Comment on the Draft National Strategy for Trusted Identities in Cyberspace (NSTIC)

Jonathan Mayer & Arvind Narayanan
Stanford University Department of Computer Science

July 26, 2010

I. Introduction

We applaud the White House and Department of Homeland Security for recognizing the immense security challenges posed by the proliferation of information technology, and for undertaking an unprecedented initiative to protect the nation online. We write to inform the NSTIC with an objective computer security perspective, and 1) clarify which cybersecurity challenges the NSTIC could mitigate, 2) detail the various security systems within the scope of the NSTIC, as we interpret the draft proposal, and 3) call attention to technical challenges in implementing the proposed security systems.

II. Problems Alleviated by the NSTIC

When approaching a computer security problem, researchers often begin with a "threat model" analysis in which they rigorously reason backwards from a negative outcome to a tenable security solution. Applying the threat model process shows how the NSTIC's proposed comprehensive identity management has varying effectiveness in resolving high priority cybersecurity vulnerabilities.

The draft NSTIC emphasizes the threats of hacking to do harm ("intrusions against the Nation's critical infrastructure," p. 4), hacking for espionage ("data theft," p. 4), and malware ("compromise of computer systems," p. 5). These security vulnerabilities stem from two underlying traits of information technology. First, computer software is riddled with exploitable bugs.[1] And second, large-scale computer networks inherently provide anonymity to a sophisticated user in a manner identity management cannot combat.[2] The recent online break-ins at Google and other leading technology companies are illustrative; attackers exploited software

The authors thank John Mitchell, Seth Schoen, and Lee Tien for their insightful comments.

[1] S. Bellovin. Comments on the National Strategy for Trusted Identities in Cyberspace. SMBlog. July 11, 2010. <http://www.cs.columbia.edu/~smb/blog/2010-07/2010-07-11.html>.
[2] J. Mayer. There's Anonymity on the Internet. Get Over It. Freedom to Tinker, Princeton University Center for Information Technology Policy. Oct. 27, 2009. <http://www.freedom-to-tinker.com/blog/jrmayer/there's-anonymity-internet-get-over-it>.

vulnerabilities to gain access[3] and redirected their network traffic to remain anonymous.[4] Comprehensive identity management like the NSTIC advocates would not defeat such intrusions.

Another focus of the NSTIC appears to be phishing ("[s]poofed websites," p. 1). Identity management certainly aids in ensuring a website is authentic, and while the SSL protocol has reliably provided a cryptographic basis for website authentication for over a decade,[5] substantial room for improvement remains in user interface design.[6] Identity management could also aid in combating "social phishing," in which a malicious party impersonates a friend via email or several other non-web-based messaging protocols.

The draft NSTIC attaches particular priority to the growing problem of identity theft (p. 5), which is frequently accomplished by physical means: personal information is most often taken either by a personal acquaintance, during a business transaction, or by theft.[7] A comprehensive identity management system could ensure that even if an identity thief steals personal information, they would lack the necessary credentials for fraudulent transactions. For example, if banks were to require a digital credential to open a new account, a would-be identity thief in possession of an individual's driver's license and social security number could not so readily exploit that information.

A final security problem implicated by the NSTIC is guaranteeing an attribute, such as age or nationality. An identity management system could certainly fulfill this task.

In sum, the NSTIC could in principle prove beneficial for phishing, physical identity theft, and attribute guarantees, though we detail several implementation concerns in Section IV. The NSTIC does not remedy hacking, espionage, and malware.

III. Technical Scope of the NSTIC

To clarify discussion of the NSTIC's relative merits, in this section we attempt to provide

[3] K. Zetter. Google Hack Attack Was Ultra Sophisticated, New Details Show. Threat Level, Wired. Jan. 14, 2010. <http://www.wired.com/threatlevel/2010/01/operation-aurora/>.
[4] J. Markoff and D. Barboza. 2 China Schools Said to Be Tied to Online Attacks. New York Times. Feb. 18, 2010. <http://www.nytimes.com/2010/02/19/technology/19china.html>.
[5] A. O. Freier et al. The SSL Protocol Version 3.0. IETF Internet-Draft. Nov. 18, 1996. <http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>.
[6] S. Schecter et al. The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies. 2007 IEEE Symposium on Security and Privacy. <http://www.usablesecurity.org/emperor/emperor.pdf>.
[7] 2006 Identity Theft Survey Report. Federal Trade Commission. <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

a non-exhaustive list of the computer security systems that, in our reading, the draft NSTIC proposes developing. We additionally provide the current implementation status of each system.

Choice of ID Providers (pp. 8-9)

Proposal: A user will be able to select an identity provider and use it to authenticate for a variety of online services.

Current Status: A number of open identity standards are in use, including OpenID,[8] SAML,[9] and Windows CardSpace.[10] Proprietary authentication systems include Facebook Connect[11] and Windows Live ID.[12]

Linking Online ID to Real-World ID (p. 13)

Proposal: Trusted identity providers will check a user's real-world credentials, then assert the user's online identity matches her real-world identity.

Current Status: A number of firms link online identity to real-world identity, ranging from financial institutions that require an in-person visit to create an account to video game companies that rely on verified credit card information.[13] Interoperable payment services, such as PayPal and Google Checkout, link real-world financial credentials to online identity. There is, however, no widely used, interoperable, strong-assurance online identity system linked to real-world identity.

Public Key Infrastructure (PKI) (p. 15)

Proposal: A nationwide PKI will enable user authentication.

Current Status: Federal and private PKI's already exist, though their application is largely constrained to SSL. Adoption of products that enable end-users to authenticate themselves has

[8] OpenID Authentication 2.0 - Final. OpenID Foundation. <http://openid.net/specs/openid-authentication-2_0.html>.
[9] SAML V2.0 Executive Overview. OASIS. <http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>.
[10] D. Chappell. Introducing Windows CardSpace. MSDN. Apr. 2006. <http://msdn.microsoft.com/en-us/library/aa480189.aspx>.
[11] D. Morin. Announcing Facebook Connect. Developer Blog, Facebook. May 9, 2009. <http://developers.facebook.com/blog/post/108>.
[12] Introduction to Windows Live ID. <http://msdn.microsoft.com/en-us/library/bb288408.aspx>.
[13] E. Galperin. New Blizzard Forum Policy Will Require Posters to Use Real Names. Deeplinks Blog, Electronic Frontier Foundation. July 8, 2010. <http://www.eff.org/deeplinks/2010/07/new-blizzard-forum-policy-will-require-posters-use>.

been minimal.

Attribute Authentication (pp. 13, 18)

Proposal: A user will have granular control over his credentials and can choose to authenticate an arbitrary subset of attributes.

Current Status: Some OpenID identity providers enable coarse control over which personal information to authenticate.

Anonymous Credentials (pp. 10, 17-18)

Proposal: A user will be able to authenticate pseudonymously.

Current Status: Research on the theoretical and practical feasibility of such systems is ongoing.[14]

Credential Management (pp. 10, 18)

Proposal: A user will be able to intuitively manage her credentials and authenticate without any detailed knowledge of computer security. Proposed hardware systems include smart cards and trusted computing hardware.

Current Status: Beyond web browser display of SSL certificates and password storage, few software credential management systems are in common usage. A number of smart card and trusted computing hardware standards are in widespread use.

Identity Interoperability (pp. 8-9)

Proposal: A user's chosen identity provider will be interoperable with every site that follows the NSTIC.

Current Status: Several interoperable identity standards are in active use and under continuing development, as noted above.

IV. Challenges in Implementing the NSTIC

[14] For example: A. Dey and S. Weis. PseudoID: Enhancing Privacy for Federated Login. Draft in Submission. Feb. 2010. <http://www.pseudoid.net/static/pseudoid.pdf>. J. Camenish and A. Lysyanskaya. An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation. In Proceedings of Advances in Cryptology - Eurocrypt 2001. <http://groups.csail.mit.edu/cis/pubs/lysyanskaya/cl01a.pdf>.

There are a number of technical challenges that follow from implementing the NSTIC, spanning system design, hardware, software, and usability. This section highlights several of the most salient problems.

Centralization: Concentrating identity management creates single points of failure and vulnerability, and provides tremendous incentive for a malicious party to steal a user's digital identity.[15]

System Security: An identity management scheme can only be as secure as the underlying systems it runs on. The triviality of compromising personal computers poses a serious threat to any comprehensive identity management system.[16]

Revocation: A user's digital credentials may be lost or stolen. The NSTIC must detail how to revoke a user's valid-on-its-face credential and issue a new credential.

Forward Compatibility: Researchers frequently discover weaknesses in security systems. Every component of the NSTIC must accommodate extensibility and forward compatibility.

Identity Provider Management and Governance: Identity providers may go out of business, be compromised, or engage in malicious activity. The NSTIC must account for issues with identity providers.

---

[15] Comments on Draft of National Strategy for Trusted Identities in Cyberspace. U.S. Public Policy Council of the Association for Computing Machinery. July 19, 2010. <http://usacm.acm.org/PDF/USACM_Secure_Identity_Comments_final.pdf> ("[T]he relatively centralized maintenance of identities and associated attributes introduces new risks that undercut potential benefits."). S. Bellovin. Comments on the National Strategy for Trusted Identities in Cyberspace. SMBlog. July 11, 2010. <http://www.cs.columbia.edu/~smb/blog/2010-07/2010-07-11.html> ("Of course, by centralizing authentication you've created a new, critical resource: the authentication manager. What better target for a malicious hacker....").

[16] Comments on Draft of National Strategy for Trusted Identities in Cyberspace. U.S. Public Policy Council of the Association for Computing Machinery. July 19, 2010. <http://usacm.acm.org/PDF/USACM_Secure_Identity_Comments_final.pdf> ("Strong identification will not compensate for information technology that is poorly designed, configured, and/or operated. Indeed, vulnerabilities in the underlying technology will threaten the integrity of such a scheme."). S. Bellovin. Comments on the National Strategy for Trusted Identities in Cyberspace. SMBlog. July 11, 2010. <http://www.cs.columbia.edu/~smb/blog/2010-07/2010-07-11.html> ("All the authentication in the world won't stop a bad guy who goes around the authentication system, either by finding bugs exploitable before authentication is performed, finding bugs in the authentication system itself, or by hijacking your system and abusing the authenticated connection set up by the legitimate user. All of these attacks have been known for years.").

Usability: The usability of authentication is a long-standing problem. SSL, for example, theoretically solves website spoofing – but users repeatedly fall prey to web phishing because they have difficulty understanding browser security indicators.[17] PGP likewise provides a functional paradigm for email security – but deficiencies in user interface and key sharing hinder adoption.[18]

Unwanted Linkage: Recent research has shown the ease of accomplishing unwanted linkage of credentials on a large scale.[19] Online behavioral tracking[20] is a particular concern.

Anonymous Credentials: Provably anonymous credentials are a subject of ongoing cryptographic research;[21] the extent to which they can be implemented reliably and at scale is unknown. A weaker form of anonymity that trusts an identity provider to not reveal a user's true identity[22] is technically feasible, but raises substantial privacy concerns.

Smart Cards: There have been many high profile breaches of smart card systems, including Boston's public transportation system,[23] San Francisco's parking meters,[24] and most recently the European payment card standard.[25]

---

[17] S. Schecter et al. The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies. 2007 IEEE Symposium on Security and Privacy. <http://www.usablesecurity.org/emperor/emperor.pdf>.
[18] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th Conference on USENIX Security Symposium. 1999. <http://gaudior.net/alma/johnny.pdf>.
[19] D. Irani et al. Large Online Social Footprints - An Emerging Threat. In Proceedings of the International Conference on Computational Science and Engineering. 2009. <http://www.cs.uga.edu/~kangli/src/SecureCom09.pdf>.
[20] R. Jeschke. Privacy in Online Behavioral Tracking and Targeting - It's Time to Protect Consumers. Deeplinks Blog, Electronic Frontier Foundation. Sept. 1, 2009. <http://www.eff.org/deeplinks/2009/08/behavioral-tracking>.
[21] For example: A. Dey and S. Weis. PseudoID: Enhancing Privacy for Federated Login. Draft in Submission. Feb. 2010. <http://www.pseudoid.net/static/pseudoid.pdf>. J. Camenish and A. Lysyanskaya. An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation. In Proceedings of Advances in Cryptology - Eurocrypt 2001. <http://groups.csail.mit.edu/cis/pubs/lysyanskaya/cl01a.pdf>.
[22] L. Tien and S. Schoen. Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns. Deeplinks Blog, Electronic Frontier Foundation. July 20, 2010. <http://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan>.
[23] R. Ryan et al. Anatomy of a Subway Hack. <http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf>.
[24] J. Grand et al. "Smart" Parking Meter Implementations, Globalism, and You. Black Hat USA 2009. <http://www.grandideastudio.com/wp-content/uploads/smart-parking-meter-slides.pdf>.
[25] S. J. Murdoch et al. Chip and PIN is Broken. 2010 IEEE Symposium on Security and Privacy. <http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf>.

Trusted Computing: Trusted computing hardware has repeatedly been compromised or bypassed, especially where substantial incentive exists, such as content protection. An implementation of the Trusted Platform Module (TPM), advertised as "unhackable," was compromised just this year.[26]

V. Conclusion

We recognize this comment raises a number of issues without providing solutions; we intend the piece will initiate a conversation between computer security researchers and the NSTIC team. We look forward to collaborating on this important policy initiative.

[26] J. Robertson. Security Chip that Does Encryption in PC's Hacked. USA Today. Feb. 8, 2010. <http://www.usatoday.com/tech/news/computersecurity/2010-02-08-security-chip-pc-hacked_N.htm>.