As I mentioned in a previous column, there’s a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) <http://csrc.nist.gov/publications/drafts.html>.

SP 800-94, “Guide to Intrusion Detection and Prevention (IDP) Systems” <http://csrc.nist.gov/publications/drafts/Draft-SP800-94.pdf> is intended to assist organizations in understanding intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention (IDP) solutions. It provides practical, real-world guidance for each of four classes of IDP products: network-based, wireless, network behavior anomaly detection software, and host-based. The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software. It focuses on enterprise IDP solutions, but most of the information in the publication is also applicable to standalone and small-scale IDP deployments. This publication replaces NIST SP 800-31, Intrusion Detection Systems.”

The document was written by Karen Kent and Peter Mell and has the following structure:

1. Introduction
2. Intrusion Detection and Prevention Principles
3. Overview of IDP Technologies
4. Network-Based IDP
5. Wireless IDP
6. Network Behavior Anomaly Detection Software
7. Host-Based IDP
8. Using and Integrating Multiple IDP Technologies
9. IDP Product Selection

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

- Organizations should ensure that all IDP components are secured appropriately.
- Organizations should consider using multiple types of IDP technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.
- Organizations planning to use multiple types of IDP technologies or multiple products of the same IDP technology type should consider whether or not the IDPs should be integrated.
- Before evaluating IDP products, organizations should define the requirements that the products should meet.
- When evaluating IDP products, organizations should consider using a combination of several sources of data on the products’ characteristics and capabilities.
As usual, the document includes a glossary (Appendix A), a list of acronyms (Appendix B) and an extensive list of print and online resources pertaining to IDP systems and charts showing vendors of various types of products:

- Common Enterprise Network-Based IDP Systems (20 product lines)
- Common Enterprise Wireless IDP Systems (8 products)
- Common Enterprise NBAD (network behavior anomaly detection) Systems (7 companies)
- Common Enterprise Host-Based IDP Products (12 product lines).

If readers have comments for improvement of the documents, they can submit them to <mailto:800-94comments@nist.gov?Subject=Comments%20SP800-94> by October 20, 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.