One of the nicest aspects of writing this column for so long (I started in 2000) is the tremendous support I get from readers in industry, education and government. For example, I just received a friendly note from Timothy Grance, Manager of the Systems & Network Security Group of the Computer Security Division (CSD) of the National Institute of Standards and Technology (NIST) http://csrc.nist.gov/staff.htm. He pointed to a number of draft publications that will interest many readers and so I'll review them in this and upcoming columns. Anyone wanting to be added to an e-mail notification list about new NIST security publications can subscribe for free.

SP 800-45A, “Guidelines on Electronic Mail Security” http://csrc.nist.gov/publications/drafts.html “is intended to aid organizations in the installation, configuration, and maintenance of secure mail servers and mail clients.” Authors Miles Tracy, Wayne Jansen, Jason Butterfield, Karen Kent, and Scott Bisker have structured the 143-page document with the following main sections:

1. Introduction
2. Background and Standards
3. Email-Related Encryption Standards
4. Planning and Management of Mail Servers
5. Securing the Operating System
6. Mail Server and Content Security
7. Implementing a Secure Network for a Mail Server
8. Mail Client Security
9. Securely Administering a Mail Server

Major topics include (quoting directly from the Executive Summary):

- Email standards and their security implications
- Email-related encryption standards
- Email-specific aspects of securing the underlying operating system
- Securing mail server applications
- Filtering email content
- Email-specific considerations in the deployment and configuration of network protection mechanisms:
  - Firewalls
  - Routers
  - Switches
  - Intrusion detection systems and intrusion prevention systems
- Securing mail clients
- Administering the mail server in a secure manner:
Backups
Security testing
Updating and patching
Log reviews
Records management/archiving email.

Highlights of the recommendations (again, quoted from the Executive Summary) include:

- Organizations should carefully plan and address the security aspects of the deployment of a mail server.
- Organizations should implement appropriate security management practices and controls when maintaining and operating a secure mail server.
- Organizations should ensure that the mail server operating system is deployed, configured, and managed to meet the security requirements of the organization.
- Organizations should ensure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization.
- Organizations should consider the implementation of encryption technologies to protect user authentication and mail data.
- Organizations should employ their network infrastructure to protect their mail server(s).
- Maintaining the security of a mail server is an ongoing process.

Readers of this column will be particularly pleased to see the appendices, which include a glossary, a list of Internet Engineering Task Force (IETF) Requests for Comment (RFCs), a detailed list of references for further reading, a list of 35 sets of e-mail security tools and applications including Web links and descriptions, a seven-page list of useful URLs and nine pages of checklists that can be used in review and auditing.

If readers have comments for improvement of the documents, they can submit them to <mailto:sp800-45a@nist.gov?Subject=Comments%20SP800-45A> by October 6, 2006.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.