

HIPAA Security Annotated Bibliography

Bill Ganucheau, MA, MBA, CMPE
WRG001@LAPHYSCORP.COM

Spring, 2001



3Com. "Enhancing Enterprise Security. An Overview of Network Security Issues and Technologies." (30 Apr. 1999). Online. Internet. 16 Feb. 2001. Available http://www.3com.com/technology/tech_net/white_papers/503023.html .
Succinct treatment of user authentication, challenge and response, digital certificates, digital signatures, access control, firewalls, encryption, and Internet protocol security [3COM-ENHANCE]

3Com. "Healthcare Information Security: How a Secure Data Network Can Help Healthcare Organizations Meet the Challenge of Healthcare Security Regulations." (3 Dec. 1999). Online. Internet. 16 Feb. 2001. Available http://www.3com.com/technology/tech_net/white_papers/503069.html .
Diagram of potential security breaches; Elements of a comprehensive security solution: 1) Physical protection: where are you? 2) User authentication: who are you? 3) Access control: what assets are you allowed to use? 4) Encryption: what information should be hidden, and how? 5) Management: what is happening within the network? [3COM-HEALTHCARE]

Alcatel Corporation. "VLANs, Authenticated VLANs, and firewalls: How they relate to the United States Health Insurance Portability and Accountability Act." (1999). Online. Internet. 12 Feb. 2001. Available <http://www.ind.alcatel.com/library/whitepapers/hipaa.html> .
Description of Authenticated Virtual Area Networks [ALCATEL]

Appgate. "Six Steps Toward Better Security." (Undated). Online. Internet. 2 Feb. 2001. Available http://www.appgate.com/sales/six_steps.html .
*Includes extensive list of links for security patches, sites for advisories and alerts, security mailing lists, firewall introduction articles, security FAQs, security sites, underground magazines, cracker tools to try against your system, and tools to prevent or detect intrusion. *8 [APPGATE]*

Arthur Andersen. "HIPAA Glossary." (2001). Online. Internet. 5 Feb. 2001. Available <http://www.arthurandersen.com/website.nsf/content/IndustriesHealthcareResourcesHIPAAGlossary?OpenDocument>
Glossary of terms used in the HIPAA security section of the Act.

Baldwin, Fred D. "Believing in Biometrics." Healthcare Informatics. (August, 2000). Online. Internet. Available http://www.healthcare-informatics.com/issues/2000/08_00/baldwin.htm
Biometric technologies not only exist—they work and are now affordable. Comparison of retinal-scan, fingerprint, facial geometry, voice recognition and dynamic signature technologies. [BALDWIN]

Boran, Seán. "An Overview of Corporate Information Security. Combining Organization, Physical and IT Security." (13 Dec. 1999). Online. Internet. 17 Feb. 2001. Available <http://secinf.net/info/policy/coverstory19991213.html> .

*Good graphic of 3 basic "domain interfaces" to the outside world (1) Physical; (2) Social/personal; (3) Data and voice networks. Concise treatment of threats and countermeasures for each interface. *2-3[BORAN]*

Brain, Marshall. "How Web Servers and the Internet Work." (Undated). Online. Internet. 10 Jan. 2001. Available <http://www.howstuffworks.com/web-server.htm?printable=1> .

*Basic introduction to the process of retrieving web pages on the Internet, including IP Addresses, domain names, domain name servers, ports, and protocols. *8 [BRAIN]*

Branco, Marcia. "Overview of HIPAA's Security Concepts." Sans Institute. 13 Apr. 2000. Available <http://www.sans.org/infosecFAQ/legal/HIPAA.htm> .

Brief introduction of the HIPAA security requirements and four categories. Brief descriptions of IPSec, 3DES, VPN, PGP, MD5 and PKI. ?1-2 [BRANCO]

Canavan, John. "Security an Issue When Considering Frame Relay." Telecommunications Americas. (June, 1999). Online. Internet. 21 Jan. 2001. Available

<http://www.telecoms-mag.com/issues/199906/tcs/security.html> .

Brief coverage of the potential security threats of frame relay networks, stressing the importance of working closely with vendors to achieve an acceptable level of security. [CANAVAN]

Centerline 2000. "A Backgrounder to Securing Your Internet Connection." (Undated). Online. Internet. 15 Jan. 2001. Available <http://www.c2000.com/papers/security.htm> .

Internet security primer, including firewall types and selection criteria, testing "probing" the strength of your firewall, selecting an intrusion detection device, user authentication, VPN's, encryption, and more. [CENTERLINE]

Cisco_Systems. "Network Security Solutions for Healthcare." (3 Jul. 2000). Online Internet. 15 Jan. 2001. Available http://www.ieng.com/warp/public/cc/pd/sqsw/tech/hippa_rg.htm

Alphabetical list of technical terms (and user-friendly definitions) used in the Security regs. A Solutions Guide discussing network security architecture for the transfer of Personally Identifiable Health Information utilizing Internet, Intranet and Extranet technologies. Good diagrams! [CISCO-NETWORK]

Cisco Systems. "Security and Health Care Enterprise Networks: Balancing Technology with Culture." (29 Dec. 2000). Online. Internet. 16 Feb. 2001. Available

http://www.cisco.com/warp/public/cc/so/veso/health/shcen_wi.htm .

Excellent bulleted list of questions or topics to address during review process. Good diagrams and treatment of the security framework of "Drivers" and "Enablers" of HIPAA

Security Policy, as well an overview of the Cisco hardware products designed to do the enabling. [CISCO-SECURITY]

Cook, Chad. "An Introduction to Encryption." (6 Nov. 2000). Online. Internet. 31 Jan. 2000. Available <http://www.securityfocus.com/> . (Basics tab; Information Security Solutions section) *From the basics of the "Caesar Cipher" to modern asymmetrical cryptography, this article covers the basic design, uses, and protections offered by encryption technology. [COOK-ENCRYPTION]*

Cook, Chad. "An Introduction to Incident Handling." (29 Nov. 2000). Online. Internet. 31 Jan. 2001. Available <http://www.securityfocus.com/> .(Basics tab; Information Security Solutions section) *This paper provides a short overview and several guidelines to handle security incidents with regards to three of the most common attacks - viruses, system compromise and denial of service. [COOK-INCIDENT]*

Fraser, B. The Site Security Handbook. (Sep. 1997). Online. Internet. 5 Jan. 2001. Available <http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt> . *This handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response. [FRASER]*

Felton, Edward W., et al. "Web Spoofing—How It Works and How to Defend from It." Princeton University Department of Computer Science . (1996). Online. Internet. 17 Feb. 2001. Available <http://secinf.net/info/www/security16.txt> . *This paper describes an Internet security attack that could endanger the privacy of World Wide Web users and the integrity of their data. The attack can be carried out on today's systems, endangering users of the most common Web browsers, including Netscape Navigator and Microsoft Internet Explorer. Web spoofing allows an attacker to create a "shadow copy" of the entire World Wide Web. Accesses to the shadow Web are funneled through the attacker's machine, allowing the attacker to monitor the all of the victim's activities including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to Web servers in the victim's name, or to the victim in the name of any Web server. In short, the attacker observes and controls everything the victim does on the Web. [FELTON]*

- Griffin, Brad. "An Introduction to Viruses and Malicious Code." (6 Nov. 2000). Online. Internet. 31 Jan. 2001. Available <http://www.securityfocus.com/> . (*Basics tab; Information Security Threats section; Viruses Part 1*)
The author discusses the different types of viruses and malicious code, what they are, how they infect your computer and what damage they can cause. [GRIFFIN-VIRUSES]
- Griffin, Brad. "An Introduction to Viruses and Malicious Code Part Two: Protecting Your Computers and Data." (27 Dec. 2000). Online. Internet. 1 Feb. 2001. Available <http://www.securityfocus.com/> .(*Basics tab; Information Security Threats section; Viruses Part 2*)
Ways in which you can help prevent a virus 'attack'. This is not another 'how-to use an anti-virus program' article; rather, it is intended to be a base reference for you to develop a safe computing policy for your business. Safe computing habits are the best defense against malicious code. How you handle e-mail attachments, floppy disks, CDs and other external media can mean the difference between a clean computer and an infected one. [GRIFFIN-INTRO2]
- Guttman, Barbara and Bagwill, Robert. "NIST's Special Publication: Internet Security Policy: A Technical Guide [DRAFT]." U.S. Department of Commerce National Institute of Standards and Technology. (21 Jul. 1997). Online. Internet. 17 Feb. 2001. Available <http://csrc.nist.gov/isptg/>.
National Institute of Standards and Technology publication, featuring sample Internet security policy statements for "low," "medium," and "high" security, covering all aspects of Internet security concerns. [GUTTMAN]
- Hazari, Sunil. "Firewalls for Beginners." (6 Nov. 2000). Online. Internet. 31 Jan. 2001. Available <http://www.securityfocus.com/> . (*Basics tab; Information Security Solutions section*)
A description of the function of firewalls, including treatment of TCP/IP, packets, ports and port scanners. Different types of firewalls are described, as well as basic questions to ask when making a purchase decision. [HAZARI]
- "HIPAA Security Summit Guidelines (Draft)." (26 Jun. 2000). Online. Internet. 10 Jan. 2001. Available <http://www.smed.com/hipaa/draft.pdf> .
Excellent point-by-point coverage of the HIPAA security regulations, including bulleted questions for each topic to begin addressing it. Also a model for continuous feedback and improvement of the security system. [SUMMIT]
- Jenkins, Joe. "Internet Security and Your Business - Knowing the Risks." (6 Nov. 2000). Online. Internet. 1 Feb. 2001. Available <http://www.securityfocus.com/> . (*Basics tab; Information Security Threats section; "Knowing the Risks"*)
Many small or home business owners do not realize that they are just as likely to be targeted as any large company. As a consequence of existing in the digital age, almost everyone is vulnerable to breaches of security. If your business relies on computer or

Internet technology, you need to be prepared to deal with security issues. This article provides an overview of the Internet-based threats to business systems. [JENKINS]

Johnson, Thomas, et al. "What CIO's need to know about Information Security and HIPAA." Sheldon I. Dorenfest & Associates. Undated. Online. Internet. 18 Jan. 2001. Available http://www.dorenfest.com/pages/press/infosec_101.htm .
Includes a good list of "10 Critical Success Factors toward Achieving HIPAA Compliance." [JOHNSON]

Kane, Beverley and Sands, M.D., Daniel Z. "Guidelines for the Clinical Use of Electronic Mail with Patients." Journal of the American Medical Informatics Association. 5 (1998). Online. Internet. 20 Feb. 2001. Available http://www.amia.org/pubs/other/email_guidelines.html .
Guidelines regarding patient-provider electronic mail are presented. The guidelines address two interrelated aspects: effective interaction between the clinician and patient, and observance of medico legal prudence. Recommendations for site-specific policy formulation are included. The purpose of this document is to guide clinicians and health care delivery organizations in the use of electronic mail (e-mail) communication with patients so that this method of communication might enhance the value of, rather than introduce complications into, the provider-patient relationship. [KANE]

Management Analytics. "Internet Holes: 50 Ways to Attack Your Web Systems." (1995). Online. Internet. 31 Jan. 2001. Available <http://secinf.net/info/www/9512.html> .
The author classifies Internet attacks from different perspectives: (1) attacks against browsers; (2) attacks against servers; (3) attacks against networks. Alternatively, internet-based attacks can be classified according to the types of harm which can be done: (a) corruption; (b) denial; (c) leakage (i.e. stolen data); (d) liability (i.e. attacked sites are themselves used to launch other attacks). The 50 most common methods of attack are then described. Finally, the author warns that many of these attacks cannot be prevented through firewall technology, so simply having a firewall is not enough. [MANAGEMENT]

McGibbon, Stephen. "Firewalls and Internet Security." Undated. Online. Internet. 17 Feb. 2001. Available <http://secinf.net/info/fw/steph/> .
Chapters include (1) Overview; (2) Introduction to Internet Security; (3) The TCP/IP Protocols; (4) Computer Security–Risks and Attacks; (5) Network Security Policy; (6) Firewall Theory and Architecture; (7) Future Developments; (8) Summary and Conclusions. Good treatment of "Social Engineering" attacks (i.e. impersonation) as well as what a firewall can and can't do. [MCGIBBON]

- Mossy, Glenn. "Securing a Medical Information System at Federal Research Agency." Sans Institute. (3 Dec. 2000). Online. Internet. 12 Jan. 2001. Available http://www.sans.org/infosecFAQ/securitybasics/med_info.htm .
A case study of the process of implementing sound security practices at a radiology practice in a research center. Good collection of related links and on-line bibliography at end, too.
[MOSSY]
- National Research Council. For the Record: Protecting Electronic Health Information. Washington, D.D. National Academy Press. 1997. Online. Internet. 15 Dec. 2000. Available <http://stills.nap.edu/readingroom/books/for/index.html> .
The National Research Council's substantial and authoritative 1997 study of current security practices in place in American health care organizations, and sound recommendations for the future. Quoted in the HIPAA proposed security regulations to support the conviction that "a set of (security) practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another" **[NATIONAL]**
- "NSA Glossary of Terms Used in Security and Intrusion Detection." (Apr. 1998). Online. Internet. 4 Apr. 2001. Available <http://www.sans.org/newlook/resources/glossary.htm> .
Excellent and extensive glossary of computer security terminology.
- Ranum, Marcus J. "Intrusion Detection: Challenges and Myths." Network Flight Recorder, Inc. (1998). Online. Internet. 17 Feb. 2001. Available http://secinf.net/info/ids/ids_mythe.html
Clear discussion of the differentiation between two types of Intrusion Detection Systems (IDS): AD-IDS (Anomaly Detection Intrusion Detection Systems) and MD-IDS (Misuse Detection Intrusion Detection Systems). **[RANUM]**
- Schell, Dan. "Biometrics in Healthcare." Business Solutions. (Undated). Online. Internet. 30 Jan. 2001. Available http://www.businesssolutionsmag.com/Articles/2000_11/001105.htm
The advantages of biometric identification (especially fingerprint scans) for healthcare, especially with the falling cost of biometric technology in general. The author makes a case for using fingerprint identification not only for health care employees, but also for patients.
[SCHELL]
- Strebe, Matthew and Perkins, Charles. "TCP/IP from a Security Viewpoint." Firewalls, 24 Seven. (Sibex, Inc., 2000). Online. Internet. 6 Feb. 2001. Available <http://www.microsoft.com/technet/security/tcpip.asp> .

Includes “vulnerabilities” and “remedies” on the Physical layer. Good technical article.
[STREBE]

Tunitas Group. “Details of the HIPAA Mandated Security Standards.” Tunitas Group Session Notes. (10 Oct. 1998). Online. Internet. 10 Jan. 2001. Available <http://www.tunitas.com/pages/sessionNotes/Notes.html> .
One consulting group's comments and notations on the HIPAA security and privacy regulations. The document raises more than a few issues with the proposed regulations, due to lack of clarity and specificity. **[TUNITAS]**

Tyson, Jeff. “How Firewalls Work.” (Undated). Online. Internet. 28 Jan. 2001. Available <http://www.howstuffworks.com/firewall.htm?printable=1> .
Introduction to firewalls. Excellent list of (1) protocols (2) creative hacker attack methods.
[TYSON]

United States. Department of Health and Human Services. “Notice of Proposed Rule Making for the Security and Electronic Signature Standards.” Cong. Rec. 12 Aug. 1998. 43241-43280.
<http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm> .
The complete text of the proposed HIPAA security standards. **[US-NPRM]**

University of Missouri Health Care. “HIPAA Security Standards: Definitions.” (01 Mar. 2000). Online. Internet. 5 Jan. 2001. Available <http://hsc.missouri.edu/~hipaa/reference/hpra09.html> .
Alphabetical list—with definitions—of all terminology used in the HIPAA security regs. **[U-M]**

Unruh, Bill. “Cryptography.” (1998). Online. Internet. 10 Jan. 2001. Available <http://axion.physics.ubc.ca/crypt.html> .
Introduction to crypto systems. The expansion of the connectivity of computers make ways of protecting data and messages from tampering or reading important. Even the US courts have ruled that there exists no legal expectation of privacy for email. It is thus up to the user to ensure that communications which are expected to remain private actually do so. One of the techniques for ensuring privacy of files and communications is Cryptography. The author itemizes a list of freely available crypto systems, hoping to serve the reader with an introduction to the technology. **[UNRUH]**