Developing a Framework to Improve Critical Infrastructure Cybersecurity

Overview

The following comments are submitted by the **Trust Nexus** of Austin, TX in Response to the February 26, 2013 Request for Information Notice by the National Institute of Standards and Technology.

From an organizational perspective, there are two types of cybersecurity risks:

- "Systemic Risks" that involve the impairment of system capabilities (e.g., DDOS attacks)
- "Intrusion Risks" that involve bad actors gaining access to data, applications or control systems

We concur with the following statement from the RFI: "NIST believes the diversity of business and mission needs notwithstanding, there are core cybersecurity practices that can be identified and that will be applicable to a diversity of sectors and a spectrum of quickly evolving threats."

The most significant core practice that cuts across all sectors is authentication.

A simple, effective, low cost, easy to implement and cryptographically secure authentication process would greatly mitigate if not eliminate all "Intrusion Risks" and would make a significant impact in identifying "Systemic Risks".

The sad state of cybersecurity in the year 2013 is that most authentication is user name and password based; this is a state of failure open to compromises from phishing, hacking and personal indiscretion (e.g., writing down passwords). **While there are complex schemes for authentication that may be effective, they are not consumer friendly. While there are simple schemes that may be consumer friendly, they are not secure.**

The complex systems are not user friendly to even the most obsessively dedicated corporate users.

Existing Authentication Systems

In terms of simplicity, there are two authentication systems vying for attention: OpenID and Oauth.

There is a great deal of controversy surrounding OpenID brought on primarily by those who have over hyped the potential of OpenID.

Stefan Brands (an information technologist specializing in digital identity, security, and privacy) so clearly stated, "OpenID was designed as a lightweight solution for 'trivial' use cases in identity management: its primary goal is to enable Internet surfers to replace self-generated usernames and passwords by a single login credential, without needing more than their browser. Concretely, OpenID aims to enable individuals to post blog comments and log into social networking sites without having to remember multiple passwords. **Beyond this, OpenID is pretty much useless.** The reasons for this are many: OpenID is highly vulnerable to phishing and other attacks, creates insurmountable privacy problems, is not a trust system, suffers from usability problems, and makes it unappealing to become an

OpenID 'consumer.'" http://www.untrusted.ca/cache/openid.html

The original OpenID authentication protocol was developed in May 2005. While there are many organizations that offer OpenID, very few users have actually created OpenID accounts. The fact is that most users do not understand the concept of pasting a URL into a sign on field instead of using a user name and pass word.

The primary problem with OpenID from an identity management perspective is that there is no coherent security model for OpenID; because of this, OpenID is relegated to a Level 1 Assurance system ("Little or no confidence in the asserted identity's validity.") by the federal government. http://maarten.wegdam.name/2009/10/01/no-need-for-level-of-assurance-level-1-and-thus-openid-for-e-government/

No doubt there are many good technical people who have committed long hours to the development of OAuth, unfortunately they have all wasted their time.

While the original OAuth spec had the potential to develop into a sound security model, OAuth 2.0 dumped all cryptographic processes in favor of becoming an "institutional blueprint" for selling services.

These changes caused one of the lead OAuth contributors to resign from the working group: In July 2012, Eran Hammer resigned his role of lead author for the OAuth 2.0 project, withdrew from the IETF working group, and removed his name from the specification. Hammer pointed to a conflict between the web and enterprise cultures, citing the IETF as a community that is "all about enterprise use cases", that is "not capable of simple". What is now offered is a blueprint for an authorisation protocol, he says, and "that is the enterprise way", providing a "whole new frontier to sell consulting services and integration solutions". http://en.wikipedia.org/wiki/OAuth

In comparing OAuth 2.0 with 1.0, Hammer points out that it has become "more complex, less interoperable, less useful, more incomplete, and most importantly, less secure"... He explains how architectural changes for 2.0 unbound tokens from clients, removed all signatures and cryptography at a protocol level and added expiring tokens because tokens couldn't be revoked while complicating the processing of authorisation. Numerous items were left unspecified or unlimited in the specification because "as has been the nature of this working group, no issue is too small to get stuck on or leave open for each implementation to decide".

The fundamental flaw with OAuth 2.0 is that it is a, "Delegated Authorization protocol, and not an Authentication protocol."

In terms of complexity, authentication systems based on biometrics, "take the cake." Systems that attempt to create vast repositories of biometric information are simply be storing extremely long passwords that are available for compromise.

There are severe limitations in using bio-metric data over a network or in a physical location with no human monitoring. The most significant compromise is the "Jack Bauer" approach where the legendary CTU agent cuts out the eye of an terrorist and uses it to "fool" an iris scanner. Similarly,

school children in Australia were able to fool fingerprint readers (by using Gummy Bears).
http://www.zdnet.com/sweet-bypass-for-student-finger-scanner-1339306878/

Digital certificates for personal authentication also fall into the simple but not effective category. When a digital certificate is issued the user (or a malicious administrator or someone who can access the user's system) can simply "share" the cert with anyone.

Digital certificates for organizational authentication can be disastrous. Contrary to the proponents of PKI, a catastrophic security breach of the PKI, similar to the Comodo Security Breach, is always a possibility, especially if you travel to a hostile foreign country or if you are a citizen under an oppressive regime.
http://www.infoworld.com/t/authentication/weaknesses-in-ssl-certification-exposed-comodo-security-breach-593

While security tokens can be effective if they are not lost or stolen, they are not consumer friendly. Would anyone want to carry a physical security token for every application that required secure access?

Also, the RSA security breach exposed the limitations of security tokens.
http://www.huffingtonpost.co.uk/andrew-kemshall/the-rsa-security-breach-1_b_1344643.html

A "Change the World Technology"

The **Trust Nexus** is a technology startup located in Austin, TX. We have have solved one of the key problems in cybersecurity: **secure mobile identity**. Our technology will enable secure authentication to all types of information systems; this will eliminate hacking, eliminate phishing, eliminate identity theft and eliminate fraudulent financial transactions. We truly have a **change the world technology** for authentication that is simple, effective, low cost, easy to implement and cryptographically secure. Touch one button on your mobile device and you are securely signed onto your web application.

In the late Seventies and early Eighties computer names were maintained by using handcrafted HOSTS.TXT files. As networks became more interconnected this process became unmanageable. Everyone knew that something needed to be done. When the **Domain Name System** (DNS) was created everyone saw it as the obvious solution. Similarly, when the solution to cybersecurity authentication emerges, everyone will say, "**Of course, that is how it had to be.**"

The essence of our process is incredibly simple: Through **secure mobile identity**, we completely do away with user names and passwords (and all of their weaknesses). If a credential is provisioned to a user's mobile device in a **valid institutional process**, then when the user presents the credential (either in person or over the network) **the receiver can be certain** that either the credential and the user are valid or the user gave his/her mobile device and six digit HEX pin (1/16,777,216) to someone else.

While many of our cryptographic processes are similar to the processes used in Public Key Infrastructure (PKI), we avoid the bureaucratic inconveniences and lax security inherent in PKI. Under PKI, when a digital certificate is issued the user (or a malicious administrator or someone who can access the user's system) can simply "share" the cert with anyone. Under the **Trust Nexus** it is far

less likely that a user will share his/her mobile device and six digit HEX pin.
http://www.infosecisland.com/blogview/12891-Digital-Certificates-Only-Provide-the-Illusion-of-Security.html
https://www.eff.org/deeplinks/2011/10/how-secure-https-today

Also, under the **Trust Nexus** a catastrophic security breach of the PKI, similar to the Comodo Security Breach, would have no ill effects for users. Contrary to the proponents of PKI, a Comodo-like security breach is always a possibility, especially if you travel to a hostile foreign country or if you are a citizen under an oppressive regime.
http://www.infoworld.com/t/authentication/weaknesses-in-ssl-certification-exposed-comodo-security-breach-593

One of the most important aspects of our technology is that we secure identity while **protecting privacy**. Our technology provides a **100% privacy protection**. We do not store personal data, we store dual signed SHA-512 message digests of digital credentials. If an assault team were to attack one of our data centers they would not be able to gain personal data. We change the mind set of authenticating using personal data; instead, we verify institutional validations.

If you are a member of the *Secret Moose Lodge of Ottumwa, Iowa*, your identity credential can be validated under the **Trust Nexus** without any detailed information about you or your organization. We simply verify the institutional validation that was created when your credential was issued.

Another major advantage of our technology is that it is **ready to go today on all smart phones** whether or not they are NFC enabled.

Our technology goes beyond secure mobile identity. It may be difficult to believe, but as a small startup in Austin we have solved the **single sign on problem**. Our technology also enables a greatly simplified **identity federation process** .
http://en.wikipedia.org/wiki/Single_sign-on
http://www.thetrustnexus.com/mobile2/01a_mobile.htm

This is not theoretical; we have a functioning prototype and **everything works**.

Complete information on our technology can be found at our website: http://www.thetrustnexus.com

We have a definite plan.

Our ultimate goal is the creation of a worldwide identity infrastructure that will be managed by governments in a fashion similar to the management of the electric power grid. I know this sounds incredibly grandiose at this time; however, everyone who has looked at our technology has told us that if we can implement this on a political basis we truly have a **change the world technology**.

We are creating an infrastructure that will support **the rapid growth of mobile-Identity and mobile-Commerce**. In order to establish our infrastructure and generate good will, much of our technology will be licensed for a nominal fee or given away for free. Our technology and infrastructure services will be **free to governments worldwide** for driver's licenses and passports. Our technology and infrastructure services will be **free to financial institutions worldwide** for internal use.

Once the initial vetting is complete and we have formalized our presentation and source code, we will do an initial release to the members of the *Information Systems Security Association (ISSA ~* http://www.issa.org*)*, the world's leading organization for security professionals. Shortly thereafter we will start deploying real world implementations; **this will occur well before the end of this year**.

Rather than compete against the existing players in the identity management field, we intend to license our authentication technology to all players for a nominal fee; this will insure a rapid and widespread implementation.

The source code for both the **TNX Secure Infrastructure** and the **TNX Secure mobile app** will be made available. There is an essential reason why we are making the source code public: **A system is truly secure if the plans for the system are public, and the bad actors can still not break in.**

We are confident that our secure mobile identity technology is **the keystone for a worldwide identity infrastructure.**

Again, we would like to stress this is not theoretical; we have a functioning prototype and everything works.

Conclusion

Because of the simplicity of the technology, we believe that within six months the authentication technology of the **Trust Nexus** will become a "consensus standard and industry best practice".

We believe there are two statements in the NIST RFI that are contradictory:

"The Cybersecurity Framework will provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties."

...contradicts the line immediately following...

"To enable technical innovation and account for organizational differences, the Cybersecurity Framework will not prescribe particular technological solutions or specifications."

We believe that NIST should make specific recommendations. If the problems of cybersecurity are going to be solved, innovative approaches must be considered in detail.

If the goal of this framework is to provide general guidance, then there should be five metrics for authentication solutions: **simple, effective, low cost, easy to implement and cryptographically secure**.

If specific recommendations cannot be made, then the final draft of the framework should reference the ***NIST National Cybersecurity Center of Excellence*** for specific guidelines.
http://www.nist.gov/itl/csd/nccoe-022112.cfm

We applaud the dedication of the individual from NIST and other government agencies who are taking a lead in this endeavor. While the problems of cybersecurity may never be completely solved, great progress will be made. The “Framework to Improve Critical Infrastructure Cybersecurity” is an important first step.