Secure and Usable Enterprise Authentication: Lessons from the Field

Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong | National Institute of Standards and Technology

Surveys of US Defense and Commerce department employees show that using Personal Identity Verification and Common Access Cards for two-factor authentication results in improved usability and security.

Over the past 15 years, the US government has deployed millions of multifunction smart cards to its workforce with the goal of using the cards to grant both physical access to facilities and logical access to information systems. The deployment and use of these cards has been inconsistent across different government agencies. The Department of Defense (DoD), with its Common Access Card (CAC), recently announced that 98 percent of its information systems had been adapted to use the smart cards, thus providing these systems with strong two-factor user authentication. Other parts of the government are significantly behind the DoD, with logical authentication deployment rates ranging from 0 to 95 percent.[1]

Practical systems for multifactor authentication have been on the market for roughly 30 years, but it's only in the past few years that industry and academia have made a concerted effort to migrate users away from pure password systems. These groups can benefit from the US government's experience in deploying multifactor systems and by comparing the results of different deployment strategies.

In this article, we present the historical background that led to different deployment strategies within the US's defense and civilian executive branch agencies. We then present the results of two large-scale surveys of password usage in the DoD and the US Department of Commerce (DoC). Both surveys were completed before the US government's 2015 Cyber Sprint program, initiated by the Office of Management and Budget (OMB) to address that year's high-profile cyberintrusions.[2] The DoD aggressively implemented the CAC on many of its business systems, while DoC was less aggressive in its Personal Identity Verification (PIV) implementation. Thus, comparing these two departments' employee reports and attitudes about password usage provides insight into the effect of successfully deploying an easy-to-use, strong, two-factor authentication method in a large organization. Our sample includes responses from 28,481 DoD and 4,573 DoC employees.

Smart Card–Based Authentication

Smart card–based authentication relies on the card and a six- to eight-digit numeric PIN. Unlike passwords that must be changed routinely, PINs are generally not changed for the life of the card. Our survey found that it was rare for DoD users to mistype or forget their PINs—common failure modes with passwords. The security advantage comes from the use of public-key infrastructure (PKI)-based authentication, rather than

Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

a secret that is shared between the user and the system. The usability advantage comes from the fact that users need not memorize and type complex passwords.

The survey data shows that the inconsistent deployment of smart cards in the defense and civilian agencies resulted in significantly different IT experiences for users—not just for authentication in general but also for password-based systems. For example, DoD users had fewer complaints about their password-protected systems, even though the DoD had more stringent requirements for password complexity. We believe this result is explained largely by the fact that most DoD systems required CAC authentication, which we'll show is both easier to use and more secure. As a result, DoD employees had more mental reserves to cope with the difficulty of using the remaining systems secured with strong passwords.

> **Inconsistent deployment of smart cards across federal agencies resulted in significantly different IT experiences for users.**

The US government's two-factor approach significantly differs from many of the two-factor approaches adopted by other organizations. Outside the government, many organizations are deploying two-factor systems based on a strong password and a hardware credential such as a cell phone or a fob with a number that changes every minute. We'll discuss how the choice of a two-factor system affects both security and usability.

Equipping the US Government Workforce with Multifactor Authentication

The DoD has led the US government's smart card efforts since 1996, when the Army started testing a multiuse card in Hawaii. The Navy took over and expanded the program in 1998. In 1999, Congress allocated $30 million to implement a smart card program for the entire DoD, with the Navy as the lead agency.[3]

The DoD CAC is a credit card–sized device containing a cryptographic processor, magnetic stripe, linear and 2D bar codes, noncontact RFID technology (a proximity chip), and an identifying photo. The CAC is part of the DoD's PKI, with each chip card containing three private keys and corresponding certificates: one for email encryption, one for email signing, and one for attestation. According to the General Accounting Office, "by November 2002 DoD had issued approximately 1.4 million CACs to military and civilian personnel and had purchased card readers and middleware for about 1 million of its computers,"[4] and was on track to deploy the 4 million CACs it anticipated needing.

At the time the list price for a smart card reader ranged from $30 to $50, so the $30 million allocated by Congress clearly didn't cover the cost of CAC implementation. However, the funding did signal to the DoD the Congressional intent to make CAC deployment a government priority. The DoD created a Smart Card Senior Coordinating Group to develop and oversee CAC deployment. This group implemented the guidance from the DoD Chief Information Office, made DoD-wide implementation recommendations, and provided strategic direction. The group was chaired by a high-level government official appointed by the Secretary of the Navy and had representatives from throughout the DoD.[5]

Today, every active duty, reserve, and civilian DoD employee has a CAC. The CACs are the identity cards used for gaining access to DoD facilities, logging into DoD computers, and for email signatures and encryption. Logging in involves inserting the CAC into a reader and typing a PIN that is six to eight digits long. This unlocks the card's 2,048-bit RSA private key that is used for attestation, simultaneously identifying and authenticating the user. If the wrong PIN is typed three times in a row, the CAC locks and can be unlocked only if the user visits a service center. Thus, the CACs provide two-factor authentication, creating an authentication experience that is largely immune to social engineering and phishing. Although users can change their PINs, they rarely do in practice. CACs also include digitized fingerprints, a biometric that might be used in the future to provide three-factor access to some systems.

The CAC was just one of 62 smart card pilot programs in the 1990s within the US government. These programs were so successful that in August 2004, President George W. Bush signed Homeland Security Presidential Directive 12 (HSPD-12), which required the government to create a "Government-wide standard for secure and reliable forms of identification" that would be used by both federal employees and contractors to gain "physical access to Federally controlled facilities and logical access to Federally controlled information systems."[6]

As part of implementing HSPD-12, the National Institute of Standards and Technology (NIST) developed FIPS 201 (Federal Information Processing Standard Publication 201), PIV of Federal Employees and Contractors. FIPS 201 established the physical, electronic, and logical aspects of PIV cards. PIV cards resemble CACs in that they have an identity photograph on the front with the employee's name, the issuing agency, and an expiration date and are also ISO/IEC 7816 compatible. However, PIV cards lack the CAC's two bar codes, and the certificates are rooted in a civilian PKI, for example, a commercial PKI provider certified under the General Services Administration's Shared Service Provider program.

Despite the similarities between the CAC and the PIV card, civilian agencies had significant difficulty deploying the cards and adapting IT systems to use PKI for authentication. Unlike the DoD, Congress created no specific budget line item to fund the transition to the PIV. Instead, the OMB stated that federal agencies were expected to use their existing funding for background investigations, access control, and identification credential activities to support PIV deployment, and that any necessary additional funds should be acquired "through the normal federal budget process."[7] Indeed, because FIPS 201 was a federal information standard pertaining to computer security, OMB policies required that agencies use their existing IT funding to update their legacy systems to meet new security requirements before spending funds on new systems (including development, modernization, or enhancement).

Today, more than 5.4 million DoD and civilian employees and contractors—96 percent of the eligible workforce—have identity-proving smart cards loaded with ITU-T X.509v3 certificates that are rooted in the federal government's PKI.[8] But the lack of dedicated funding for upgrading systems to utilize the PIV card had lasting consequences. Although PIV cards replaced other cards for entering federal facilities, agencies lagged in using the cards for logical access. Many agencies didn't equip workstations with smart card readers, nor did they modify back-end systems so that the cards could be used for logical access to federal information systems. For example, a 2008 audit of the US Agency for International Development (USAID) found that the agency's deployment of PIV cards had been significantly hampered by the lack of funding.[9] A 2014 audit of the Internal Revenue Service (IRS) likewise found that the tax-collecting agency's ability to utilize PIV cards to authenticate access to IRS networks and information systems was hampered by the lack of funding.[10]

The OMB's February 2015 Annual Report to Congress found that although some agencies used strong authentication for logical access 95 percent of the time in 2014, a handful of agencies didn't use strong authentication at all.[11] The OMB stated that 52 percent of the cybersecurity incidents that federal civilian agencies experienced could have been prevented by the strong authentication provided by the PIV cards. OMB called this figure "troublingly high," especially considering that the civilian agencies were using strong authentication for just 41 percent of their computer accounts—"well below the 75 percent target."[11]

Four months after OMB released its report, the US Office of Personnel Management (OPM) discovered that it had been the victim of two massive cybersecurity incidents in which attackers used stolen passwords to acquire sensitive information belonging to millions of federal employees. Following the OPM hack, the OMB ordered a Cyber Sprint, giving agencies 30 days to improve their system's security. A key focus area was strong authentication for privileged administrator accounts.

The Authentication Conundrum

Authentication has been a major theme in usable security research for nearly two decades.[12] Most of this research has focused on passwords and similar authentication schemes based entirely on a shared secret between the user and the computer system. The inherent usability problem with password-based systems is that passwords force their users into a tradeoff between usability and security. Passwords must be memorable enough that they don't need to be written down; easy enough to type that they can be reliably entered quickly; and long and strong enough that they can't be guessed, either in a targeted attack against a single individual or in a mass attack against an entire user base.

Passwords have also created implementation problems for system engineers for more than 40 years.[13] The earliest systems (as well as some current websites) stored passwords in plain text, forcing all users to change their passwords if the system administrator's account was compromised. Password hashing was supposed to cure this problem, but dictionaries of popular passwords, faster computers, and "rainbow tables" of precomputed hashes eliminated many of the protections of hashed passwords in the event that a system password file was compromised.

Passwords pose other security risks. Because many people use the same password on different systems, a compromised password has considerable value. Thus, malware that steals a password (either on the user's computer or on the remote system) might grant access to multiple unrelated systems. The same is true of passwords stolen through a phishing attack. Other than prevention of the compromise in the first place, the only way to minimize the risk of compromised passwords is to require that users change their passwords regularly—further decreasing usability. Passwords need to be changed regularly to guard against unknown compromise, but the act of changing passwords further contributes to users' cognitive burden. As a result, the past two decades have also seen significant efforts to replace passwords with some other authentication mechanism,[14] or at least to supplement them with a second factor.

Certificate-based smart cards that use PKI offer a usable two-factor alternative to passwords. The smart card contains a miniature cryptographic processor and storage for both private keys and third-party certificates. To authenticate, the user connects to a relying system and initiates an authentication request. The relying system can be a local computer, a local application, a remote website, or an application running on a remote system. The user's local computer asks the user to insert the smart card and enter a PIN, a password that typically contains six to eight digits. From the user's point of view, that's the entire process. But behind the scenes, strong cryptography is at work:

> **The Common Access Card provides two-factor authentication that's largely immune to social engineering and phishing.**

- When the authentication session is initiated, the relying system provides a challenge (a nonce) to the user's computer. It's this challenge that causes the user's computer to prompt for the PIN.
- After the user types the PIN, both the challenge and the PIN are provided to the smart card.
- If the PIN is correct, the smart card unlocks the card's private key and uses it to sign the challenge, which is then returned, along with a copy of the card's attestation certificate, to the relying system. The relying system uses the certificate to verify the signature. If the verification is successful, the relying system then verifies that the certificate is signed by a trusted certificate authority (CA) and is therefore trustworthy.
- If the PIN is entered incorrectly more than three times in a row, the card is locked and can't be used until an administrator either unlocks or reprograms it—something that's typically done in person after verifying the card holder's identity.

When a person authenticates with a smart card, the system receives cryptographic assurance that the client can make effective use of the card's private key, which means that the client has the card and a valid PIN. Identity is established by the identifying information on the digital certificate accompanying the authentication transaction. In US government systems, each CAC or PIV card includes the user's legal name, an identification number (which is not the user's Social Security number), and a certificate serial number. If the card is lost, a replacement card will have the same name and an identifying number. Certificates are revoked when they are no longer used (for example, because the card has been lost or the certificate's owner has left the organization). Operational systems should verify that the certificate hasn't been revoked, either by checking a certificate revocation list or using the Online Certificate Status Protocol.

In summary, deployment includes the physical smart cards identifying individuals to ensure that the individuals issuing the cards are who they claim; end-user hardware that can read the smart cards; back-end systems adapted to perform cryptographic challenge–response authentication; and an identity management system that allows back-end systems to match the usernames in their databases with the identities presented by the smart cards.

The Surveys

One goal of the CAC and PIV deployments was to minimize or eliminate the use of authentication passwords within the federal government. Therefore, we thought that a survey of US federal government employees would be helpful and designed an online survey to collect data on the end users' password management and attitudes. In June 2010, this instrument was piloted in NIST, resulting in a two-step approach: lab management sent an email informing employees of the research study, after which the employees were sent the link in an email requesting their participation.

Department of Commerce

After the NIST pilot, we used the same two-step approach to distribute the survey instrument to nine other DoC bureaus. Ultimately, we worked with DoC bureaus to send the survey to each of the approximately 38,000 DoC employees between February and June 2011. The anonymous survey included 11 questions on login procedures for work-related accounts, seven questions on work-related passwords used frequently, six questions on work-related passwords used infrequently, and four questions on cybersecurity. We received 4,573 responses (a 12 percent response rate).

Department of Defense

Separately, we worked with the DoD's Defense Manpower Data Center (DMDC) to develop a survey with 11 questions on login procedures for work-related accounts, seven questions on work-related passwords used frequently, six questions on work-related passwords used infrequently, and 10 questions on cybersecurity. That survey was ultimately distributed to 74,962 individuals who were chosen from the DMDC Civilian Personnel Master File by single-stage, nonproportional stratified random sampling. About 0.2 percent of the sample was deemed ineligible because it included employees who weren't with the DoD as of 10 September 2012, the Web survey's first day. The survey ran through 19 October 2012, during which time respondents were sent six email reminders to encourage participation. Completed surveys were received from 28,481 eligible respondents. Surveys were considered completed if at least 50 percent of the questions were answered, and responses were weighted by sample representation using the industry-standard three-stage process, adjusting for selection probability, nonresponse, and known population values. The overall response rate, weighted for eligibility, was 41 percent.

Findings

We found that DoC employees had nine work accounts that required logging in with a password, with an average of five accounts requiring frequent access and four accounts occasional access. (In a previous meeting with DoC chief information officers, we learned that there was no significant deployment of logical PIV authentication in the DoC, so we didn't include questions about this on the DoC survey.)

Of the 28,481 DoD respondents, 97 percent used a CAC to log in to at least one work-related system. Roughly 33 percent of DoD employees used only the CAC for system access (that is, no other method of authentication to the system was used). However, 66 percent of DoD employees also used systems that they could access only with a PIN and 56 percent used systems requiring a "character string" password. Focusing on the systems that required only a password to access, we found that the DoD employees who used passwords had an average of three accounts that they accessed frequently with passwords, and two accounts that they accessed occasionally.

As these survey statistics show, both DoD and DoC employees must access multiple systems regularly. When a CAC or PIV card is used, the hardware token authenticates the user independently to each remote system, providing maximal assurance and usability. Users might need to retype their PIN from time to time, but the use of single sign-on—which allows employees to sign in once and have their identification and authentication sent by proxy from one system to another—can minimize the number of authentication actions required during the course of the day. Our survey found that single sign-on was far more prevalent in the DoD than DoC: 54 percent of DoD respondents reported that they used single sign-on 50 percent of the time or more, compared to just 25 percent of DoC respondents. At the other end of the spectrum, 27 percent of DoD respondents said that they never used single sign-on, compared to 53 percent of DoC respondents.

Despite CACs' prevalence, 65 percent of DoD respondents indicated that they used a work-related system that required a password for access. These respondents had to manage 5.1 ± 0.2 such passwords on average, ranging from 4.8 ± 0.2 for Army employees to 5.4 ± 0.3 for Air Force employees. Greater variance was seen between occupational groups: those in the "administrative" occupational group managed 5.6 ± 0.2 and "professional" employees managed 5.3 ± 0.2 passwords, while "blue collar" workers managed 4.3 ± 0.3 and "other white collar" workers managed 4.2 ± 1.0. The survey didn't collect information about the types of systems that were still requiring passwords, so we don't know whether they were legacy systems that hadn't been adapted for CAC use or systems operated by organizations outside the government.

Users traditionally cope with the need to manage multiple accounts by using the same password. The DoC survey found that 20 percent of respondents "always" used the same password for different accounts, 20 percent used the same password for "more than half of my accounts," and 19 percent used the same password for "about half of my accounts."

At the time of our survey, the DoD had stricter password policies than the DoC, typically requiring longer and more complex passwords. Nevertheless, 52 percent of DoD employees thought that their password length policy was "about right," compared to just 36 percent of DoC employees. On the other hand, 41 percent of DoD employees felt that the password length requirement was "too long," compared to 57 percent of DoC employees. There are many possible explanations for these differences. For example, DoD employees could have a security culture that justifies more stringent password requirements because of higher security threats. Our favored explanation is that DoD and DoC have similar compliance budgets[15] for long passwords, but DoD employees experience less authentication fatigue because they can use the CAC to authenticate to the majority of their business-critical day-to-day systems.

CAC authentication might be less stressful than password authentication, because CAC users only need to recall and type a six- to eight-digit PIN, rather than a strong password containing letters, numbers, and symbols. DoD users need never change their CAC's PIN, but passwords must be changed on a regular basis—typically every 90 days.

Smart card authentication requires additional hardware that is not always properly recognized by the host OS. Of the 91 percent of DoD employees who answered the question on problems experienced with the CAC, 35 percent said that they hadn't experienced any problems having their CAC recognized, 45 percent said that they had experienced these problems to a "small extent," 14 percent a "moderate extent," 4 percent a "large extent," and 1 percent a "very large extent," with a measuring error of ±1 percent. Typing the PIN on the CAC three times incorrectly results in the CAC being locked; this can occasionally happen as the result of repeated software failures. In the surveys, 64 percent of those responding said that they hadn't been locked out of their CAC, 29 percent said that they had experienced lockout to a "small extent," 5 percent a "moderate extent," 1 percent a "large extent," and 1 percent a "very large extent," with a measuring error of ±1 percent.

> **Defense Department users have fewer passwords to maintain, which results in less forgetting and better authentication outcomes.**

Another source of user frustration is when users forget their authentication secrets, be they PINs or passwords. In the surveys, 90 percent of DoD users reported having no authentication problems resulting from forgotten PINs, compared to 40 percent of DoC users. At the other end of the spectrum, 0.6 percent of DoD respondents reported having "very large" problems and a "large amount" of frustration from forgetting CAC PINs, compared to 3.3 percent of DoC employees.

Passwords have many obvious costs to organizations, including cybersecurity losses from stolen passwords and the cost of password resets when users forget their passwords. But passwords have another pervasive—though largely invisible—cost for organizations: password creation.

In our DoC survey, we asked respondents the average and longest times it took for them to create their frequently used passwords. The mean time that respondents reported was 6 minutes, while the mean maximum time was 20 minutes. Considerations that employees reported in creating their passwords were ease of remembering (81 percent), compliance with password requirements (58 percent), synchronization with other account passwords (46 percent), ease of entering/typing (38 percent), and strength (31 percent). Considering both frequently and occasionally used passwords, we found that the average DoC employee with nine passwords spent roughly 3.5 hours per year creating passwords for organizations that had 90-day password expiration policies—an estimated cost to DoC of $6 million each year.

DoD users have fewer passwords to maintain, which results in less forgetting and better authentication outcomes. Overall, CAC users have more positive attitudes toward and experience less frustration with the authentication process.

Two-Factor Security's Outlook

With increased society-wide attention to cybersecurity in recent years, awareness of the need to strengthen, supplement, or replace passwords is growing. Organizations have repeatedly increased password complexity requirements, both to protect against offline password attacks resulting from the theft of hashed password files[16] and as a signal that the organization is serious about cybersecurity.

Unfortunately, complex passwords protect against only a single kind of attack: an offline, brute-force attack against a stolen database of password hashes. Complex passwords don't provide additional security against online attacks, since accounts automatically lock after a few incorrect guesses. Strong passwords also don't protect passwords stolen via phishing, keyboard loggers, and malware—no amount of complexity can protect a password that is provided directly to the attacker. For this reason, some researchers have concluded that strong passwords provide little additional account security when accounts automatically lock after a few login attempts.[17]

In recognition of this, organizations are increasingly deploying two-factor security solutions, so that a password by itself is insufficient to gain access to a logical resource. Several online service providers have deployed systems that authenticate users with text messages sent to a trusted device or by having the user provide a code generated using an application enabled with a time-based one-time password algorithm. Users are challenged to provide the second factor the first time they connect to a website using a previously unseen browser. After the initial contact, the user can choose to "trust" the browser by having the remote website store a cookie. On subsequent contacts, the cookie becomes the second factor.

Although such two-factor systems improve security and allow some organizations to meet their obligations under regulations affecting the health and finance sectors, they don't provide the same level of security as smart card–based solutions employing PKI. Cookie-based two-factor solutions are susceptible to phishing and man-in-the-middle attacks: the user authenticates to the phishing website, which transfers authentication to the real website, stealing the authentication cookie in the process. Malware on the end user's computer can also steal authentication cookies.

A more significant concern regarding the trend of supplementing strong passwords with a second factor is that the second factor does nothing to improve the poor usability of strong passwords. Such passwords still need to be remembered, typed, and changed on a regular basis. In addition, these kinds of two-factor solutions don't provide for strengthened identification security. Whereas websites that rely on HSPD-12 credentials can trust the identity provided by a client certificate, websites that rely on strong passwords and a second factor must devise some other approach for identity proofing their users.

Smart card–based identification systems have significant advantages over other two-factor systems. For example, smart card systems inherently allow organizations to integrate physical and logical access, one of the original reasons for the CAC and PIV deployments. Cards can be supplemented with other technologies, such as bar codes or magnetic stripes, for compatibility with legacy systems. Smart cards also allow for offline operation, since CA keys and certificate revocation lists can be easily downloaded and stored in handheld readers.

Malware also exists that can compromise smart card–based authentication. For example, in 2012 the threat intelligence company Alien Value discovered a Sykipot malware variant that could capture a Windows user's PIN and covertly use a smart card to authenticate to remote websites.[18] However, such malware is generally difficult to write and rare, and the malware's ability to authenticate as the user ends when the card is removed from the reader.

With the coming year, a growing number of people will become familiar with smart cards, thanks to the increased deployment of credit cards that follow the EMV (Europay, MasterCard, Visa) standard and the requisite smart card readers. As such, organizations might want to consider smart cards as a replacement for passwords, rather than deploying two-factor systems that address only some of the security and none of the usability problems inherent when using "strong" passwords. ■

Acknowledgments

Although the National Institute of Standards and Technology (NIST) previously reported the results of the US Department of Commerce survey,[19] this publication marks the first time that the results of the US Department of Defense survey[20] have been publicly reported and the first time that the lessons of the two surveys have been put in the context of the government-wide deployment of high-assurance credentials and the lessons that the deployments might have for private industry. Specific products and organizations identified in this report were used to perform the evaluations described. In no case does such identification imply recommendation or endorsement by NIST, nor does it imply that those identified are necessarily the best available for the purpose. William Barker at NIST and Carla Scanlan at the Defense Manpower Data Center provided useful feedback on a draft of this article.

References

1. "Annual Report to Congress, Office of Management and Budget," The White House, 27 Feb. 2015; www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
2. "Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity," Executive Office of the President, Office of Management and Budget, 12 June 2015; www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf.
3. "Use of Smart Card Technology in the Department of Defense," National Defense Authorization Act for Fiscal Year 2000 (Public Law 106-65), Sec. 373, 5 Oct. 1999.
4. *Electronic Government: Progress in Promoting Adoption of Smart Card Technology*, tech. report GAO-03-144, US Government Accountability Office, 3 Jan. 2003; www.gao.gov/products/GAO-03-144.
5. "Smart Card Senior Coordinating Group Charter," US Dept. Defense, 14 Apr. 2000; www.doncio.navy.mil/Download.aspx?AttachID=300.
6. "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors," US Dept. Homeland Security, 27 Aug. 2004; www.dhs.gov/homeland-security-presidential-directive-12.
7. "HSPD-12 FAQs," Office of Management and Budget, 1 Oct. 2009; www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNLjAAO&field=File__Body__s.
8. "HSPD-12 Implementation Status Reports," Office of Management and Budget, 24 Dec. 2015; www.whitehouse.gov/omb/e-gov/hspd12_reports.
9. *Audit of USAID's Implementation of Selected Homeland Security Presidential Directive 12 Requirements for Personal Identity Verification of Federal Employees and Contractors*, audit report A-000-08-004-P, Office of the Inspector General, 6 Feb. 2008; http://pdf.usaid.gov/pdf_docs/PDACS047.pdf.
10. "Progress Has Been Made; However, Significant Work

Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12," reference no. 2014-20-069, Treasury Inspector General for Tax Administration, 12 Sept. 2014; www.treasury.gov/tigta/auditreports/2014reports/201420069fr.pdf.

11. "Annual Report to Congress: Federal Information Security Management Act," Office of Management and Budget, 27 Feb. 2015; www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
12. S. Garfinkel and H. Lipford, *Usable Security: History, Themes, and Challenges*, Morgan & Claypool, 2014.
13. R. Morris and K. Thompson, "Password Security: A Case History," *Comm. ACM*, vol. 22, no. 11, 1979, pp. 594–597.
14. J. Bonneau et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *Proc. IEEE Symp. Security and Privacy* (SP 12), 2012, pp. 553–567.
15. A. Beautement, M.A. Sasse, and M. Wonham, "The Compliance Budget: Managing Security Behaviour in Organisations," *Proc. Workshop on New Security Paradigms* (NSPW 08), 2008, pp. 47–58.
16. D. Florêncio, C. Herley, and P.C. Van Oorschot, "An Administrator's Guide to Internet Password Research," *Proc. 28th USENIX Conf. Large Installation System Administration* (LISA 14), 2014, pp. 35–52.
17. D. Florêncio, C. Herley, and B. Coskun, "Do Strong Web Passwords Accomplish Anything?," *Proc. 2nd USENIX Workshop on Hot Topics in Security* (HOTSEC 07), 2007, article 10.
18. J. Blasco, "Sykipot Variant Hijacks DoD and Windows Smart Cards," AlientVault Blogs, 12 Jan. 2012; www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards.
19. Y.-Y. Choong, M. Theofanos, and H.-K. Liu, "United States Federal Employees' Password Management Behaviors—A Department of Commerce Case Study," Nat'l Inst. Standards and Technology, 8 Apr. 2014; http://dx.doi.org/10.6028/NIST.IR.7991.
20. *QuickCompass of DoD Civilian Employees: Statistical Methodology Report*, report 2012-045, Defense Manpower Data Center, 2012.

Mary Theofanos is a computer scientist at the National Institute of Standards and Technology (NIST) and was the principal architect of the Usability and Security Program. Her research interests include usability and human factors of systems. Theofanos received a MS in computer science from the University of Virginia. Contact her at mary.theofanos@nist.gov.

Simson Garfinkel is a computer scientist at NIST. His research interests include computer security and privacy. Garfinkel received a PhD in computer science from the Massachusetts Institute of Technology. Contact him at simson.garfinkel@nist.gov.

Yee-Yin Choong is a cognitive scientist at NIST. Her research interests include human factors and cognitive engineering. Choong received a PhD in human factors from Purdue University. Contact her at yee-yin.choong@nist.gov.