RAND

HOMELAND SECURITY AND DEFENSE CENTER

CHILDREN AND FAMILIES

EDUCATION AND THE ARTS

ENERGY AND ENVIRONMENT

HEALTH AND HEALTH CARE

INFRASTRUCTURE AND TRANSPORTATION

INTERNATIONAL AFFAIRS

LAW AND BUSINESS

NATIONAL SECURITY

POPULATION AND AGING

PUBLIC SAFETY

SCIENCE AND TECHNOLOGY

TERRORISM AND HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: Jump to Page 1

Support RAND

Purchase this document

Browse Reports & Bookstore

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND Homeland Security and Defense Center

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Influences on the Adoption of Multifactor Authentication

Martin C. Libicki, Edward Balkovich, Brian A. Jackson,
Rena Rudavsky, Katharine Watkins Webb

Sponsored by the National Institute of Standards and Technology



HOMELAND SECURITY AND DEFENSE CENTER

This report was sponsored by the National Institute of Standards and Technology and was conducted under the auspices of the RAND Homeland Security and Defense Center, a joint center of the RAND National Security Research Division and RAND Infrastructure, Safety, and Environment.

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2011 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Authentication in cyberspace is the process of verifying user identity prior to granting access to specific computer, network, or Internet services and resources. The user password is the form of authentication that remains the primary means of user identification. Passwords can be very convenient, requiring little more than memory and typing to apply them. Yet, as nearly every computer and security professional will attest, passwords are a notoriously weak form of authentication; they can be compromised at any point in the authentication process.

Since passwords alone no longer provide adequate authentication for many types of information (especially in the face of new sniffers,[1] keystroke loggers,[2] and better cracking algorithms, coupled with faster machinery), the use of multiple factors for network access might be recommended. The benefits of multifactor authentication are that hackers (or insiders) have to break (that is, gain unauthorized access to systems protected by) not one but many authentication devices. Each tends to have different strengths and different weaknesses. NIST Special Publication 800-63[3] recommends MFA for remote authentication to achieve assurance levels 3 and 4. Nevertheless, its implementation is not widespread. Although MFA is mandated for federal agencies, as per Homeland Security Presidential Directive-12 (HSPD-12)[4] coupled with Office of Management and Budget (OMB) Memorandum M-06-16, many private organizations tend to avoid its use for employees, much less for other associates and customers (e.g., account holders).

Hence the question: What factors account for the decision of organizations to use, or alternatively, to reject MFA in favor of passwords or other forms of single-factor authentication? Among those who require MFA, where do they use it, and what factors do they require for various types of system access?

RAND sought to understand what motivates organizations to adopt MFA through a variety of approaches. First, RAND reviewed existing academic and quasi-academic literature to discern patterns and insights. The results are presented in the first half of Chapter Two. Second, RAND collected articles from the business press to elicit commentary on these questions and examples from various sectors on what forms of authentication were being pursued and to what end. The results complete Chapter Two.

The third, but primary, approach was to interview representatives from a variety of organizations regarding their perspective on MFA within their organizations. In a few cases, we

[1] A *sniffer* is software that intercepts information as it is going over a network.

[2] A *keystroke logger* is software that intercepts what a person types and sends it to a third party.

[3] Burr, Dodson, and Polk, 2006.

[4] DHS, 2004.

interviewed suppliers of MFA solutions to gain their perspectives on industry perceptions and trends. The selection of interviewees was not random; it was influenced by self-selection among organizations, which are normally quite reluctant to discuss important elements of their network security posture (of which MFA is surely one). This, in turn, influenced the distribution of organizations that *were* willing to discuss such matters. We interviewed six defense contractors (technically, federally funded research and development centers or FFRDCs), four health care organizations (hospitals), one government agency, two financial firms, one foundation, and four technology providers or representatives (two of which also answered questions about their own use of MFA).

Findings

MFA choices depend in large part on what sector an organization is in. The six FFRDCs we interviewed all had very similar rules regarding MFA: They employed tokens and PINs as log-in requirements for remote access but not for most internal access. Practices in the health care sector reflected the exigencies of health care: the need to attract doctors to the facility; the relative infrequency of off-site users wanting to come into the network; the tendency to carefully control medical information, even to patients; and the well-known potential for abuse in writing prescriptions. The federal government, for its part, operates under HSPD-12, which mandates the use of smart cards (the Common Access Card, or CAC, for the Department of Defense [DoD]) but in such a way as to couple network access to physical access. The financial sector is potentially the most varied in its implementation practices. Despite regulations (more like "guidelines") that require financial institutions to protect certain data to a certain minimum level and indicate that MFA meets these criteria, organizations in this sector make network access decisions internally. Such decisions tend to be based on competitive customer retention strategies or potential liability calculations in the face of the rising tide of cybercriminality and hard legal limits on the customer's responsibility for losses. This trade-off tends to make financial institutions sensitive to high-end losses and thus more likely to demand stronger credentials for Internet banking when the transaction sums involved are high.

User resistance after implementation is a nonissue, so far. We heard little evidence from organizations that their users pushed back against MFA adoption—particularly once it became mandatory. Prospectively, however, the fear of user pushback *does* inhibit MFA adoption, particularly among organizations that cater to users who have a choice regarding which organization to patronize.

MFA adoption tends to "stick." In no case did an organization adopt MFA and later change its mind.

Tokens rather than biometrics predominate. Among private users of MFA, tokens of the sort that generate one-time passwords are by far the most important second-factor authentication method (if one defines PINs/passwords as the nearly universal first factor).

Threat models are in their nascent stages. In no case did a respondent offer a systematic process for evaluating the requirement for particular security levels. None, also, claimed to have adopted MFA because they had suffered a cyberattack that might have been prevented with MFA. Several respondents had, however, suffered cyberattacks in the past—which often made it easier to sell MFA to top management.

MFA tends to be part of a broader security architecture. Typically, an organization that has reviewed its security posture and found it wanting takes a large number of related steps at the same time—not just adopting MFA. These steps may include more-intensive monitoring, intrusion-detecting systems, closing unnecessary communications ports, curtailing administrative privileges or access from certain locations or machines, and improving physical security.

Deterministic authentication methods compete with probabilistic authentication methods. Organizations may choose to use one or—more likely—a collection of authentication methods that meet their requirement for sufficient authentication. Many probabilistic authentication methods allow organizations without MFA to have what they deem a sufficient level of confidence that the individuals carrying out transactions are likely who they say they are.

Future plans favor wider MFA use. Some companies plan to search for MFA technology that is easier to use than their current chosen MFA solution; this is especially true if early MFA choices relied on complex and immature technology. Other organizations, particularly within health care, are working to collaborate with industry partners in their geographic vicinity to create shared MFA solutions.

Compulsion and expectations tend to drive MFA adoption. Many organizations have no choice but to adopt MFA, at least for some functions. Federal agencies must comply with HSPD-12. In one state, pharmaceutical prescriptions can be made electronically only if two factors are used to authenticate the prescriber. The Drug Enforcement Administration is working on regulations that would require two-factor authentication for all prescriptions of controlled drugs. Bank regulations have also influenced adoption. Other organizations appear very conscious of how secure their customers or other vital stakeholders perceive them to be. This is particularly evident in the case of FFRDCs, which are considered part of the defense industrial base. Similarly, those whose product offerings include security in some way also operate under similar, if not as precisely defined, expectations. Conversely, those whose customers do not care (or more precisely, have no need to care) or those whose other stakeholders (e.g., practicing physicians in the case of hospitals) are more sensitive to operational hassles than to the lack of security have no such incentive or may tilt away from MFA.

Table S.1 is a matrix that summarizes how different influences on the adoption of MFA play out in three of the sectors we examined.

Table S.1
Influences on the Adoption of MFA, by Sector

Influence	FFRDCs	Health Care Providers	Financial Institutions
Compulsion	Not explicit[a]	Only for writing prescriptions	Not explicit
Customer expectations	Primary customer (DoD) expects as much, so MFA is not an issue	Customers do not care	Larger customers may increasingly expect MFA as an option
Cost control	No cost savings identified from MFA adoption	No cost savings identified from MFA adoption	Cost savings an implied driver for MFA adoption for large transactions

[a]Refers to access to unclassified networks; classified networks operate under more explicit rules.

Recommendations

1. *The U.S. government should, with NIST guidance, develop methodologies by which the costs and benefits of mandating MFA can be evaluated.* The fact that mandates work does not mean that mandates should be employed everywhere. In some cases, institutions themselves bear all or most of the costs and benefits of whatever level of security they deem necessary; thus, they are in the best position to determine how much security is optimal. In other cases, broader interests are involved—e.g., national security, infrastructure protection, and financial integrity. NIST guidance to other federal agencies, as well as advisory guidance to state and local governments, may be useful in helping them sort out the various arguments for and against mandating MFA in one sector or another.
2. *The promotion of interoperability standards is worthwhile, but expectations of the benefits of doing so should be tempered.* No respondent cited the existence of standards as a reason to adopt MFA and no one cited the lack of comprehensive standards as a reason not to. There has yet to be much cross-enterprise demand for MFA in general, much less any particular MFA (e.g., one-time password tokens vis-à-vis smart cards). Most people have only one job (that is, they report to only one organization) and the demand to authenticate e-commerce transactions to a degree of rigor associated with MFA use has yet to become compelling. Nevertheless, if MFA proliferates, users may tire of having to present different credentials for multiple sites, especially if they include multiple tokens in addition to passwords. MFA's spread may then slow to the point where no one has to carry more than one authentication device: Either there will be a master registry or sufficient peering among multiple registries.[5] Standards may help us reach that point. But note that an older quest—for interoperable public-key infrastructure registries—is far from complete.
3. *Research is needed to permit MFA to work in the light of the possibility that user computers may be suborned by hackers.* Any device that is or can temporarily be connected to the Internet is at risk of having malware (such as the Zeus Trojan) unintentionally installed by the authorized user. Once installed, that malware can masquerade as the authorized user (whose identity is established by multiple factors) in order to compromise confidentiality, integrity, or availability of the device and/or trusted networks that device is authorized to use.

---

[5] *Peering* is as an agreement among entities (such as networks or authentication services) to exchange information.