economics.

It is this author's contention, that while PKI are complex, they can be managed through education and diligent operations. At one time, it was inconceivable to bankers that customers would use an Automated Teller Machine

(ATM) and the two-factor based bank cards to transact with the ATMs. Today, most of the industrialized world cannot function without ATMs.

Digital certificate credentials using cryptographic tokens, can follow in the successful footsteps of the ATM card. As long as the policy guiding the infrastructure, and the deployment & operations of the infrastructure is sound, users will rise up to meet the challenge and deal with it. As a result, we can expect a technological environment that will be based on a far more secure foundation than what exists today.

X. Bibliography

1. US Postal Service website on Identity Theft: http://www.usps.com/postalinspectors/idthft_ncpw.htm and a GAO Report on Identity Theft: http://www.consumer.gov/idtheft/reports/gao-d02363.pdf).