This Issue: Security and Resiliency in Banking

Volume 2, Issue 1

In This Issue:

Dan Schutzer,
Executive Director and Editor

Adam Gluckman,
Electronic Publishing

Welcome

Welcome to the second all-electronic issue of FSTC Innovator.

2007 has been a great and busy year for FSTC. FSTC has again demonstrated how it is effectively harnessing technology to solve problems and issues in the financial services industry. Addressing issues of security and trust have represented some of our major efforts.

In 2008 we will continue to address, among other things, some of the challenges in the

security and resiliency area, including:

- Fighting fraud
- Improving authentication and identity management
- Addressing the needs for credentialing
- Preventing data leaks; improving business processes to be more efficient, secure and resilient
- Addressing the challenges of data retention
- Addressing the insider threat
- Improving the security of mobile banking and payments
- Improving the resiliency of the financial services industry
- In this issue, we will cover the following topics:
- Barry Horowitz and Johnathan Crawford of the University of Virginia wrestle with the complex issue of how one justifies investments in cybersecurity and trades of investments in security with other investments.
- Joe Gersch of Secure64 Software Corp. describes DNSSEC as a

means of preventing pharming, and discusses the barriers towards its adoption.
- Ziv Barzilay of Cell Max systems discusses the advances in voice biometrics and predicts a future where voice biometrics will be an integral part of many authentication solutions.
- Russ Ryan of the National Biometric Security Project provides a review of best practices in implementing a biometric system and discusses some of the newer emerging biometrics
- Joel Weise of Sun discusses the importance and use of trust models in security design and identity management.

Dan Schutzer, FSTC, introduces the concept of safe web browsing, and its recommended changes to the web browser that helps the user be sure that the website they access is actually their bank's website and is not a spoofed site.

- Robert Brandewie of ActivIdentity discusses the FRAC card and presents a business case for its use in the enterprise.
- GRBDe Digital Home Study Group reports on progress in the emergence of the Digital Home

After perusing the articles found within this second edition of FSTC Innovator, I'd like to hear your opinion. What did you think of this issue? How would you improve it? What kind of articles would you like to see in the future?

If you would like to become involved in FSTC's initiatives, and join the on-going conversation, Contact Dan Schutzer, dan.schutzer@fstc.org; or John Fricke, john.fricke@fstc.org.

Application of Collaborative Risk Analysis to Cyber Security Investment Decisions

**Barry M. Horowitz and Jonathan Crawford
University of Virginia**

1. Introduction

Many CISOs are taking a growing interest in the potential applications of risk analysis methods to decision-making related to cyber security investments. This interest was made obvious at a recent October, 2007 workshop attended by one of the authors. The workshop was organized by the Tuck School of Business at Dartmouth and was sponsored by the Institute for Infrastructure Information Protection (I3P). The purpose was to provide a forum for CISOs (about 25 participated representing a variety of business sectors) to discuss the state of application of risk analysis. The application of risk analysis to cyber security is far from being a straight-forward matter. What was being said at the workshop is that CISOs are being successful at identifying low-cost, high-leverage cyber security opportunities for IT project leaders, and at apprising project leaders of legal compliance issues, but are not nearly as effective in adjusting expenditures in cases that were not clearly supported by evidence. The reason for this resides in the basic requirements for a risk analysis. The premise of a risk analysis is that risk is measured by answering three questions:

1) What can go wrong?
2) What is the likelihood?
3) What are the consequences?

And, of course, for cyber security, knowing the likelihoods of possible attacks is elusive. Furthermore, the likelihoods are constantly changing due to ongoing adaptations between attackers and defenders. In addition, the relationship between likelihoods of attack and increased cyber security are not known, and this relationship changes over time as well. Based on the authors' experiences, and reinforced by the discussions at the workshop, the uncertainties surrounding likelihoods serve to dissuade the application of risk analysis, and seriously weaken the basis for gaining agreement on the appropriate level for investments in greater protection.

2. Collaborative Risk Analysis

Over the past two years, in an effort to develop new and viable risk analysis methods related to cyber secu-rity, the University of Virginia (UVa) has been engaged in developing collaborative computing tools for application to risk analysis for guiding cyber security investments. The factors that shape this research effort include:

- Rationale for decision making about investment levels in cyber security currently tends to be ad hoc because of the inability to validate critical risk assumptions, as described above. Correspondingly, corporations do not document the risk basis for their decisions, resulting in both the inability to reconcile previous decision logic with events that occur later in time and the inability to improve decision rationale over time.

- Cyber security risk analysis must include considerations of risk along with other opportunities for use of capital. Consequently, a broad set of corporate managers would necessarily be required to participate in a well-thought-out cyber investment analysis, including representatives of the departments competing for the same dollars that the cyber security advocates might like to see devoted to computer security. These non-cyber security focused parties would naturally include marketing and sales, R&D, legal, and finance. For example, the corporate legal organization would make a valuable contribution in considerations of privacy liabilities related to reducing insider threats, and how they compare to the liabilities posed by the insider threat. They would also be involved in assessments of regulatory risks that could become prominent if security is not treated sufficiently. Similarly, marketing, sales, and R&D would be advocating the return on investment that they could provide with the funding of their efforts, as opposed to cyber security.

- To be considered rational, risk-based decision-making by a group of corporate managers should include the following three steps:

1) **A delineation of the assumptions that surround the cyber security investment decisions.** Logically, based on the discussion above, the assumptions to be accounted for must be determined by a group of managers

representing the knowledge of their part of the overall corporation. Assumptions would include such factors as the consequences of an attack that could be protected against, the likelihoods of the attack with and without the cyber protection under consideration, the expected return on R&D investment using the same dollars that might otherwise go into cyber security investment, etc. They could also include considerations about time sensitivity; i.e., the criticality of a particular decision being made now versus at a later point in time. Note that establishing the set of assumptions that need to be considered is viewed as a separate step from actually setting assumption values, which is accomplished in step two.

2) **A group determination of the values for the assumptions and the uncertainties surrounding these values.** Clearly, no single person in a corporation is sufficiently expert in all of the topics surrounding a rationale business decision on investments in cyber security. A group determination allows the broader expertise to be accounted for and, quite importantly, also allows a transfer of knowledge about decision factors to take place among the group members involved in the decision process. This knowledge transfer is especially critical because of the time sensitivity of assumptions, and the corresponding need to have a decision-making group that is continuously learning and adjusting its outlook about the balancing of future corporate risks and opportunities.

3) **A group determination of decision-making qualities within the variation boundaries for assumptions.** This step involves the development of distinct assumption scenarios that lie within the boundaries of the assumptions established in step 2. The selection of scenarios must be accomplished in a manner that would "logically" lead to different, assumption-specific, solutions. This permits, through the use of a decision-making exercise, an assessment of the readiness of the organization's management team to adjust decisions as a function of varying assumptions. Clearly an organization that is "stuck in the mud" is not acting rationally;

alternatively, there is some unstated assumption concerning risk orientation that is critical to actual decisions and, as a result of the group decision-making effort, can be discovered and recognized. The result of a decision-making exercise is the documented understanding of how the company converts its assumptions into decisions.

3. Models and Initial Results

The UVa research effort has been integrating, from openly available software packages, collaborative computing tools that can permit groups of managers to work together in a time asynchronous manner to carry out the above three steps required for rational business decision-making. . The use of collaborative computing seems to be a necessity when considering the number of company meetings that would otherwise be required to carry out the three steps described above. In order to apply collaborative computing technology, a variety of models have been developed that support the desired collaborations for both assumption gathering and decision making. For assumption gathering, a method called Hierarchical Holographic Modeling (HHM) has been adopted (Reference 1). The HHM methodology is designed to recognize that: 1) complex decisions usually involve the need to address a multitude of conflicting objectives (the holographic aspect of HHM), and 2) that potential risks reside at various levels in a large system's hierarchical structure (the hierarchical part of HHM). Accordingly, HHM provides a structured method for eliciting risk-related information from an organized group of participants whose integrated knowledge spans the full range of system hierarchies and decision objectives. The result of an HHM exercise is a diagrammatic representation of the relationships between risks, opportunities, possible solutions, their predicted costs and benefits and the uncertainties surrounding the various estimates that participants offer. Based on experiences to date, the results of the HHM assumption activity generates too many assumption variables to practically deal with in decision-making. As a result, the HHM collaborators need to complete their effort by selecting what they collectively believe to be the most important factors to consider for decision-making. The selected higher-priority assumptions can then be organized into value combinations, or clusters, that range from being more to less favorably oriented to increasing investments in cyber

security. A collaborative decision exercise can then be constructed based on the assumption clusters, utilizing a set of distinct decision-making scenarios that permit an evaluation of the sensitivity of investment decision choices made by participants to the particular scenario parameters. The result of an exercise is a post-mortem analysis of how the collaborators adjust their views as scenarios and assumptions vary. This result serves to identify for the group those assumptions that are truly critical to their thinking and, in turn, creates the opportunity for further dialogue and analysis regarding the most influential assumptions prior to finalizing judgements on an actual decision. An important aspect of the decision exercise process that we have used is, for each scenario of assumptions, to include multiple years of decision-making, supported by simulations that, on an annual basis, provide input to the collaborators about cyber attacks on the company. For example, if in a five year exercise, the initial year's decision is to invest less in cyber security, the simulation generates a successful attack and its consequences (parameters determined through the assumption generation activity) with greater likelihood than if the decision had been made to invest more in cyber security. Since successful attack likelihoods are low, a multiple-year exercise creates a window of time that increases the likelihood for attacks, and increases the sensitivity of collaborators to the long term consequences of their decisions.

Three different industry workshops have been organized to get feedback on both the potential value of the decision support concepts described above, and on tool design details. The workshops were used to explore: 1) the influence of opportunity costs on decision-making (two cases were looked at - oil and gas distribution industry and manufacturing industry), and 2) the influence of potential government regulation on decision-making. The following paragraph describes one of the decision experiments that was conducted. This early experiment was not focused on supporting a corporate team making decisions, but instead was focused on a set of different companies, each making its own decisions about investment. Using the results of all three workshops, we expect to field a prototype system that allows us to evaluate the overall decision support concept described in this paper within a variety of corporations' operating frameworks.

3.1 More Cyber Security or More R&D

A group of 23 cyber security managers participated in a collaborative computing supported decision-making exercise where they each represented a different company, and independently made decisions about cyber security investments. The investment scenario was whether to invest in further protecting intellectual property (IP) information, or whether to increase the size of the corporate sales force. Three assumption scenarios were developed, each covering a five year sequence of annual decision-making. Using expected outcome analysis, the scenarios were organized so that in one case the expected outcomes were the same, in another case the sales force decision had a superior expected investment result, and in the third case the cyber investment led to a superior expected investment result. The five year decision sequence included an annual report to the participants on whether their company suffered an attack, as well as the overall number of successful IP attacks that the entire set of companies had experienced. The attack results were determined through a simulation that accounted for each participant's investment decisions. The results showed that:

1) Participants had a strong pre-disposition to investing in the sales force opportunity; i.e., in the case where expected cyber risk and expected sales opportunity outcomes were the same, about 80% of the participants elected to invest in the increased sales force option. However, as time went on and simulated cyber attacks were accumulating, this ratio reduced to about 60%.

2) When the scenario for decision-making shifted to clearly favoring cyber security investment, the decision-makers did indeed shift accordingly. In fact, about 25% of the decision-makers that had favored sales force growth in the equal risk/opportunity scenario shifted their investment choice from sales growth to cyber security.

3) When the scenario shifted to clearly favoring sales force expansion, the decision-makers did not shift their decisions; i.e., those that had supported cyber security

investments in the equal risk/opportunity scenario were not persuaded to shift their investments in spite of the more favorable assumption parameters.

Independent of actual decisions, the participants learned about their implied views concerning cyber investments, providing an opportunity to adjust their decision-making. Furthermore, results documented the factors that went into the decision that could be used for future improvements in how decisions are made.

3.2 Continuing Efforts

The results to date have resulted in significant interest from companies. However, more work is needed on developing tools that will permit companies to set up their own processes, customized to operate in their own working environment. In order to accomplish this objective, our plan over the next year is to work with a few companies to further develop the decision support concepts described in this paper. Upon completing this work, we intend to provide the resulting collaborative computing tool as an open source package, available to any company that can potentially gain value from its use. We will also continue to document the results from our continuing experimental efforts. Hopefully this will provide sufficient encouragement to companies to explore the concept of carrying out collaborative risk analyses regarding their investments in cyber security.

References

Y.Y. Haimes and B.M. Horowitz, "Modeling Adaptive Two-Player Hierarchical Holographic Modeling Game for Counterterrorism Intelligence Analysis" *Journal of Homeland Security and Emergency Management,* Volume 1, No.3, pp. 1-21 (2004).

Protecting the DNS with DNSSEC

Joe Gersch
Secure64 Software Corp

DNS (Domain Name System) is a core component of the Internet and TCP/IP network infrastructure. When customers visit your financial institution's web site,

DNS works in the background to translate the site's domain name into the correct IP address. It also helps to direct traffic to the correct email servers. Essentially, DNS acts as the address book for the Internet, getting people and information where they need to go.

But what happens if an attacker is able to change an address in the DNS? This is known as pharming. With pharming, an attacker alters the DNS entry for your web site (say 192.168.0.1) to point to the IP address of a web server under the attacker's control (say 10.45.12.32) in order to direct customers to a fake web site. Unsuspecting customers can enter private information such as usernames, passwords, and account numbers, or the fake site can cause worms and Trojans to populate customers' computers.

Unlike phishing, where the URL of the web site is changed, it is nearly impossible for a customer to detect that the underlying IP address has been hijacked by an attacker. And attackers can use this technique because today's DNS infrastructure has not adopted the means to authenticate the answers the DNS system provides.

Authenticating DNS

How can consumers be assured that the DNS is directing them to their financial institution's legitimate web site and not a false site set up by an attacker? Authentication of the DNS using DNSSEC (DNS Security Extensions) is a solution that has been discussed for many years. DNSSEC protects customers from pharming by validating the source of the answers provided by the DNS.

DNSSEC is a set of IETF (Internet Engineering Task Force) standards outlined in RFCs 4033, 4034, and 4035. Its purpose is to authenticate the response to a DNS query through the use of a trusted chain of name servers. It does this in part by utilizing public-key cryptography to digitally sign DNS data.

Securing the DNS Query/Response Transaction

When an Internet user enters a domain name, such as www.example.com, in a web browser, the DNS system finds the corresponding IP address as follows:

- User enters www.example.com in a web browser, which queries a DNS resolver for the IP address of www.example.com
- DNS resolver contacts a DNS caching server to determine whether it knows the location (IP

address) of www.example.com
- If the DNS caching server does not have information about www.example.com, it contacts a root-level server
- The root-level server does not know the answer, but refers a list of gTLD (generic top level domain) servers for the .com domain
- The .com gTLD server does not know the answer, but refers the authoritative DNS server for the example.com domain
- The example.com domain provides the authoritative answer for the IP address of www.example.com

In this DNS query-response process, the user has no assurance that the response came from the DNS server authorized to provide answers for the requested domain. In addition, the user has no assurance that the IP address received has not been altered in transit. DNSSEC is a solution to these problems because it provides:

- Authentication of the source of the response to a DNS query
- Verification of the DNS data integrity

Source Authentication
DNSSEC utilizes public-key cryptography and digital signatures to validate the authenticity of a query response. Starting with a trusted DNS server, DNSSEC-enabled DNS servers verify the digital signature of the pubic key of a child by its parent to establish an unbroken chain of trust down to the source of the query response. This chain of trust allows the recipient to know for sure that the response came from an authorized DNS server, and not from an attacker.

DNS Data Integrity
Digitally signing DNS data also provides proof that the data has not been altered or tampered with. It confirms that the data sent by the queried DNS server is the same data received by the server that receives the response.

In addition to validating DNS data in a response, DNSSEC provides a mechanism for validating non-existing DNS data. A special response is returned to authenticate that the requested data does not exist. This proof of non-existence can prevent additional types of DNS attacks.

DNSSEC Example
In order to implement DNSSEC, the authoritative DNS server for the requested zone, the DNS caching

server, and all parent servers must be configured to be security aware. In addition:

- The authoritative name server administrator must digitally sign its zones with its private key.
- The parent of the authoritative name server must contain the public key of the child, and it must be signed with the parent's private key.
- The caching server must obtain the public key of DNS server that is the source of the chain of trust (known as the trust anchor).
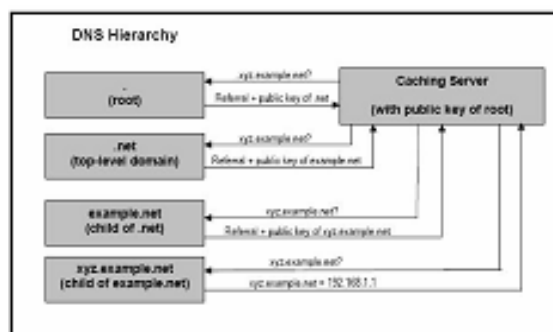

Figure 1 *Chain of trust starting at the DNS root*

The example above illustrates the following:

- The root (.) DNS server is the source of the chain of trust (trust anchor).
- As the trust anchor, the root (.) DNS server contains the public key of the *.net* top-level domain.
- The root (.) DNS server vouches for *.net* by signing it with the root (.) DNS server private key.
- Each successive parent domain signs its child domain with the respective parent private key.
- The caching server contains the public key for the root (.) DNS server so that it can follow the chain of trust.

In the example, the chain of trust is established at the top of the DNS hierarchy at the root (.) level. The caching server needs only the public key of the (.) root DNS server to follow the chain of trust when it receives a query for *xyz.example.net*:

- When the caching server queries root (.) for *xyz.example.net*, root responds with a signed referral to *.net* along with the *.net* public key. The caching server can read the response

using the root (.) public key.

- The response from *.net* is a signed referral to *example.net* along with the *example.net* public key. The caching server can read the response using the *.net* public key provided previously by the parent root (.). The response from *example.net* is a signed referral to *xyz.example.net* along with the *xyz.example.net* public key. The caching server can read the response using the *example.net* public key provided previously by the parent *.net*.

- The authoritative name server *xyz.example.net* provides the signed response with the IP address for *xyz.example.net.* The caching server can read the response using the *xyz.example.net* public key provided previously by the parent *example.net.*

With the root (.) DNS server as the trust anchor, all domains below the (.) root would be securable through DNSSEC and a single (.) public key published on the caching server. This is the ideal scenario for DNSSEC deployment; however, the root and most top-level domain DNS servers have yet to implement DNSSEC signing services in practice.

Challenges for DNSSEC Implementation
If DNSSEC provides such important benefits, why hasn't it been adopted on DNS servers everywhere? Although the technology itself is capable, implementation has been slow due to several challenges.

No Chain of Trust
One of the challenges to widespread use of DNSSEC is establishing the chain of trust. The DNS namespace is extensive, and it does not contain unbroken hierarchical sequences of DNSSEC-signed zones. Instead, there are "islands" of signed zones; the parents of signed child zones are not necessarily signed themselves. And the root and more than 250 top-level domains, with the exception of the Swedish *.se* ccTLD and a few others, have not yet signed their zones. For these reasons, a true chain of trust does not exist.

The figure below illustrates the concept of islands of trust, which results from trust anchors located at various points within the DNS hierarchy. The trust anchors in this example are *example.net*, *abc.example.com*,

and the *.se* top-level domain. Only the signed child zones within the hierarchy of each of these chains of trust can deploy DNSSEC.
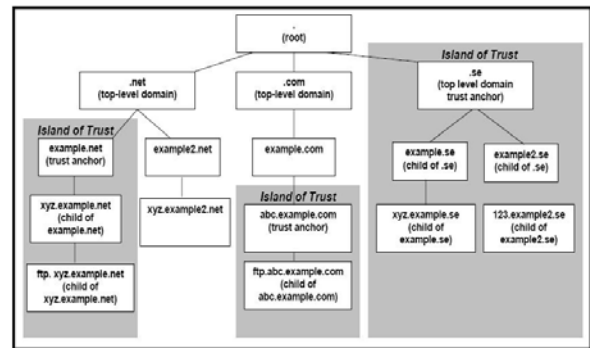

Figure 2 *Islands of trust*

In order to validate each of these islands of trust, caching DNS servers must be supplied with the public key of each of the trust anchors. Combining this with the periodic need to roll over or change keys for security makes the maintenance of DNSSEC-aware caching servers a complex process.

Mostly Manual Processes
Key generation, zone signing, key distribution, and key management are manual processes, for the most part. For example, public keys must currently be distributed through an out-of-band method such as web sites or emails. Keys should be rolled over on a regular basis to prevent compromise, and the key generation process is generally handled by manually invoked utilities.

Some automated scripts have been developed for tasks such as key management and zone signing (see www.dnssec-tools.org and www.verisignlabs.com/dnssec-tools/). However, until DNSSEC is a fully automated process, it remains complex to implement, and current methods are prone to errors.

Secure Storage of Private Keys
Another challenge to DNSSEC implementation is secure storage of the private key in the public-private key pair. The private key must remain secret, or the security of the DNS response is compromised. Currently, best practices recommend offline storage of the private key so that it cannot be obtained or tampered with. The problem again is one of automation. Storing the private key offline requires some form of manual intervention or process to manage the keys. This problem also affects dynamically updated DNS zones, which require automated signing of new DNS records.

What's Needed Now

In order for DNSSEC to become a reality, the Internet community, DNS administrators, companies with a Web presence, and even the federal government must work together to create an environment and the demand for workable solutions.

Demand Infrastructure Solutions

Russ Housley, chair of the IETF (Internet Engineering Task Force) has stated that DNS security is one of his top priorities. The Internet community has worked for more than ten years on DNSSEC, and it will need to continue to coordinate efforts to implement a solution that the Internet infrastructure can feasibly implement. Some top-level domain operators have committed to providing DNSSEC signing services. Implementing these services would facilitate establishment of the chain of trust and decrease the number of keys needed for trust anchors.

Demand and support for DNSSEC from companies with a large online presence, Internet providers, and the government can only help to back these efforts. Most of our nation's critical computing infrastructure is vulnerable—not just financial institutions. Imagine if attackers hijacked online news and federal government web sites to publish stories about phony terror attacks.

Easy DNSSEC

In addition to making the DNS infrastructure work with DNSSEC, it must be easy for DNS administrators to use. Today's jumble of scripts, manual methods, and disconnected utilities make DNSSEC complex to implement and manage. Commercial implementations of DNSSEC should provide automation, security, ease-of-use, and ongoing manageability.

Companies such as Secure64 Software Corp. (www.secure64.com) are endeavoring to develop secure DNS servers that facilitate DNSSEC and other DNS security standards. By developing a TCP (trusted computing platform) with a secure operating system, Secure64 is working towards an easy DNSSEC solution that provides:

- Automation of DNSSEC signing operations
- Automation among networked DNS servers to manage parent-child delegation points (the chain of trust)
- Secure online storage of private keys

- Secure interoperability with other DNS server platforms
- Encryption and authentication of information on disk
- Self-protecting network stack to prevent denial-of-service and packet-flooding attacks
- Protected memory compartments to store signing keys safely online
- Granular authorization categories to limit access to software services
- SNMP alerts for administrator notification and alerts of attack events
- BGP capability to promote anycast deployments

Secure64's current DNS server solution already provides many of these features. Continuing development is underway for DNSSEC automation and ease of use.

Making DNSSEC a Reality

DNS is behind the billions of requests made on the Internet every day. But today's DNS infrastructure cannot authenticate the answers the DNS system provides, leaving users vulnerable to a wide variety of fraudulent activities. Only through the concerted efforts of the Internet community, the demands of businesses and the government, and the solutions developed by commercial providers can the protections of DNSSEC be truly realized.

About The Author

Joe Gersch
VP of Engineering
Secure64 Software Corp.

Mr. Gersch is responsible for software development for Secure64. He led the development of a genuinely secure operating system, SourceT, which is immune to rootkits and malware and resistant to network attacks. He also led the development of the Secure64 DNS server, which is built on SourceT and represents a significant advance in DNS security and performance. Previously, Joe was at Hewlett-Packard where he led product development for smart cards, cryptography, network security as well as OpenView R&D.   Joe earned a B.S. in Computer Science at the University of Michigan and an M.S. in Computer Science from Colorado State University. He is also a board member of the Vivit (formerly OpenView Forum International) and is an advisory board member of Voyence, Inc.

Additional Resources

- NIST Secure Domain Name System (DNS) Deployment Guide - csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf
- DNSSEC Web Portal—www.dnssec.net DNSSEC Deployment Initiative—www.dnssec-deployment.org/
- DNSSEC How To Tutorial -www.nlnetlabs.nl/dnssec_howto/
- DNSSEC Tools & Scripts—www.ripe.net/disi/dnssec_maint_tool, www.dnssec-tools.org, www.verisignlabs.com/dnssec-tools/
- DNS Cache Poisoning-The Next Generation—www.secureworks.com/research/articles/dns-cache-poisoning/

References

Pro DNS and BIND
Ron Aitchison
Apress; 1st edition (August 8, 2005)

DNS and BIND
Cricket Liu and Paul Albitz
O'Reilly Media, Inc.; 5th edition (May 1, 2006)

NIST Secure Domain Name System (DNS) Deployment Guide, csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

Banking On Voice Biometrics

Ziv Barzilay
Cell Max Systems

A silent revolution took place this year. 2007 was the compliance deadline for the US Federal Financial Institutions Examination Council (FFIEC) guidelines for online banking user authentication, and marked the official launch of biometric banking, financial fingerprinting and eye scan economics. The age of biometric identification and verification has begun.

It's about time, too. A recent survey conducted by Javelin Strategy & Research found that while 35% of US consumers continue to use bank telephone systems to perform automated banking tasks such as checking account balances or paying bills, weak authentication measures still continue to be used for phone banking. According to Javelin, there will be increased theft attempts via telephone -- only 1 in 4 of US financial institutions ask for a full Social Security number, and only 8% require a password or answer to challenge questions.

Moreover, while Internet banking is gaining in popularity -- Forrester Research expects 76% of US households will be banking online by 2011 – this will most certainly include Voice over Internet protocol (VoIP).

At the same time, customers are irritated and confused by phone and online security measures. According to Forrester Research, many consumers believe that banks apply unnecessary measures to ordinary transactions. Plus, they're bombarded daily by news reports about identity thieves that leave them feeling unprotected and, in the long run, less likely to buy products from banks, insurers and, in particular, brokerages. The challenge: to provide a higher level of security that is also reassuring to customers.

The Case For Voice Biometrics

The FFIEC guidance eschews single-factor authentication (personal identification number-PIN, password or challenge question alone) and calls for the use of multifactor authentication, layered security and other methods that can be used to mitigate risk when allowing access to a system or network. Layered security requires customers to pass additional tests en route to performing additional transactions. Multifactor authentication must answer the question, "Is this person who he/she claims to be?" using three factors:

1. Something the person knows
2. Something the person has
3. Something the person is

Voice is a complex function created and generated by at least 15 physical parameters. Combine that with the knowledge of a PIN or password, and you have a strong security solution that nonetheless feels easy and natural to users.

The leading biometric technologies currently are fingerprint, AFIS (Automated Fingerprint Identification System), facial recognition, iris recognition, hand geometry, voice authentication and signature verification. All have their strengths and weaknesses but of all the options, voice biometrics is the only biometric output that can be delivered over any type of communication network: landline or mobile phone, wired and/or unwired virtual private network (VPN), voice over IP network (VOIP), radio network and, of course, local micro-

phone. Moreover, voice biometrics has the potential to replace the swipe ID cards, cash or tokens that get lost or stolen, PINs that are forgotten or used by others, and fingerprint and iris scans that require special equipment.

The accuracy of voice biometrics is also on the rise, with new technologies reaching Equal Error Rates (EER) of less than 1%. In a recent interview with Opus Research, Dr. Aladdin Ariyaeeinia, of the Audio Processing and Biometrics Group at the University of Hertfordshire in the U.K., noted that, "the effectiveness of voice biometrics has continuously improved over the last few years". Dr. Ariyaeeinia went on to say that, "when it comes to such applications as telephone banking, it is voice biometrics which is the preferred choice mainly because of the convenience, not requiring additional hardware, and cost."

By the way, voice biometrics, meaning speaker recognition, identification and verification technologies should never be confused with speech recognition technologies. Speech recognition technologies have the ability to recognize what a person is saying but do not recognize who the person is. Applications of speech recognition for security purposes or secure transactions are therefore limited. By contrast, speaker recognition, verification and identification technologies can be used to ascertain if the speaker is the person he or she claims to be. CellMax Systems, the company that I founded, provides both a speaker identification and speaker verification technology.

Voice Biometrics – Applications, Challenges and Solutions

Given its ease of use, ability to identify individuals remotely, and high rate of accuracy, the natural market for voice biometrics are companies and institutions interested in preventing identity theft. Applications in the financial and banking world include: on-site or remote ID verification services such as voice & card access control, call center access control, branch to branch transactions, VoIP Internet login, password reset, secured conference bridge, call center hidden authentication, VIP call centers, quality of service (QoS), blacklist warning and more.

"Voice hacking" has become a hot button issue, with spoofers using technologies such as voice changers

and scramblers to modify the quality of their voice, or playing back a recording of the fraud victim's voice, all in order to gain access to their account. Unlike speech recognition, voice biometrics is impervious to voice changer hacks. It is a physical biometric, as permanent and personal as the contour of a fingerprint or iris. Using the 15 physical parameters that create a personal voiceprint, the system makes calculations of voice input, taking voice instability into account -- even something as dramatic as an adolescent boy's voice cracking or a stuffy nose from a bad cold.

In the case of record & play spoofs, speaker identification and verification is backed up by speech recognition, wherein callers are always presented with new and different challenge questions at the authentication point, generated by random algorithm asking for a random sentence or number combination. Even the most persistent hacker would be hard-pressed to have pre-recorded all the answers in an ever-changing roster of personal questions.

There is also cost to consider: a pure software voice biometrics solution requires no special hardware – aside from the ubiquitous phone or mic – and is easily installed onto servers. It increases process automation for call and contact centers; a voice biometrics system recognizes an individual voiceprint within 3-7 seconds, while answering a challenge question takes 20-40 seconds. Voice biometrics can also be used to eliminate the time-consuming password reset process. With information input automatically, without the involvement of call center operators, data control levels rise, quality of service increases, wait time is reduced, and return on investment (ROI) can be achieved within a few short months.

Input quality, the most important factor, is greatly affected by the type of input device (professional microphone vs. cell phone, for example) and environment (noisy street vs. quiet office). State-of-the-art voice biometrics will automatically measure voice sample quality, then correct and clean it to produce the clearest possible data.

Multi-biometrics, the combination of two biometric techniques, allows the advantages of one overcome the shortcomings of the other (and vice-versa), and gives additional control over security levels. A new CellMax Systems invention combines the techniques

of voice verification and fingerprint matching for enhanced security. It comprises a voice registration unit that finds voice parameters in a registration sample and stores it in a sample database, and an RF-based fingerprint registration unit finds fingerprint parameters in a registration sample and stores it in a sample database. The result is an almost foolproof system that uses the tried-and-true biometric technique of fingerprint-based identification together with voice biometrics to improve verification.

Voice Biometrics – Technical Outline

Voice biometrics differs from the other forms of biometrics, as voice is a complex function created and generated by at least 15 physical parameters (see Fig. I):

1. Nasal cavity
2. Nostril
3. Lip
4. Tongue
5. Tooth
6. Oral cavity
7. Jaw
8. Trachea
9. Lungs
10. Diaphragm
11. Esophagus
12. Larynx
13. Pharyngeal cavity
14. Soft palate
15. Hardpalate

FIG I: VOICE BIOMETRICS - PHYSICAL PARAMETERS

These physical parameters are the basic constant body points that produce the sound waves of the human voice, are calculated as vectors and measured as a voice model or voiceprint.
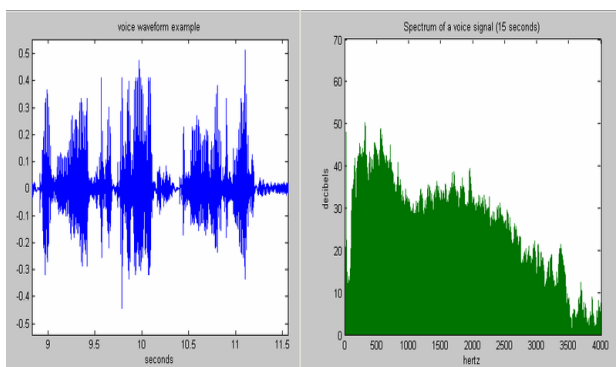

FIG II: VOICE BIOMETRICS – VOICE WAVEFORM AND SPECTRUM

Image courtesy of Wikimedia® a registered trademark of the Wikimedia Foundation, Inc.

Mathematically, sound is represented as a sequence of values, forming a temporal series. There are several techniques to extract features of time series and analyze the original sound waveform, without needing to individually analyze each point of the time series.

Like the other biometric markers, the result of a biometric measurement of the voice is totally dependant on 1. input, 2. accurate mathematical algorithms, and 3. computing power.

Input refers to the biometric sample, such as a voiceprint, taken and stored in a database.

Algorithms are a set of precise steps that describe a limited procedure or task. Algorithms in biometric systems are used to find out whether a sample matches the stored input. The more precise the algorithm, the more accurate the matching process.

Levels of accuracy are measured in terms of False Acceptance Rate (FAR)/ False Rejection Rate (FRR).

- J. Markowitz Consultants defines false acceptance as "when a speaker-verification application allows an impostor to get in." False rejection is "when a verification system rejects a valid user."
- FAR refers to the probability that a biometric system will incorrectly identify a valid user, or will fail to reject an impostor. FRR refers to the probability that a biometric system will fail to identify a true enrollee.
- Real-time algorithms refer to algorithms that process information and return results so rapidly that the interaction appears to be instantaneous.

Computing refers designing system to process voice biometrics data efficiently so that individuals are quickly identified and verified, or rejected.

Voice Biometrics - Technology

CellMax Systems utilizes a voice verification algorithm to provide an improved method and system for registering and authenticating secure, voice-based, e-commerce transactions over telecommunications networks.

The technology provides a method and system for voice registration involving three major steps:

- fractal analysis
- spectrographic analysis
- determination of Lyapunov exponents (see Glossary)

The method performs fractal analysis, where raw data is investigated and each sample gives a set of non-dimensional numbers that characterize a speaker's voice uniquely.

The method also produces a vector consisting of the aforementioned 15 physical voice parameters that form the key index for the verification.

The system performs a spectrographic analysis, investigating the raw data to generate a uniquely identifiable pattern.

The system includes a voice registration unit for providing unique initial identification by finding the speaker/user's voice parameters in a voice registration sample and storing it in a database.
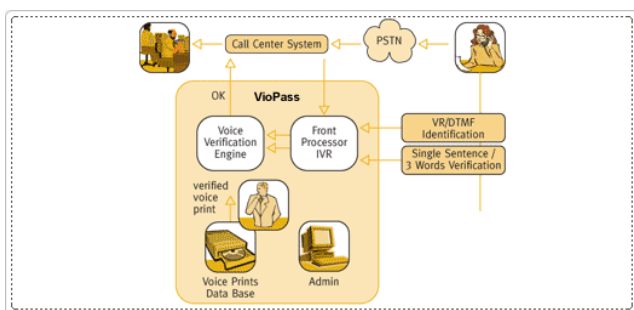
The system also includes a voice-authenticating unit for verifying one of a plurality of users. The voice-authenticating unit includes a recognition unit for providing a voice authentication sample that operates with the database. The voice-authenticating unit also includes a decision unit that operates with the recognition unit and the database, to decide whether the user is the same as the person of the same identity registered with the system. In this way, the user's identity is verified absolutely.

Conclusion

New high rates of accuracy coupled with ease of use will, in the coming years, make voice the biometric technology of choice for identification and authentication in an ever-expanding range of both stand-alone and multi-biometric applications.

According to a recent report by Dan Miller, Senior Analyst at Opus Research, the market for voice biometrics-based authentication software is maturing, having generated nearly $80 million in licensing and applica-

tion revenue in 2006. There has been greater acceptance by corporate security officers and IT integrators, and voice biometric-based authentication has proven its value to selected applications, such as password reset, in specific enterprises, such as call and contact centers. Miller forecasts $800 million in revenue for this market by 2011.

From the user's point of view, voice eliminates certain psychological barriers. Many people don't like the feeling of having their conversations recorded. However, with voice verification, no personal information is given -- it's rendered completely irrelevant because the person is the password and their voice is the verifier. Once people feel safe and comfortable they'll make more voice-based transactions.

This has great significance for all phone-based financial transactions. For example, brokerages and investment houses, cited earlier as vulnerable, could expand their business, secure in the knowledge that they're dealing with approved and verified solvent individuals, and that those individuals feel confident dealing with them.

Voice could also liberate the credit industry from plastic. Because your voice is your identity, you don't need that plastic card – you can leave it at home, it can get stolen – it doesn't matter. You're identified and verified on the spot, your credit card company gets satisfactory verification that you are you, and the supplier has indisputable verification that your credit is approved.

Clearly, legislation in the US and Europe is forcing certain changes on these institutions. Opus Research believes that a cut-off date for stronger phone channel authentication will be set by FFIEC for the end of 2008. Deadlines are closing in and non-compliance is not an option. The only question is whether conservative financial institutions will take the leap and implement new technologies that make the difficult tasks of identification and verification appear to customers as simple and natural as saying, "Hello, it's me".

BOX
Voice Biometrics - The Case For Standardization

The day is coming when voice biometrics will be part of everyday life, be it in on-site or remote situations. We will be able to call over a landline or mobile phone, laptop or PC; simply say a few words; be automati-

cally, instantaneously processed; and our secure transaction will begin.

However, industry standardization is needed to bring this vision into reality. The biometrics industry overall currently includes hundreds of separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. The voice biometrics segment alone includes dozens of hardware/software vendors.

Standards are now being formulated to provide a common software interface, allow sharing of biometric templates, and permit effective comparison and evaluation of different biometric technologies.

Actively involved standards organizations include:
- American National Standards Institute (ANSI)
- European Telecommunications Standards Institute (ETSI)
- International Standards Organization (ISO)
- International Telecommunication Union (ITU-T) International Telecommunication Union (ITU-T)International Telecommunication Union (ITU-T)
- Internet Engineering Task Force (IETF)
- World Wide Web Consortium (W3C)
- Institute of Electrical and Electronics Engineers (IEEE)

Biometric standards currently under development for voice interface include:
- Biometric Application Program Interface (BioAPI)
- Media Resource Control Protocol (MRCP)
- Voice Extensible Markup Language (VoiceXML)
- Voice Browser (W3C)

Of these, BioAPI has been cited as the one truly organic standard stemming from the BioAPI Consortium, founded by over 120 companies and organizations with a common interest in promoting the growth of the biometrics market.

In January 2007, ISO approved a new work group for standard for Voice Data File Format. Ziv Barzilay, founder and CTO of CellMax Systems and member of the Standards Institution of Israel, was chosen by the

ISO / International Electrotechnical Commission (IEC) Joint Technical Committee (ISO/IEC JTC) Special Committee (SC) 37 as the editor of the "Speech Data Interchange Format for Speaker Recognition" project.

The project's goal is to create an international standard that will enable universal installation, communication and interface between all voice biometric formats.

Glossary of Terms Used in This Article

AFIS (Automated Fingerprint Identification System) - A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc).

Authentication - The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: "This individual's name is 'Joseph K.' " or "This child is more than 5 feet tall." 2. In biometrics, "authentication" is sometimes used as a generic synonym for verification.

Authentication factor - In authentication, a factor is a piece of information used to verify a person's identity for security purposes. The three most commonly recognized factors are: 'Something you know', such as a password or PIN; 'Something you have', such as a credit card or hardware token; 'Something you are', such as a fingerprint, a retinal pattern, or other biometric. (Source: Wikipedia)

Biometric Application Program Interface (BioAPI) - The BioAPI Consortium was founded to develop a biometric Application Programming Interface (API) that brings platform and device independence to application programmers and biometric service providers. The BioAPI Consortium is a group of over 120 companies and organizations that have a common interest in promoting the growth of the biometrics market. The BioAPI Consortium developed a specification and reference implementation for a standardized API that is compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies. (Source: BioAPI Consortium)

Equal Error Rate (EER) - A statistic used to show biometric performance, typically when operating in the verification task. In general, the lower the equal error rate value, the higher the accuracy of the biometric system. EER is sometimes referred to as the "Crossover Error Rate."

Facial Recognition - A biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

False Acceptance (also: False Match) - Occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim.

False Acceptance Rate (FAR) - A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept.

False Rejection (also: False Non-Match) - Occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.

False Rejection Rate (FRR) - A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject.

Fingerprint Recognition - A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems.

Hand Geometry Recognition - A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

Identification - A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity.

International Organization for Standardization (ISO) - ISO is a network of the national standards institutes of 146 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. Although ISO standards are voluntary, the fact that they are developed in response to market demand, and are based on consensus among the interested parties, ensures widespread applicability of the standards. Consensus, like technology, evolves and ISO takes account both of evolving technology and of evolving interests by requiring a review of its standards at least every five years to decide whether they should be maintained, updated or withdrawn. In this way, ISO standards retain their position as the state of the art, as agreed by an international cross-section of experts in the field.

Iris Recognition - A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes, as illustrated below. The iris muscle is the colored portion of the eye surrounding the pupil.

JTC 1/SC 37 - Established in June 2002, ISO/IEC Joint Technical Committee 1 (JTC 1/SC 37) is the international technical committee within ISO responsible for creating and maintaining standards in biometrics. SC 37 is comprised of 26 participating countries with numerous others observing. SC 37 works in conjunction with SC 17, which is the international technical committee for cards and personal identification, and SC27 that is responsible for IT security for ISO. (Source: BioAPI Consortium)

Lyapunov exponents - One of a number of coefficients that describe the rates at which nearby trajectories in phase space converge or diverge, and that provide estimates of how long the behavior of a mechanical system is predictable before chaotic behavior sets in. (Source: McGraw-Hill Dictionary of Scientific and Technical Terms)

Media Resource Control Protocol (MRCP) – MRCP specifies a common interface to media processing resources that provide capabilities such as automatic speech recognition, speech synthesis (text-to-speech), as well as speaker verification and identification. MRCP allows client devices, such as VoiceXML browsers, to interact with these resources in a standards-based, vendor-independent manner. There are

two versions of the protocol; the original MRCP (now commonly referred to as MRCP v1) draft has been superseded by the newer MRCP v2 specification, which is under active development by the Internet Engineering Task Force (IETF). (Source: The VoiceXML Forum)

Recognition - A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply the verification, closed-set identification or open-set identification (watchlist).

Retinal Recognition (also: Retinal Scan) - A biometric technique that uses the unique patterns on a person's retina to identify them. (Source: Wikipedia)

Signature Verification (also Dynamic Signature Verification or Signature Dynamics) - A behavioral biometric modality that analyzes dynamic characteristics of an individual's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Verification - A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Voice Browser – A web browser that presents an interactive voice user interface to the user. In addition, it typically provides an interface to the PSTN or a PBX. Just as a visual web browser works with HTML pages, a voice browser operates on pages that specify voice dialogues. Typically these pages are written in VoiceXML, the W3C's standard voice dialog markup language, but other proprietary voice dialogue languages remain in use. (Source: Wikipedia)

Voice Recognition (also Speaker Recognition) - A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said and is not a biometric technology.

Voice Extensible Markup Language (VoiceXML) - VoiceXML is a markup language for creating voice user interfaces that use automatic speech recognition (ASR) and text-to-speech synthesis (TTS). (Source: W3C)

VXML Forum - An industry organization founded by AT&T, IBM, Lucent and Motorola to establish and promote the Voice eXtensible Markup Language (VXML). The goal of VXML is to make Internet content and information accessible via voice and phone. (Source: VoiceXML Forum)

Source: National Science & Technology Council's (NSTC) Biometrics Glossary unless otherwise noted. http://www.biometricscatalog.org/biometrics/GlossaryDec2005.pdf

About the Author

Ziv Barzilay is the founder, Chairman and Chief Technology Officer and Founder of voice biometrics company CellMax Systems Ltd., as well as the developer and patent-filer of CellMax Systems' innovative technology. Ziv Barzilay is a member of the Biometric Committee at the Standards Institution of Israel (SII) and the editor of the "Speech Data Interchange Format for Speaker Recognition project" of the Biometric Committee of the International Standards Organization (ISO).

Biometrics: Deployment Considerations for Successful Implementation

Russ Ryan
National Biometric Security Project

As biometrics become an evermore critical component of next generation identity assurance and risk management systems, careful attention to pre-deployment considerations is vital to ensure interoperability, scalability, usability, reliability and security. Whether one is preparing to deploy traditional or emerging biometric modalities there are a number of deployment considerations that must be addressed to help assure a smooth deployment. These considerations can be broadly categorized as follows:

- Requirements Definition
- Operational Considerations
- Life-cycle cost Analyses
- Societal Issues

Requirements Definition

Requirements definition is key to the entire process. The first step should be a detailed vulnerability assessment. What is it you are trying to achieve and/or protect? What is its value? Who/what are you protecting it from? What are the implications should your protection fail? Once the vulnerability assessment is complete one needs to conduct application impact studies to help frame the operational and commercial issues: what are the functional, performance, and quality requirements? What are the cost limitations? What training will be required? Defined answers to these questions will result in a specification that is driven by the requirements of the application as opposed to being written to fit an untested vendor-proposed system. A good requirements definition will not only help you determine the degree of resources -- financial, material, personnel -- that the effort warrants; but also lead you to the biometric technology that best addresses your requirements.

With the vulnerability and application impact assessments complete the next step is to develop the statement of work. This step is so critical for it drives the shape of the proposals you will receive. It is extremely important that those responsible for developing the SOW not only be well versed in the operational aspects of the security system, but also have a thorough understanding of biometrics and the attributes and nuances of each modality with respect to its application environment. The SOW should focus on the application requirements….not on the technology. Allow the bidders to focus on the technology they believe will best address your requirements.

When evaluating proposals bear in mind that most vendors will support their product's claim of superior performance with their own test and evaluation results. The use of a third-party, vendor-independent testing program eliminates the bias that is inherent in many vendor claims. Additionally, a biometric device's performance is closely tied to the application environment. Therefore, device selection should be supported by thorough trade studies (paper or physical) with solution-based and weighted criteria. The use of independent biometric subject matter experts throughout the process of requirements definition and system specification development will help to ensure the system selected will produce the desired results.

Operational Considerations

The operational environment will also determine the performance level of the system i.e.: if the application anticipates a high throughput, speed of the application will be a determining factor in biometric modality selection. Another consideration is accuracy. One may think that accuracy is a given, but the degree of accuracy (False Accept Rate, False Reject Rate) can be modulated by the setting of the algorithms. From a commercial perspective, the security settings for a bank vault or a narcotic storage facility will be more stringent than those for entry into an amusement park or a health club. In the former, any False Accept is unacceptable; in the latter, a high throughput rate may be of most importance and a few False Acceptances may be tolerated.

Interfaces must also be considered. Will the new biometric system interface with existing legacy systems? Are the biometrics products selected compliant with existing biometric standards? (Standards conformance is key to seamless add-ons and interoperability.)

Life Cycle Costs

Another potential constraint is budget. When costing out a biometric system one must consider the total cost of operation (TCO). In addition to the initial hardware, software and installation costs, there are other costs to consider. These include:

- Enrollment costs. How many people are to be enrolled into the system? Are they co-located or are the enrollment sites geographically dispersed? How long is the enrollment process? How much time away from the enrollees' jobs will it take? How many employees will be conducting the enrollments….and how much training will they need to ensure a smooth and accurate enrollment process? Depending on the size of the application, these costs can mount up.

- Per use costs. How many biometric devices comprise the security system? What is the throughput? What costs are involved for each authentication…in terms of IT costs, personnel costs and device depreciation?

- Maintenance costs. What is the cost of maintaining the system: devices, software and underlying IT support?

- System revocation costs. If shortcuts were taken with the requirements definition and the newly installed system failed to fulfill expectations and had to be taken down what would be the cost to your company?

Societal Issues

Other potential operational constraints, though non-technical can be most crucial to a successful application. These are your employees, customers, contractors, all the individuals who are to be enrolled in the system. Many will have concerns about privacy. Some will wonder if and how easily the biometric data can be compromised or what happens to the biometric data after the application is complete…or if the data is secure during the data transmission stage. The best way to address these concerns is through employee training. Don't wait until the system is installed to explain it to your personnel. Educate them up front as to why the system is being installed, how it works and how it will change (hopefully for the better) their work environment. Make sure that you have a privacy policy in place prior to system rollout and that you publicize and explain that policy to your personnel.

In some cases you will have to deal with religious, cultural or physical exceptions. In such instances you will need to have an alternate method of exception handling. Finally, set and manage expectations. In virtually every case history we have reviewed early education has led to a smooth installation from a personnel perspective.

Phased Approach to Installation

In countless applications that we have chronicled in the forthcoming Volume II of our "Biometric Technology Application Manual", the key to successful biometric implementations is the use of a phased deployment approach. (See Figure 1). This is especially true for financial institutions where it is estimated that employees are involved in up to 40% of fraud/theft. The first phase of a biometric installation could be limited to employees at one or more locations. Upon understanding the operational implications of the system, its

costs and its benefits, the system could be expanded to employees at other locations…then on to contractors, suppliers or high-value customers. At each stage of deployment some operational, application or training modifications could be made to address lessons learned in the previous deployment phase.

Figure 1: Phased Deployment Pyramid

Figure 1: Phased Deployment Pyramid
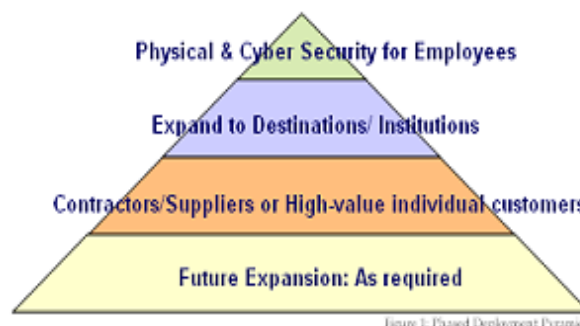
According to a 2006 report by Celent LLC of Boston, the phases of biometric adoption in the financial services industry are very similar to the example above. In the Celent example, phase one consists of bank employees; phase two, to begin in late 2007, will include some commercial clients; phase three will begin to see the capture of customer biometrics during the new account process in 2008; call center operations, online banking and ATM applications will see accelerated use of biometrics in phase four in late 2008/early 2009 followed by universal deployment beginning in 2009.

Emerging Biometric Technologies

Some of the more common biometrics in use today include fingerprint recognition, facial recognition, hand geometry, iris recognition and speaker recognition. However, there are a number of biometrics that are just beginning to find their niche in identity assurance applications and still others that are still in the developmental stage.

Dynamic Signature Analysis

Signature recognition authentication or dynamic signature analysis authenticates identity by measuring and

analyzing handwritten signatures. Dynamic signature analysis does not rely on the physical appearance of the signature, but instead on the manner in which a signature is written, using a stylus on a pressure-sensitive tablet to track hand movements. This technology measures how the signature is signed, looking at changes in pressure, position, and velocity of the pen during the course of signing, using a pressure-sensitive tablet or personal digital assistant (PDA).

Robustness

Dynamic signature analysis devices have proved to be reasonably accurate in operation and lend themselves to applications where the signature is an accepted identifier. Some systems have difficulties with individuals whose signature changes substantially each time it is written or with left-handed people.

Applications

Despite its user friendliness, long history, and lack of invasiveness, signature verification has not become a market leader like other biometric technologies (i.e., fingerprint). Most likely, the biggest market application for signature verification will be in document verification and authorization.

Keystroke Analysis/Keystroke Dynamics

Keystroke dynamics is an automated method of analyzing the way a user types at a terminal or keyboard, examining dynamics such as speed, pressure, total time taken to type particular words, and the time elapsed between hitting certain keys. Specifically, keystroke analysis measures two distinct variables: "dwell time", which is the amount of time a person holds down a particular key, and "flight time", which is the amount of time it takes between keys. The technique works by monitoring the keyboard inputs at thousands of times per second in an attempt to identify the user by his/her habitual typing rhythm patterns. These behavioral characteristics are then created into statistical profiles, which then become the enrollment template and verification samples. These templates also store the actual username and password

In comparison to other biometric technologies, keystroke dynamics is probably one of the easiest to

implement and administer. This is primarily because the technology is completely software-based; there is no need to install any new hardware. All that is needed is the existing computer and keyboard.

Limitations

Keystroke dynamics-based systems possess the same flaws as username/password systems, in that they do *not* ease the burden of having to remember multiple passwords, decrease the administrative costs of having to reset passwords; nor enhance convenience to the individual using the system. Rather, keystroke dynamics enhances the security to an existing username/password-based system.

Keystroke dynamics-based systems are only used in one-to-one verification applications and cannot be used in one-to-many identification applications due to the limitations in the matching accuracy.

Additionally, at the time of this writing, keystroke dynamics has not been fully tested in wide-scale deployments.

Applications

One potentially useful application is computer access, where this biometric could be used to continuously verify the computer user's identity. Dynamic or ongoing monitoring of the interaction of users while accessing highly restricted documents or executing tasks in environments where the user must be "alert" at all times (for example, air traffic control) is an ideal scenario for the application of a keystroke authentication system.

Vein Pattern

Vein biometric systems (also called hand vascular pattern recognition systems) record subcutaneous infrared (IR) absorption patterns to produce distinctive identification templates for users. The technology could be likened to a vascular "barcode" reader. Veins and other subcutaneous features present large, robust, stable, and largely hidden patterns that can be conveniently imaged within the wrist, palm, and dorsal surfaces of the hand.

Limitations

Obviously, gloved, otherwise covered or extremely dirty hands cannot be (or cannot easily be) identified using a hand vein pattern recognition system. Also, current vein pattern recognition systems use cameras that are not portable – or certainly less portable – than other technologies.

Applications

The technology can be applied to small personal biometric systems and to generic biometric applications, including intelligent door handles, locks, etc.

Some business applications are using vein recognition technology for time and attendance (to prevent "buddy punching"); allowance and payment control; login and information protection; safe deposit box access; e-commerce; membership management; and others.

Facial Thermography

Facial thermography refers to the pattern of heat in the face caused by the flow of blood under the skin. IR cameras capture this heat to produce a thermal pattern. Because the vein patterns in a person's face are distinctive, the IR thermal pattern they produce is also distinctive to each person. The process is based on the principle that, while the underlying vein and tissue structure is stable, the dynamic nature of blood flow causes fluctuations and the appearance/disappearance of secondary patterns. Environmental conditions (such as ambient temperature) and the introduction of alcohol or drugs, for example, can alter the thermal signature of the face.

This technology is better suited to determine "liveness" of the subject (no thermal image indicates no life) than for actual identification of the individual. Facial thermography, used in conjunction with other biometric technologies, could indicate a rested or fatigued person or determine physical condition, such as indications of alcohol use, although this has never been demonstrated in any commercially available technology.

Summary

The search for the perfect assurance of our identity or "uniqueness" may never be over. However, ***biomet-***

rics has clearly differentiated itself from other forms of identification that rely on something you own (driver's license) or something you know (password) in that you can't lose or forget your biometric. In some instances it might change over time (a result of accident, illness or prolonged harsh or abrasive usage) but any such changes will prove to be the rare exception rather than the rule as is the case with compromised passwords and lost i.d. cards. (How much does your organization spend each year in changing passwords?)

The issue of how biometrics impact the treasured right of or desire for "privacy" and our "civil liberties" is a valid concern. Any advance in automated human identification can be a double-edged sword; abused by those who dismiss the importance of the individual for the "greater good", yet also holding the potential as a tool for enhanced individuality and protection of identity when used properly. Achieving the proper balance is critical.

Trust Modeling for Security Architecture Development

Joel Weise
Sun

Information technology architects must build applications, systems, and networks that match ordinary peoples' sociological expectations of trust in terms of identity, authentication, service level agreements, and privacy. Yet the inherent insecurity of many business systems is, in fact, the failure of the underlying security architecture upon which those systems are built. In particular, deficient trust models often fail to address every layer of business, technology, people, and process. And the consequence might be an implementation with weaker security than the designer intended or expected. The trust model relies on complete requirements that include business, technical, legal, regulatory, and fiduciary requirements. We recommend that you develop a formalized trust model as part of a security architecture methodology and risk analysis for all business systems to ensure that they are protected according to their stated requirements and identified risk thresholds.

A key principle of effective security design and implementation is that security should be built into every

layer of a solution rather than added as an after-thought. This article describes the vocabulary of trust relationships and demonstrates the practical importance of using trust modeling to formalize the threshold for risk.

This article shows how to use a trust model to accomplish the following tasks:

- Elaborate on and provide context to the other components of a security architecture
- Determine and formalize a threshold for risk
- Support the risk analysis process utilized during the development of a security architecture
- Attenuate discovered risks

Understanding Trust

As with many seemingly complex concepts, a good starting point is to consider the commonplace, every-day meaning of a word. Trust is an important part of our lives and it has numerous definitions. Consider questions like the following, which we deal with regularly even if we don't formalize a model:

- What does it take to establish trust?
- How do I determine the degree of trust to assign to an individual or process?
- Would I trust a recommendation from an auto mechanic or a child care provider the same way?

Defining Trust

According to the ITU-T X.509, Section 3.3.54, trust is defined as follows:

"Generally an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects."

For the sake of defining trust and trust modeling relative to security architecture methodology, the following set of principles or elements are offered:

- Trust is a characteristic and quality of a security architecture.

- Trust is a balancing of liability and due diligence. For example, you must decide how much effort

to expend to reduce liability to an acceptable level for a particular business proposition and stated security policy. You must establish an equilibrium of trust.

- Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability.

- Trust is the binding of unique attributes to a unique identity, for example, accountability. This is both a qualitative and a subjective measure of expectations regarding another's behavior and relative to a defined security policy. Essentially, a trust relationship is established when a satisfactory level of confidence in the attributes provided by an entity is achieved.

- Trust is defined as a binary relationship, or set of compounded binary relationships, based on individual identity or unique characteristic validation. That is, trust is the establishment of a trust relationship through a validation process and the subsequent use of that relationship in some transactional context.

Establishing Trust

To establish trust or confidence, there must be a binding of unique attributes to a unique identity, and the binding must be able to be tested satisfactorily by a relying entity. When you achieve a satisfactory level of confidence in the attributes provided by an entity, you establish a trust relationship. This element of trust is commonly called authentication.

Trust involves a binary relationship, or a set of compounded binary relationships based on validation of unique individual identity. Consider the following examples of simple trust models:

- A trusts B. (Note that this means A can validate the unique identity of B. It does not mean that B necessarily trusts A.)
- A trusts B, and B trusts A.

A trusts B, B trusts C, therefore, A trusts C.

It is also important to note what a trust model is not. A trust model is not the particular security mechanisms utilized within a particular security architecture. Rather, it is the combination of those security mechanisms in conjunction with the security policy when they address all business, technical legal, regulatory, or fiduciary requirements to the satisfaction of a relying entity.

The examples noted here are, in effect, simple trust models. So let's proceed to the characteristics of trust that shape a trust model.

Defining Trust Modeling

A security architecture based on an acceptable trust model provides a framework for delivering security mechanisms. Trust modeling is the process performed by the security architect to define a complementary threat profile and trust model based on a use-case-driven data flow analysis. The result of the exercise integrates information about the threats, vulnerabilities, and risk of a particular information technology architecture. Further, trust modeling identifies the specific mechanisms that are necessary to respond to a specific threat profile.

To provide a baseline, we define trust modeling as follows:

- A trust model identifies the specific mechanisms that are necessary to respond to a specific threat profile.

- A trust model must include implicit or explicit validation of an entity's identity or the characteristics necessary for a particular event or transaction to occur.

Gradients of Trust

The purpose of a trust model is to respond to a specific threat profile. A threat profile is the set of threats and vulnerabilities identified through a use-case-driven data flow analysis that is particular to an organization. Essentially, a threat profile identifies likely attackers and what they want.

The level of trust necessary for one organization or circumstance may be different from the level of trust required by another organization or circumstance. For example, the level of assurance that an organization needs regarding the authentication of a user may be different in particular use cases.

Trust exists on a gradient—there is no one-size-fits-all solution. To illustrate this point, consider the requirements of two institutions: a public library and a financial institution.

- The library may implement a minimal trust model for those who simply want to browse the stacks. Perhaps the only check will be upon exit to ensure books are not being stolen. However, the library will probably implement a somewhat more stringent model for those who want to check out books. Commonly, the library will issue a library card with your name on it, and perhaps with your picture, to increase their trust that you are who you say you are.

  There may be specialized collections (for example, rare manuscripts) that are accessible only to qualified researchers. Your library card serves to authenticate you, but you need additional privileges beyond what is standard. Granting specific access privileges is the process called authorization. A possible requirement for this authorization would be proof that you are on the staff of a recognized educational institution.

- Now, consider a financial institution that is entrusted to maintain a great deal of personal information about clients and that is heavily regulated by various governmental agencies. Clearly, a more robust trust model is in order.

For example, if a customer wants to use a home banking application to review his account, before the bank's application transmits the customer's data, it must validate the customer's identity. Commonly, banks require a login, supplemented by a personal identification number (PIN). But once a customer has been authenticated, the bank must take extra steps to protect the confidentiality of the customer's data, perhaps by establishing an encrypted tunnel between the bank's distributing application and the customer's home banking application.

These examples illustrate three points that are essential to understanding trust and trust models.

- Trust requirements must be matched to the specific kinds of threats or vulnerabilities facing an organization and to the degree of risk that the threats will occur.

- There must be a starting point in establishing credentials for identity. In our example, the library may have accepted a driver's license as the credential for granting a library card. What credential does the issuing authority of a driver's license require for granting a driver's license?

- Trust does not happen spontaneously. It requires a methodical process of credential establishment and consistent validation. Trust is not free, it takes capital and effort..

Threat Profile and Risk Analysis

Threat profiles and risk analyses are intrinsically related. One without the other is of limited value.

Threat profiles identify the specific threats that are most likely to put your environment at risk.

The most common types of threats fall into categories such as:

- Actual or attempted unauthorized probing of any system or data
- Actual or attempted unauthorized access
- Introduction of viruses or malicious code
- Unauthorized modification, deletion, or disclosure of data
- Denial of service attacks

Looking at the above list, you might initially assume that all threats come from external sources, and that a system not on the Internet is not at risk. However, remember that poorly trained, careless, or malicious employees can represent every one of the threats mentioned.

So, how do you build and evaluate your specific threat profile? The recommended tool is a use-case-driven data flow analysis, the process of methodically tracing the flow of various use cases and their data throughout your system to identify threats and vulnerabilities. (Note that we differentiate between threats that are dependent on the specifics of a system's implementation, and vulnerabilities that are intrinsic to a system.)

Original Entity Authentication and Bootstrapping

Original entity authentication permeates all trust models. This refers to a situation where, before trust can be established, relying entities must be convinced of the identity of all other entities with which they communicate or conduct transactions. The level of satisfaction required to convince the relying entity should be specified in a published security policy.

As the name implies, original entity authentication occurs only once, at the beginning of a trust relationship. Returning to the examples of a library and a financial institution, the library was satisfied with a rather lightweight authentication process (such as quickly checking a driver's license), whereas the financial institution required more rigorous methods. And the more rigorous the original entity authentication process is, the greater the degree of trust.

To be more precise, original entity authentication establishes a credential that can be evaluated, tested, or referenced by an authenticator or relying entity. For the library, a plastic library card may be enough. For the financial institution, there may be some kind of cryptographic key that enables the use of different encryption services.

To ensure a reliable validation or authentication process, tokens or credentials must be unique and bound to a specific entity. Furthermore, there should be an agreed upon and standardized format for credentials, as well as for the protocols used to test those credentials. Such standardization becomes an important attribute when a trust model is implemented in an application or business system.

Let's step through the process of original entity authentication.

1. Entity A requests a trust relationship with Entity B.

2. Entity B, in accordance with its stated security policy, requires Entity A to provide proof (or various proofs) of identity.

3. Entity B validates these proofs of identity.

4. Entity B returns to Entity A some unique identity credential that Entity B can test to validate Entity A in future interactions.

The last step suggests the remaining requirement: bootstrapping. This means the association of a unique entity (Entity A) with a unique credential (provided by Entity B).

As emphasized earlier, trust depends on the ability to bind unique attributes or credentials to a unique entity or user. This is precisely the bootstrapping process. Central to a trust model is the assurance that this binding is completely reliable.

To put this in context, consider the example of a financial institution. Assume that the bank uses a public key infrastructure (PKI) for its home banking application. First, the bank requires proof(s) of identity from the customer who wants to bank online. Once the bank is satisfied (according to its own policies), it issues a unique identity credential in the form of a public key certificate. That certificate provides a unique binding of the customer's identity to a set of unique cryptographic keys. These keys are subsequently used to enable the reliable implementation of various security services such as:

- *Authentication*—Verification of identity.

- *Authorization*—Granting of specific privileges.

- *Confidentiality*—Information will not be accessed by unauthorized parties.

- *Integrity*—Data will not be modified by unauthorized parties.

- *Non-repudiation*—Legitimate transactions cannot later be denied by either the customer or the bank.

There must be an agreed upon and standardized format for credentials, as well as for the protocols that are used to test those credentials. This will be an important attribute when an actual trust model is implemented in an application or business system.

Qualities of Trust Relationships

This section describes some common qualities or characteristics of trust relationships. All trust models should exhibit these qualities to be considered viable.

Portability and Interoperability

Portability and interoperability are similar, but with subtle differences. Portability depends on standardized credential types and formats to be used anywhere, and at any time. The use of a standards-defined public key certificate recognized across multiple PKIs is an example of portability.

Interoperability depends on the standardization of protocols for testing credentials. Interoperability relies on applications and systems to implement standardized protocols for credential testing. The use of standards-defined protocols (for example, those from the Liberty Alliance) to perform security functions such as authentication and authorization across multiple platforms is an example of interoperability.

Reliability

Reliability embraces a closely related aspect of credentials and their evaluation. Credentials and the mechanism that evaluate them must perform consistently, in a repeatable fashion over time.Assurance

Assurance is a critical quality of any trust relationship. Relative to trust, assurance is concerned with the preservation of the binding between a unique entity and its credentials. Here, preservation means that a credential continues to be accurately bound with the correct entity to which it is associated.

Major Trust Models

This section discusses three primary trust models. Different organizations have different thresholds for risk, and the choice of a trust model should be based on that threshold. Specific security solutions should map to the applicable trust model.

Direct Trust

Direct trust exists when you perform the validation of an entity's credentials without reliance on any other entity. There is no delegation of trust, because all relying parties are subordinate constituents of the trust hierarchy. All entities gain trust by their association with a common entity responsible for the original entity authentication of each relying entity, always following a stated security policy. Distinct binary trust relationships are established between a common trust point and the various end entities.

A direct trust model is found in some architectures using a PKI. In this example, the root certificate authority (CA) initiates all trust relationships. The CA is the common trust entity that performs all original entity authentications and the generation of credentials that are bound to specific entities. A key difference with other models is that the direct trust model does not allow the delegation of original entity authentication. And every relying party must use this CA directly for all validation processes.

The advantage of the direct trust model is that the validation of credentials is performed by one's self with no delegation, thus ensuring a high level of confidence in every entity associated with the trust implementation. Direct trust is often necessary to reduce liability for organizations bound by regulatory or fiduciary requirements. Organizations involved with financial transactions, e-commerce, insurance, or health care should consider a direct trust model.

However, as we stated earlier, trust is not established without effort. The primary disadvantage of the direct trust model is that it may be more labor intensive and more expensive than other trust models.

Transitive Trust

Transitive trust is trust transmitted through another party. Transitive trust allows the following:

- Entity A validates and trusts Entity B.
- Entity B validates and trusts Entity C.
- Entity A trusts but does not need to validate Entity C. For example, Entity A trusts Entity C, but does not perform original entity authentication of Entity C.

Such a trust model is common in distributive or peer-to-peer systems. It relies on participating entities to align their security policies that control credential validation (for example, original entity authentication). In the preceding example, for A to trust C, A needs confidence that B has validated C by the same standards that A used to validate B. Because you are explicitly trusting another entity to perform credential validation, you should, at the very least, evaluate that entity's security policy, validation process, and position on liability management.

The advantage of the transitive trust model is that it enables the linkage of different entities that share similar security policies while reducing the credential validation effort.

Consider the following example of transitive trust, which is common with the frequency of bank mergers in recent years. You are a customer of Bank ABC, which is acquired by Bank XYZ. Because XYZ trusts ABC's original validation process, you are trusted by XYZ to continue your normal banking activities (unless previously allowed activity somehow significantly violates the new owner's security policy). The new portfolio owner has presumably reviewed, very carefully, ABC's financial statements, security policy, and validation process to have confidence in extending trust to the customers it gains through the acquisition.

Assumptive Trust

Assumptive trust is a formal name for a model that was earlier described as spontaneous trust. With this model, there is no mandatory, explicit, direct credential validation. With essentially no control over the validation process, you must either "take it, or leave it."

An example of an assumptive trust model is the pretty good privacy (PGP) web of trust. The validation of entities is essentially one personally vouching for another. Although this web of trust has some value for relatively simple activities, such as signing email messages, it is not sufficient in the business realm. Many users have false confidence that PGP is based on a transitive trust model, so it is important to emphasize that which differentiates a transitive trust model from an assumptive

one is the validation process (or lack thereof). A transitive trust model requires a validation process, and an assumptive one does not.

There are many other examples of assumptive trust models. If more than casual, noncritical information or processes are involved, you should consider implementing these and other protocols with at least a transitive trust model.

Conclusions

Trust modeling is not an abstract intellectual exercise. It is not something interesting to do if you think time permits but dispensable if you don't want to spend time on it. Trust modeling is an essential step in designing a secure architecture.

A trust model must be constructed to match specific business requirements. No generic trust model can be assumed to be valid for a specific situation.

Given the urgency of having a trust model and the need to construct it to match specific business requirements, it is important to assign the necessary resources to develop a model based on a threat profile and risk analysis and to identify the appropriate response mechanisms. Establishment of trust does not happen spontaneously or without effort.

Do not focus solely on technical solutions. As with all aspects of a security architecture, a successful trust model must consider people, process, and technology.

Finally, if you remember nothing else from this article, do not forget the following:

- Failure to understand what trust model (if any) is actually in effect can create a false sense of security that may lead to serious, even catastrophic, financial and legal problems.
- Adversaries exploit weak trust models.

References

ITU-T Recommendation X.509, ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks."

Safe Web Browsing Mode (SBM)

Dan Schutzer
FSTC

Overview

This paper reviews a concept we have been developing that we name Safe Web Browsing Mode (SBM). SBM is intended for the user who wishes to be sure that they are at the intended known, trusted website before they exchange sensitive information. SBM refers to a state that a browser can be placed in, where the user has both a real and perceived sense of security with respect to his/her knowledge that they can only be communicating and exchanging information with trusted websites and not a spoof. This is because when in SBM, the browser will only permit user-selected, highly trusted websites to be accessed. A highly trusted website is a website that can be certified as such. These are websites that have gone to some lengths to allow being reliably identified as authentic and trusted; that is, they have met the necessary technical requirements, as well as contractual requirements that include a rigorous certification and compliance process.

SBM is ideal for users who want to be careful before they conduct financial and other high risk transactions and information exchanges with a website, and desire higher assurance that they are communicating with the intended site, e.g. their bank. When in SBM mode the browser will only permit user-selected websites that can be validated as being highly trusted to be accessed. This prevents the user from being able to receive and/or log on to the wrong site, an untrustworthy site.

General Principles Of Safe Web Browsing

The user must take an active step to go into and out of SBM. This could involve clicking a special control sequence. This mode of interaction requires the user to know of and take explicit actions up front. When a browser is placed in SBM by typing in the SBM control sequence, and a user attempts to access a web page, that page will not be delivered unless it can be verified as one of the selected highly trusted websites.

In various usability studies it has been found that both "good indicators," (e.g. green bars or locks that cur-

rently are used to indicate the user is at a good website and/or is exchanging information with the website securely); and "bad indicators" (e.g. red alerts that indicate the website is a spoofed or untrustworthy website) are often ignored by many users. Furthermore, the absence of these "indicators" (good or bad) is often overlooked by many users. In addition, even poor spoofs of these indicators (indicators painted outside the chrome, or painted over the chrome) can fool enough users to make them not particularly useful. If users are somehow automatically placed into SBM mode without any action on their part, we are back to the same problem we are trying to avoid, which is getting users to recognize something that is "safe" solely on the basis of some kind of visual or other cue.

SBM creates a separation between the space where users conduct sensitive transactions from the space and where they casually browse the internet. When in SBM mode, the browser should have a distinct look, but the success of SBM is not dependent upon the user actually paying attention to this look.

One way to achieve this would be to require the website to belong to a community (e.g. FI, healthcare, government) that is willing to work with the EV CAB Forum, and the EV certificate issuers, to put in place a process that would allow a website to apply for an EV Cert with a Community logo type. To obtain this logo, the community authority must strongly certify those of its members who have agreed to meet special technical, contractual, audit and compliance requirements, and to put its website through a rigorous certification process. Only websites signed by an EV Cert with an approved Community logo type would be allowed to be accessed by the browser when it is in Safe Web Browsing Mode.

When in SBM, the browser will be automatically placed in a default highly secure mode, where the browser's security settings are pre-selected. Many features deemed dangerous will be turned off. The current security zone interface, such as in IE7, provides a long list of very technical terms that a user has to select, and it is somewhat cumbersome to change and reset. We would like something much simpler to be invoked by the user, which by default eliminates when in safe mode all but the sites that both qualify and are selected by the user, as well as selecting a default security zone setting (most of the technical settings for safe

mode are determined for the user, but if the user wishes he/she can see the settings).

SBM should be designed to be extensible. The initial operational capability will be built by adapting currently available technologies (e.g. EV Certificates with logo type extensions). However, SBM should be able to be strengthened over time, by including new, better technology that can be used to authenticate a website, as they become available (e.g. CardSpace and its Open Source equivalent; a Community CA Bridge similar to the Federal Bridge; DNSSEC; a stronger, more tightly controlled Top Level Domain).

The user can accept all highly trusted sites, or can start out with an empty personal list and can add allowed "trusted" sites to the list as they are accessed and used, much as one now adds to their web favorite list, provided the site is approved to be accessed while in SBM. The user can also take away sites from being accessed in SBM. Alternatively, the user can choose to enable all the sites approved to be accessed while in SBM.

Although the creation of a SBM mode is vitally important to the financial services community where real dollar losses to our customers is at stake, the notion of safe browsing is inherent to many other communities; e.g. e-Bay, Amazon, your health care provider. SBM should therefore be developed so it can scale up to include any interested community that is willing to enforce compliance with the stringent technical and contractual requirements.

As with privacy, there may ultimately be different degrees of trust (multiple SBM levels, associated with different communities of varying trust, related to the strength of the technical and contractual certification process and the relevant rules and policies governing the community with respect to security measures and behavior subscribed to by participating members). However, to start with, we might keep things simple; either a site is trusted and included in SBM, or not.

The goal of SBM mode is not to eliminate phishing attacks, but to protect those who are willing to take proactive steps to avoid them. SBM mode will not be required, but will be voluntary

It should be pointed out that the concept of filtering out certain websites is not new. There are already various

filters and a number of circumstances where browsers, or browser add-ons, already block web sites from being accessed, so the concept of blocking a website is not entirely new or unproven in use. Examples include as anti-spyware blockers, privacy filters, and parental control filters (e.g. filtering out pornographic sites). SBM differs in that it doesn't block certain specified sites, but only allows certain eligible sites; it blocks sites that are not verifiable as well-known, often visited, trusted sites. This concept of a "white list" is also not entirely new; Miss America is providing a browser for kids, which only allows access to parental approved websites.

Operational Concept – How This Might Work?

To provide a better understanding of SBM, we have provided below an illustration of how this might work:

When a user opens the browser, the first page they see requests them to click on one of two choices:

1. Go into Safe Web Mode (restricted to only trusted websites)

2. Browse the entire Internet

When in Safe Mode, the entire browser chrome will be a distinctive different color, such as green. There should be a default color, but it should be adjustable by the user. A button will appear in the chrome that says "Safe Mode, click to return to Full Internet." When not in Safe mode the button, will say "Full Internet Browsing, click to return to Safe Mode"

Once selected, the browser will stay in Safe Web Mode until the user either closes down the browser, or clicks on a button in the Chrome that says "return to Full Internet"

Anytime a user is at a web site, the user should be able to "add" or "delete" that site from Safe Mode. There should be a button in the chrome that allows this action.

To be added to Safe Mode, a site must be qualified. If a site is not qualified to be in placed in Safe Mode, and a user attempts to add this site to Safe Mode, the browser will return a message that says "This web page is not qualified to be viewed in Safe Mode"

To be allowed in Safe Mode, a site would have to con-

form to the requirements specified in the Safe Web Browser Recommendation; namely, the site must be able to be authenticated as a safe site (for example: page must be digitally signed with an appropriate certificate and logo type, which validates the site has undergone appropriate investigation and on-going auditing by an authorized authority, and the site's IP addresses match addresses previously registered and signed by registration agent).

When in Safe Mode, besides the web page checking, the browser's security settings will be automatically set to maximum protection.

Card Space Example:

Another example is how this might work in Card Space, or its Open Source equivalent. This is described below:

Some cards are managed, some are personal (self-issued) . One way this could work is that the banks or some entity for the banks would issue cards for their users. If a bank issued its own card to access its website, it would be both a Relying Party and the Identity Provider. The bank website will only accept its own managed card issued to the user. When in the equivalent of a safe browsing mode (could be invoked in a manner similar that described above for web browsers), the only cards not grayed out are those issued by this "trusted websites" who agree to operate under the "trusted" terms and who issue cards which first validate the website as authentic before providing any user authentication.

If a site attempted to accept this bank-issued card for authentication of their site, first the card would attempt to authenticate the requesting site as the real bank site that issued the card;only after this website authentication would the card authenticate the user. If the site did not pass the authentication test, its site would not be allowed to be accessed while in safe mode. This validation could be done by checking the signature or using some other mutual authentication protocol.

Expected Behavior

Over time and through education, it is hoped that more and more users will elect to invoke SBM mode before they bank on-line, or do other high risk transactions where personal information is exchanged and high risk

transactions performed. In fact, banks and other "trusted sites" could incent users to only access them on-line via SBM Mode (e.g. provide loyalty points, safety guarantees, fee discounts or higher interest rates).

Once SBM is widely understood, it might also help with embedded links in emails. If a user got an email from a "trusted website" (or one they believe is coming from a "trusted website") with a link in it and they wanted to be extra-sure that this was a link to a genuine bank web site and not a phony (phishing) website, they could select SBM mode, and let the browser filter out all non-authentic websites from being accessed.

Requirements

The Secure Browsing Mode needs to be extremely difficult, if not impossible, to fool into passing through an "untrusted site". This is assured by the technical requirements imposed on the website and on a conforming browser.

The user should also be able to include in Safe Mode any website that has met the technical requirements to be reliably authenticated and that the user knows sufficiently well so that they do not require a certifying community type logo. An example of this would be a user, who is an employee of Corporation X, who wishes to be able to access his company's website under SBM.

One thing SBM is not: it is not a defense against malware. For example, if your browser is infected with malware it could do things during that session that you are not aware of; it could quietly watch what you do, waiting until you log into a bank, then perform a transaction you are not aware of. So, SBM would need to be augmented with other protections, such as anti-virus, anti-spyware protection, and keeping your computer patched with all the latest software updates. Some vendors, such as Authentium, claim to provide defenses against malware along with SBM-like browsing capability. We are also in discussions with Microsoft research staff who are also working in this direction.

Summary

This paper introduces the concept of Safe Web Browsing and provides the motivation behind it and some supporting rationale as to why we think it would be effective. Finally, a list of implementation requirements is presented. This concept is being talked about as a recommendation by the W3C Web Secure Content Working Group and Microsoft and other vendors are looking at implementations for browsers (e.g. IE7) and CardSpace. We are also working with the Higgins Group on an open source version. If you are interesting in working with FSTC on this concept, please contact us and we will help get you involved.

References

[1] Dhamija, R., Tygar, J., and Hearst, M. "Why Phishing Works" In Proceedings CHI. (2006)

[2] Jackson, C., Simon, D., Tan, D., and Barth, A. "An Evaluation of Extended Validation and Picture-in-Picture Attacks" In Proceedings Usable Security. (2007)

[3] Shneiderman, B. "Designing the User Interface". [4] Wu, M., Miller, R., and Little, G. "Web Wallet: Preventing Phishing Attacks by Revealing User Intentions" Symposium on Usable Privacy and Security. (2006) RecommendationDisplayProposals/RecoTempl (last edited 2007-06-06 15:58:01 by ThomasRoessler)

Putting strengths of FRAC cards to work help companies achieve ROI

Robert Brandewie
ActivIdentity

Once financial institutions have set a course for issuing and managing First Responder Access Cards (FRAC), they must draw on the strengths of the smart card – network authentication, single sign on, digital signature and data protection and encryption – to stimulate their use, capitalize on the security enhancements that the cards can bring, and increase the companies' return on investment (ROI).

"CIO's must use their ingenuity and business acumen to match these new capabilities to real world business problems in their organization – thereby maximizing

the returns for their agency," said Jason Hart, CEO at ActivIdentity.

As it turns out, the difficult march toward adopting an in-house solution, a managed service option or an out-sourcing approach to rolling out smart cards in the face of HSPD-12 and FRAC, is only half of the battle.

HSPD-12 and FRAC "means the use of a single token (PIV Card) to access facilities and to log onto information networks," says Philip Lee, a partner at the Identity Alliance.

Getting workers to overcome lingering resistance and actually use the cards is another struggle altogether – one that requires finding a compelling application or two that make cardholders keenly aware of the value of their smart card – and also solves pending security issues for many companies.

Today's cards feature a number of capabilities that can increase their value in an agency and make workers want or need to use them.

Network Authentication

Determining whether a user is who he or she claims to be when trying to access a network has never been easier than with the FRAC cards. Instead of users having to remember long, complicated passwords that change every 30 days or so, required authentication information is carried in a protected mode on the card.

The most cardholders have to do is remember a personal identification number (PIN), much easier because the number is shorter than a password, rarely changes, and can be used for all enabled applications.

This helps boost security, too, by eliminating the likelihood that users will jot down passwords and other security information on a sticky pad. The results can be stunning. Using common access cards to support its Public Key Infrastructure (PKI) initiative, the Defense Information Systems Agency (DISA) has already seen a dramatic downturn in successful network attacks.

Similarly, the number of help desk calls should decline,

since users don't have to remember or regularly change their network password.

Application Authentication and Single Sign-On

Widespread use of smart cards make it possible for financial institutions to set up single sign-on privileges for workers. "It's basically the end of user authorization," says Hart. "Once you're on, you're on."

Single sign-on provides a secure store of user name and passwords that can be stored on the smartcard – protecting them and requiring another factor for authentication. Used this way, single sign-on can serve a bridge technology - providing increased security for legacy applications while they are modernized with more secure access methods like PKI.

Printer Authentication

Despite establishing stringent security policies and specific guidelines for handling sensitive information, financial institutions face continuing challenges as technology improves. One relatively new area of concern is the increasing capabilities of printers to scan, print and even forward information. These multifunction printers provide great productivity enhancements but can present a challenge for protection of sensitive information. In addition, documents containing privacy-related or other sensitive data are often sent to unsecured, shared printers.

Using FRAC cards can help staunch the flow of sensitive information to printers and beyond. User identities are authenticated using the card and the worker can only access the device or perform a function if authorized. In addition, audit files are generated that allow management to review transactions to ensure compliance with agency regulations.

Printer manufacturers are already working smart cards into the equation. For instance, Hewlett- Packard recently announced that its printers now had these capabilities and would require smart card based authentication before printing, emailing or scanning a document.

Data Protection and Encryption

Much of the strides in data protection and encryption have focused on data in transit. But as many financial institutions have learned, sensitive data is often in jeopardy when data is atrest in a laptop computer or other mobile device that has been lost or stolen.

The names and social security numbers of state employees in Ohio recently went missing on a back-up tape that was stolen out of the unlocked car of an intern. And remediation can be expensive – involving extensive investigative resources, outreach to the people who may have been impacted, and even buying identity theft protection for those affected.

But technology is available that ties encryption to FRAC cards and lets workers use the cards in combination with data at rest encryption software to protect the information. "This new technology adds another level of security, another factor for authentication while protecting the privacy of any customer and the confidentiality of an agency's business data," says Hart.

About The Author

Robert Brandewie has more than 30 years of identity strategy and policy development experience. Prior to joining ActivIdentity as SVP Public Sector Solutions, Robert served as Director of the Defense Manpower Data Center (DMDC) and was architect of the Common Access Card system (CAC) for the Department of Defense.

Digital Home Issues and Opportunities

GBDe Digital Home Issue Group

Driven by widespread broadband Internet access and the convergence of hardware, communications, and content, digital home services have gradually become a reality in recent years. The broadband access subscribers in Japan – 50.9% of households use BB access at '07/March -- which may lead to the provision of abundant and useful Internet services for daily life. In Taiwan, Chunghwa Telecom and Intel conducted joint research on "Understanding Taiwanese Perception of Digital Home" in 2007. The awareness of digital home overall is high. Over 54% of respondents like the digital home concept and 40% will adopt digital home in the next 12 months. Home is almost ready to provide access to coming integrated services. A private home will become more intelligent and convenient with home networking and new and emerging online digital home services.

In light of current developments, GBDe initiated the Digital Home Issue Group (IG) in 2007 to facilitate global dialogue on issues related to digital home. The findings of Digital Home IG indicate that digital home service should be a comprehensive service package but that many issues still need to be resolved before the promise of digital home can be fully realized. Furthermore, to promote advanced and comprehensive development of digital home, there needs to be a cohesive promotion platform involving government, IT/CT industries, network operators, home builders, and service providers.

Trend of Digital Home Solutions

To understand the current circumstances, motivations and expectations of the digital home industry, Digital Home IG carried out a survey of trends in digital home solutions in the different countries.

Regarding the scope of digital home services, respondents were queried about specific examples of operating digital home services, such as Home Monitor/Control, Home Banking, Home Healthcare, High Speed Surfing, High Speed Downloading, Video Communication, Entertainment, and Education. As the survey shows, the most popular and well-known digital home service is Entertainment, with High Speed Surfing close behind. Entertainment is also recognized as being first priority of digital home service deployment. Video Communication, High Speed Surfing, High Speed Downloading, and Home Monitor/Control are considered as the next focus topics. Entertainment will drive the consumers to buy digital home solution. Respondents also think that Entertainment is most suitable for cross-border application.

Digital home is an emerging service, and various stakeholders and players are involved in building a new business ecosystem around it. What is the preferred business model for digital home service?

- Most people prefer that content providers offer and operate digital home services, with access providers next most preferred.
- Consumers prefer service providers to cover installation and training of the digital home solution rather than home builders or retailers.
- Service providers should also cover maintenance of the digital home solution.
- The best way to offer the digital home service is by bundling with device(s).
- Pay-by-month or pay-by-use is the best pricing structure for service content, and one upfront payment is most suitable for device/equipment.
- New construction is the best entry point for digital home market.

The value chain of the digital home market includes service providers, IT/CT device makers, and consumers. As digital home technologies increase in complexity, all vendors seek to offer more proactive solutions. The major considerations of each party in digital home value chain are:

- Two major considerations for consumers are Ease-Of-Use and Price.
- Two major considerations for service providers are Maintenance and Price.
- The main consideration for device makers is Price, followed in order (with only insignificant difference) by Installation, Ease-Of-Use, Security, and Maintenance.

Issues Involved in Digital Home Services

As digital technologies become mainstream, consumers have more incentive to purchase digital home services. For obvious reasons, consumers would like a total solution that integrates value-added services with end-user products and network access. A good service must provide products, value-added services and applications, meaning the service must also have close links to installation, configuration, extended warranties and troubleshooting. In addition, as consumers acquire and create more and more digital content, the demand for reliable, economical, and high-capacity storage and backup solutions is growing. The service delivery network must handle the bandwidth requirement, IP addressing, and quality-of-service. For the home network, digital home control software is needed to automatically recognize the insertion of devices into the network, to read the contents of newly added de-

vices, and to direct the contents from any device to any other devices. The end point for users to enjoy digital home services will be new IP-based devices with wired or wireless connections. Furthermore, home Internet users are concerned about Internet security and privacy. It is imperative to be able to prevent unauthorized capturing and further dissemination of private content through network intrusion when home IP devices are exposed on the public Internet and hence subject to hacks and attacks. For the sake of safety, regulations are needed to clarify whether or not the installation of digital home products must be conducted by certified technicians and whether or not service providers must obtain operation license before they are permitted to offer services.

The value chain of digital home solution includes broadband service providers, cellular carriers, Internet portals, home builders, service installers, IT/CT product makers, and consumers. Although various digital home services have been fervently promoted and many kinds of small service systems are now on the market, issues still need to be addressed before the promise of digital home can be fully realized. Figure 1 shows these digital home issues covering considerations on service, network, device, users, and regulatory aspects.

Figure1. Issues Involved in Digital Home Services

Proposed Promotion Framework

To promote advanced and comprehensive development of digital home, it is important to establish a relevant framework supported by the government, IT/CT industries, network operators, home builders, and service providers.

- The government should set up the digital home industry's supply chain, promote common industrial standards, and enhance the interoperability of products. They should also establish national R&D programs, experimental projects, and models for government-industry collaboration.

- IT/CT industries should establish a common platform on which to provide seminars and share information on markets and marketing, technical standards, patent application maps, compatibility testing, and advanced resources for product development.

- Network operators need to build up network infrastructures and provide home networking set up service.

- Home builders should provide solid infrastructure for digital home services, including building automation and e-Home functions to satisfy customers' entertainment, leisure, safety and security needs.

- Service providers should coordinate their efforts to bring about inter-connectability of digital appliances in customers' homes and develop platform management technology to ensure compatibility of different machines. They also should contribute toward the establishment of business models.

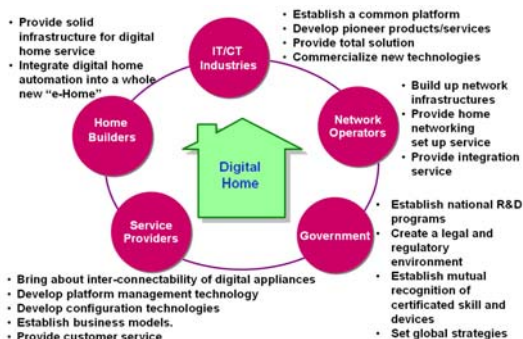Figure 2 shows the proposed promotion framework for developing digital home services.

Figure2. Proposed Promotion Framework

About the Author

The Global Business Dialogue on electronic commerce (GBDe) is a worldwide, CEO-led, business initiative, established in January 1999 to assist the development of a global policy framework for the emerging online economy. GBDe has been actively promoting a private sector/Government dialogue on convergence-related issues since 2001.

The GBDe has initiated the Digital Home IG in 2007 so as to facilitate the global dialogue for exploring related issues of Digital Home. The Digital Home IG members include Chunghwa Telecom, NEC Corporation, Intel Taiwan and Microsoft Taiwan and lead by Chunghwa Telecom.

FSTC STANDING COMMITTEES (SCOM)

Business Continuity (BCSCOM)
FSTC Managing Executive: Charles Wallen

Security and Infrastructure (SSCOM)
FSTC Managing Executive: Mike Versace

Payments and Check Imaging and Truncation (PSCOM)
FSTC Managing Executive: John Fricke and Dan Schutzer

Banking Techynology Operations (TOSCOM)
FSTC Managing Executives: John Fricke and Dan-Schutzer

If you are interested in getting involved in any of theseStanding Committees, contact the appropriate Managing Executive or Dan Schutzer, Executive Director.

Project Initiatives

FSTC projects center around supporting the themes of **Strengthening Identity**, **Reducing Fraud**, **Improving Resiliency**, and **Promoting Interoperability,** which all contribute to providing the necessary foundations to improve the effectiveness, acceptance and profitability of important Financial Service business applications,such as **Improving Payments**.

Below is a short summary of current FSTC project initiatives in progress and formation. If you have an interest in learning more about any of these projects, or joining them, visit our website www.fstc.org, or contact John Fricke or Dan Schutzer:

- **Resiliency Maturity Model Initiative**
  FSTC's Resiliency Maturity Model (RMM) developed in collaboration with Carnegie Mellon CERT provides a framework that allows organizations to systematically measure and improve capabilities to manage operational risk and resiliency. The Model provides unbiased common ground for enterprises, third party service providers, and government agencies to develop cost-effective risk management solutions. The focus of the RMM 3B initiative is implementation, benchmarking and the building of a toolkit to support the broader utilization of the Model.

- **I2PADS Account Opening and Funds Transfer**
  In conjunction with OMG, FSTC isinvestigating and developing recommendations for next-generation business process models for account opening and funds transfer, where the financial processes are modified to be more efficient and secure. This project looks at ways of minimizing or eliminating the need to exchange and sensitive information, even to the point of eliminating the need for relying on information, such as social security and account numbers that is increasingly accessible by fraudsters. The project manager is VISA. This area is likely to be focus of next FFIEC guidance.

- **Fighting Fraud: Better Collaboration Tools & Real-Time Sharing of Information**
  Real-time sharing of information on fraud incidents and patterns to improve fraud forecast, detection and mitigation is the focus of this project in which we will determine the feasibility and benefit of near real time sharing models of fraudulent behavior, better prediction and mitigation of fraud, and better forensics and prosecution. This project will result in an analysis of legal and regulatory requirements related to sharing of information; a taxonomy of available fraud and fraud pattern data and services; a taxonomy of fraud patterns and a concept of operations. E&Y is the project manager

- **Capture System Calibration**
  This is a mini project during which we are testing the current version of the Harland printed Capture System Calibration documents developed as a result of the FSTC Project. During the initial project, the FSTC project team reviewed over 20,000 images of test documents from over 45 capture runs on 30 different systems to identify key drivers of differences between captured images. As a result of this testing, FSTC developed a calibration document, which can be used throughout the industry to ensure that image capture systems are creating consistent images within desired ranges of performance. This will be particularly useful for remote capture equipment. While this project will help all participants to get familiar with the calibration documents, the output will be to update the scoring document produced as a result of the initial project. Frank Jaffee is the project manager

- **Authenticating the FI to Consumers and Safe Web Browsing**
  This ongoing project involves the development of use cases dealing with authenticating the financial services institutions to consumers, along with applicable threat analyses, processes, evaluation metrics and the testing of combinations of various important emerging technology solutions against these financial services community use cases and requirements. This process utilizes a Columbia University lab for testing the use cases.

- **Safe Web Browsing Mode (SBM)**
  Addresses the need for the user who wishes to be sure they are at the intended known trusted website before they exchange sensitive information. The browser can be placed into a mode which will only permit known trusted websites to be accessed while in this Safe Browsing Mode (SBM). Only known and trusted websites, that can be verified as such can be accessed when in SBM. Can start with FI's but should be extendable to other trusted communities. To get on list, have to comply with special security requirements that allow the site to be reliably distinguished from Spoof sites; have to undergo a rigorous certification and compliance process. Goal is not to eliminate attacks, but to protect those who are willing to take proactive steps to avoid them. SBM is voluntary

- **Credentialing Strategy for Financial Institutions**
  We are working with a variety of organizations including FSSCC (Financial Services Sector Coordinating Council), Chicago FIRST, SIFMA (Securities Industry and Financial Markets Association), Treasury, and DHS to facilitate the development of an effective approach to implementing a standardized and widely accepted credentialing solution (e.g. FRAC – First Responder Authentication Credential). Also will examine applicability of FI Credentialing solution to other applications such as Safe Web Browsing

- **A2A Payments**
  Leverage existing bank products to provide P2P and keep DDA central to Customer Relationship. Make more user friendly, more consistent across products, more secure. Extend to new Channels; e.g. Mobile and integrate with value-added services tied to DDA. Improve security and simplify user interaction. Design to take advantageof new revenue opportunities (Advertising, Guarantees and loans, Cross border Remittance, Pre-paid debitand secured accounts)

- **Healthcare and Financial – Cross Industry Initiative on Identity Assurance**
  This initiative will introduce a framework for high assurance identity authentication for the healthcare and financial services industries. When utilized, the framework of operating policies, rules, and control practices will act as a catalyst to enable identity services across these industries. The project will also explore other topics for cross-industry collaboration, including data sharing and protection strategies, privacy, and regulatory compliance

- **Records Management and Prevention of Data Leakage**
  This project will study the issues and related requirements of timely classification, protection, storage, retrieval, and destruction of unstructured content. The requirements will be designed to satisfy electronic discovery requirements of financial regulations, and to minimize data leakage. The requirements will

be described in an overall enterprise architecture of standards, technologies and business processes that can greatly improve the effectiveness of records management solutions, while greatly reducing manpower required, and that can scale to meet the Industry needs.

Will also explore the relationships between record/unstructured information management and IAM/entitlements/digital rights mgt

- **Thoughts about Insider Threat – in exploration as a project**
  Some of the ideas being discussed with respect to an Insider Threat initiative include: Need for better compliance and audit management; Better controls and checks and balances; Stronger identity management, authorization and access controls; Better monitoring, forecasting and detecting an insider turned bad; More dynamic, adaptive access controls and entitlements; More effective screening and employee selection; Biometric measurements to help detect bad employees; Use of First Responder Authentication Credential Card (FRAC) within enterprise for physical and logical access; Benefits of Information sharing amongst FI's

Subscribe to:

FSTC Innovator—FSTC.org/innovator/subscribe.cfm

Please check our website at www.fstc.org. FSTC's 2008 Annual Conference program and registration information will be featured soon. In the meantime, if you are interested in sponsorship or exhibits, please contact Betsy Love at betsyl@truenorthintl.com.