Editor: Barry Leiba • barryleiba@computer.org

The National Strategy for Trusted Identities in Cyberspace

Enhancing Online Choice, Efficiency, Security, and Privacy through Standards

Jeremy A. Grant • *US National Institute of Standards and Technology*

Dear Password,

It's time for you to retire. You've served us well, but the reality is that you're woefully outdated and fundamentally insecure. Moreover, our reliance on you is making it difficult to move some very interesting and valuable types of transactions online. It's time to replace you with a new set of trusted authentication technologies.

It's not that you were never helpful: when we first went online some 20 years ago, you were downright essential. But our old clunky desktops with green screens have been replaced by ultra-light, high-powered laptops and mobile devices. Dial-up has been superseded with broadband, both wired and wireless. Yet while almost every aspect of our online experiences has been upgraded, we're still authenticating to these systems — and managing our online identities — via the same username and password technology that we used when we were dialing into Bulletin Board Systems over 1200-baud modems.

Actually, in some ways, we've regressed. As attacks against password-based systems have increased, organizations have required that you, password, become more and more complicated — to the point that you're nearly unusable. The complexities password requirements impose on most individuals to craft 20 to 30 passwords with letters, numbers, symbols, and such have prompted most individuals to give up — and then use the same one or two passwords everywhere they go.

Moreover, our continued dependence on you as our primary means of authentication has left us woefully vulnerable and insecure. Key-logging malware, phishing attacks, man-in-the-middle attacks, and brute force attacks, among others, have proven you to be an easily defeated technology. Our continued reliance on you has created a soft underbelly on the Internet that makes not just government but also ordinary citizens and businesses vulnerable to an increasing array of attacks.

So long, farewell, Auf wiedersehen, adieu. We need better authentication technologies to replace you.

Alternatives Exist — and Are Needed More than Ever

The US Department of Defense (DoD) learned just how commonly used password-centric attacks were several years ago when it mandated replacing passwords with the cryptographic capabilities of the Common Access Card (CAC) for all log-ons to DoD computers and networks. The results were stunning. The DoD found that its network intrusions fell nearly 46 percent overnight, as all of the stolen and spoofed identities attackers were using to access its systems suddenly became useless. To be clear, this was no silver bullet: the DoD still had the other 54 percent of breaches to contend with. And it's no secret that the bad guys moved on to other methods, one reason attacks on DoD networks have grown sharply since then.

Regardless, as government and the private sector focus on shutting down the most commonly exploited holes in our systems and upping the ante against hackers and criminals, you would think that the rest of the country

Published by the IEEE Computer Society 1089-7801/11/$26.00 © 2011 IEEE

Editor's Introduction

In the last issue, Lucy Lynch, of the Internet Society, gave an overview of the identity management landscape, telling us what some of the problems are and how some organizations are looking at resolving them. In this issue, Jeremy Grant, of the US National Institute of Standards and Technology, discusses a particular aspect of identity management – how we authenticate – and introduces us to the US's National Strategy for Trusted Identities in Cyberspace (NSTIC), which aims to replace the pile of passwords we currently use with a more robust and secure identity ecosystem.

—Barry Leiba

would have adopted a stronger identification technology such as CAC. Instead, most of us are still trying to manage 20 to 30 passwords, each with more characters than can practically be remembered. More often, we're using the same one or two passwords wherever we go online.

This is particularly true in our personal lives, where a side effect of recent data breaches – such as the one Sony Playstation suffered earlier this year – has been the theft of myriad passwords offering direct access to individuals' online email accounts from providers such as Google, Microsoft, and Yahoo. Consider that the majority of Americans have free email accounts from one or more of these providers, and use those email addresses as their identifiers to log in to sites with which they do business online. This might not be surprising, but what is surprising is that anecdotal evidence shows a significant proportion of the population also uses the exact same password to log in to business sites as they use to log in to their email.

For hackers, this password reuse makes firms that store millions of emails and passwords tied to their customers a treasure trove of information. Consider the Sony Playstation breach. Thousands of email accounts were associated with Sony customers – and once the criminals had stolen customers' Playstation passwords, they could see whether those passwords would also work with the associated email accounts.

Where there is a match in these cases, they now have, at minimum, a live and valid email address they can use to send out spam to everyone in your contact list – and others. Even worse, they can use the fact that you're likely trusted by those on your address list to stage phishing attacks against your contacts. With a bit more patience, the adversaries can go through your messages, learn more about you – where you live, what you've bought, where you bank, who your friends and family are – and use that information to craft a more sophisticated attack that can really yield some serious returns.

Our reliance on weak password technology has been a growing attack vector that threatens to erode the confidence we have in the online world. It's estimated that 8.1 million US citizens were victims of identity theft or fraud last year, at a cost of some $37 billion (see www.javelinstrategy.com/news/1170/92/1).

The problem is only getting worse. Beyond the Sony attack this year, we've seen multiple high-profile attacks on systems that exploited password insecurity. This past spring, Google announced that it had disrupted a spear-phishing attack that focused on getting the email passwords of accounts held by, among others, senior US government officials. These attacks – in which targeted individuals received emails that appeared to be from colleagues and friends – prompted those individuals to enter their passwords at a spoofed Gmail login site. Once the perpetrators had the passwords in hand, they could monitor all activity in those accounts and covertly change the "mail forwarding" settings to ensure that they received new messages even if the victims later changed their passwords.

In June, we saw the hackers at LulzSec publish 62,000 email passwords culled from sites they'd hacked – inviting others to try out the combinations and wreak havoc where they could (see http://gizmodo.com/5812530/lulzsec-leaks-62000-emailpassword-combo-internet-goodie-bag). That same month, a Maine court ruled in the case of *Patco Construction Company vs. People's United Bank* that the bank wasn't liable for hundreds of thousands of dollars in losses after a criminal used a man-in-the-middle attack to compromise the bank's password-based authentication system and steal money from Patco's account (see www.med.uscourts.gov/.../jhr_05272011_2-09cv503_patco_v_ocean_bank.pdf). Small businesses such as Patco aren't subject to the same rules that protect individual consumers in attacks like this, which is one reason why cybercriminals have increasingly targeted such firms' online bank accounts. There have been other cases around this topic as well; so long as they continue, it will be bad for both businesses and financial institutions.

With passwords as our primary security tool, healthcare providers won't put many electronic health records online. Government agencies aren't comfortable moving high-value transactions out of brick-and-mortar locations and onto the Internet. And individuals and business are vulnerable.

Removing Barriers to Trusted Authentication

Amidst these problems with passwords, the US government is making

an effort to change things. President Barack Obama signed the National Strategy for Trusted Identities in Cyberspace (NSTIC) this past April; it was launched at an event hosted by the US Chamber of Commerce.

The strategy focuses on working in partnership with the private sector to remove the barriers that have precluded most of the country from easily adopting online identification technologies that are secure and trusted and looks to technologies such as those the DoD has used to securely manage identities.

Despite the DoD success story, however, strong authentication technologies have had a hard time gaining wider adoption owing to several issues. To date, high-assurance credentials have come with higher costs and burdens that have made them impractical for many organizations and the public sector at large.

For starters, despite its security benefits, many people find higher assurance credentials more difficult to use. Moreover, most credentials deployed have been good only for a single application; they aren't interoperable. This makes them expensive, and means that if someone requires strong credentials for numerous applications, they'll need to manage (and often carry) a number of credentials.

In theory, this is an area where Metcalfe's law should apply — the more applications people can use interoperably with their credentials, the more valuable having one becomes — but barriers exist, such as concerns about privacy and a lack of solid interoperability standards or operating rules to settle economic tussles that might arise on thorny issues such as liability. To date, the market has struggled to overcome these obstacles.

Four Guiding Principles for the Identity Ecosystem

NSTIC was a direct action item in President Obama's Cyberspace Policy Review from 2009, which called for the creation of "a cybersecurity-focused identity management vision and strategy ... that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation."

It's essential that identity solutions offer us a real improvement in our online security over the password-based solutions we see today.

The strategy lays out a path for creating an *identity ecosystem*, "an online environment where individuals and organizations will be able to trust each other because they follow agreed-upon standards to obtain and authenticate their digital identities."

NSTIC has four guiding principles. Identity solutions will be

- privacy-enhancing and voluntary;
- secure and resilient;
- interoperable; and
- cost-effective and easy to use.

So what does this mean, exactly?

Privacy-Enhancing and Voluntary

The second part of this principle is quite simple: participation in the identity ecosystem will be entirely voluntary. There will be no mandate; individuals won't be compelled to get a more secure credential — the choice will be theirs. Of course, if the ecosystem is designed right, the benefits of having one will be compelling.

The privacy-enhancing part of the principle deserves more attention. A key focus of NSTIC is to craft solutions that not only offer individuals more security and convenience but also more control over their personal information — empowering them to have more say over when and where this information is disclosed. Another goal is to craft alternatives that will allow both individuals and the parties with which they're doing business to have higher-assurance transactions without needing to exchange the gobs of information that we usually do when registering with a new business online.

New privacy-enhancing encryption technology that offers both improved security (especially compared with passwords) and the ability to provide only certain attributes (rather than a complete dataset of personal information) is very appealing, and an area in which we want to encourage the development of new solutions. Imagine a world in which, rather than having to provide a page of personal information when you go to a new e-commerce site, you instead can rely on your identity provider to — at your direction — provide that site with only the specific data necessary to complete the transaction. It's an approach rooted in technology that could fundamentally change how we disclose data about ourselves and empower individuals to better control their personal information.

Beyond this new technology, the NSTIC embraces eight key Fair Information Practice Principles (FIPPs) as a foundational set of privacy protections to ensure that the identity ecosystem enhances, rather than threatens, individual privacy. It also protects

anonymity and pseudonymity — there are times when nobody cares if you're a dog on the Internet, and the US government has no interest in changing that.

Secure and Resilient

It's essential that identity solutions offer us a real and material improvement in our online security over the password-based solutions we see today, and that they create a new foundation for increased levels of trust online.

Identity solutions will provide secure and reliable methods of electronic authentication. Authentication credentials are secure when they are

- issued based on sound criteria for verifying the identity of individuals and devices;
- resistant to theft, tampering, counterfeiting, and exploitation; and
- issued only by providers who fulfill the necessary requirements.

In addition, the ability to support robust forensic capabilities will maximize recovery efforts, enable enhancements to protect against evolving threats, and permit attribution, when appropriate, to ensure that criminals are held accountable for their activities.

Interoperable

Interoperability allows individuals the benefit of using their secure credentials at all sites and ensures that businesses and other relying parties can accept and rely on any NSTIC-certified credential.

Interoperability encourages service providers to accept a variety of credential and identity media, similar to how ATMs accept credit and debit cards from different banks. It also supports identity portability: it lets individuals use a variety of credentials in asserting their digital identities to service providers. Finally, the interoperability of identity solutions envisioned in this strategy will let people easily switch providers, thus harnessing market incentives to meet people's expectations.

This guiding principle recognizes two interoperability ideals within the identity ecosystem:

- standardized, reliable credentials and identity media will be in widespread use in both the public and private sectors; and
- individuals, devices, or IT systems should be able to present valid and appropriate credentials that any qualified relying party can accept and verify as proof of identity and attributes.

To achieve these ideals, identity solutions should be scalable across multiple communities, spanning traditional geographic borders. Interoperable identity solutions will let organizations accept and trust external users authenticated via third party. Identity solutions achieve scalability when all participants in the various identity federations agree on a common set of standards, requirements, and accountability mechanisms for securely exchanging digital identity information, resulting in authentication across identity federations.

Identity solutions will achieve at least two types of interoperability: technical and policy-level. Technical interoperability (including semantic interoperability) enables different technologies to communicate and exchange data based on well-defined and testable interface standards. Policy-level interoperability lets organizations adopt common business policies and processes (such as liability, identity proofing, and vetting) related to the transmission, receipt, and acceptance of data between systems.

Many existing standards and standards organizations address these issues, and the identity ecosystem will encourage using existing, nonproprietary solutions. When new standards are needed, the ecosystem will emphasize nonproprietary, international, and industry-led standards.

In addition, identity solutions will be modular, letting service providers build sophisticated identity systems using smaller and simpler subsystems. This implementation philosophy will improve the flexibility, reliability, and reuse of these systems and allow for simplicity and efficiency in change management: service providers can add and remove components as the identity ecosystem evolves.

Only the private sector can build and operate the complete identity ecosystem, and NSTIC's final success depends on private-sector implementation.

Cost-Effective and Easy to Use

NSTIC expressly recognizes that solutions that embrace the first three principles will fail to take hold if they aren't also cost-effective and easy to use. Indeed, these are two issues that have vexed technologists in the security sector for years, with enterprise adoption of strong authentication technologies often stymied by cost and usability issues.

The good news is that a wide range of new solutions are coming to

market — many leveraging mobile devices — that are today breaking through these barriers. The pace of innovation in the sector has picked up tremendously in the past two years. NSTIC looks to take advantage of this and help provide a foundation where the marketplace of solutions can thrive.

The Way Forward

Although the government took the lead in crafting the strategy, NSTIC specifically looks to the private sector to lead its creation and implementation. Only the private sector can build and operate the complete identity ecosystem, and NSTIC's final success depends on private-sector leadership and implementation.

The government keenly understands that we don't have all the answers and that it would be silly to try to prescribe them to industry and other stakeholders. We firmly believe that the private sector is in the best position to identify which barriers must be overcome and drive the technologies and solutions that address them.

What the government does look to do here is provide support. This isn't a traditional government program in which an agency is looking to architect and build something. We're asking the private sector to do that – we just want to help.

The White House has asked the US National Institute of Standards and Technology (NIST) to establish a National Program Office to lead NSTIC implementation. NIST — with its long history of working collaboratively with the private sector to develop standards and best practices for cybersecurity and identity management — is uniquely suited to work with the private sector to bring the nation's collective expertise to bear in implementing the strategy.

An early priority is to help develop a private-sector-led governance model (a steering group) that can successfully bring together stakeholders with diverse interests from across the country to develop policy and technical standards that will become the identity ecosystem framework. Getting this right will be tricky and essential, and is the focus of much of the government's efforts. This steering group is on pace to be established by the end of 2011.

Beyond governance, the government looks to work with the private sector to help

- facilitate and lead the development of interoperable standards;
- provide clarity on national policy issues that are essential to NSTIC's success, such as legal frameworks, rules around liability, and ways to ensure privacy protection; and
- lead adoption of NSTIC solutions to stimulate demand.

The government will also aim to stimulate identity ecosystem development by funding pilot programs. The White House has requested $17.5 million for NSTIC pilots in its fiscal year (FY) 2012 budget, and NSTIC will be looking to use that funding on a variety of innovative pilots that can jumpstart different elements of the strategy. In advance of the funding, the government is developing criteria for pilot selection and assessing potential pilot programs, so that we'll be ready to move aggressively when we enter FY12. We're very interested to hear ideas, and welcome your submissions through our website at www.nist.gov/nstic or nstic@nist.gov.

The Time Is Now

NSTIC is an ambitious strategy. Although it certainly won't be easy, several factors make achieving this vision feasible that weren't possible five years ago:

- Identity and authentication technology is better than it's ever been: between existing technologies' maturity and new technologies that leverage mobile devices, industry can deliver a wide array of reliable, easy-to-use solutions.
- The problems caused by password-based systems keep getting worse: many people now understand that we need a better solution, and individuals, businesses, and organizations all want something different.
- The market for identity solutions exists, but it's nascent: it needs a nudge toward interoperability and standardization; clarity on national policy and legal frameworks (for issues such as liability and privacy); and an early adopter to stimulate demand.

The government can meet these needs and can play a unique role in bringing together stakeholders across the country to collaborate on fulfilling the NSTIC vision "that individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Together, we can finally retire the humble password and create a better way to enhance trust online.

Acknowledgments

Certain commercial equipment, instruments, or materials are identified in this article to foster understanding. Such identification does not imply recommendation or endorsement by the US National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Jeremy A. Grant is senior executive advisor for identity management with the US National Institute of Standards and Technology. He has a BS with dual concentrations in biology and political science from the University of Michigan, Ann Arbor. Contact him at nstic@nist.gov.