

The IT Governance Institute® is pleased to offer you this complimentary download

This research material has been made available by the IT Governance Institute (ITGI®). By downloading this document, you acknowledge that you have read and understood the copyright restrictions of this publication and that you agree to abide by them. ITGI retains all copyrights and other proprietary rights in or relating to the content.



What:

The IT Governance Institute (ITGI) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimizes business investment in IT, and appropriately manages IT-related risks and opportunities. The IT Governance Institute offers symposia, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Activities

- ◆ Sponsors high-level conferences and symposia around the world.
- ◆ Offers as an open standard (www.isaca.org/cobit) *Control Objectives for Information and related Technology* (COBIT®), a breakthrough IT governance tool that uses nontechnical language to help organizations focus their information technology in support of overall business objectives.
- ◆ Conducts original research and publishes guidance to help boards of directors, executives and management understand their changing roles and implement effective IT governance.
- ◆ Offers case studies on how leading global organizations are implementing IT governance programs and activities.
- ◆ Offers the IT Governance Business Game, a day-long training session.
- ◆ Hosts the IT governance listserv for professionals to share experience.

What:

The Information Systems Audit and Control Association® (ISACA®) is the leading association of professionals in information systems (IS) audit, control, security and governance. ISACA has a global membership of more than 35,000 in 100 countries in Asia, Central America, South America, Europe, Africa, North America and Oceania. Founded in 1969 as the EDP Auditors Association, ISACA is a global leader in IT governance, security, control and assurance. It is the single leading international source for information technology controls. ISACA is dedicated to serving the needs of its members, who are internal and external auditors, CEOs, CFOs, CIOs, educators, information security and control professionals, students and IT consultants.

Activities

- ◆ Offers the Certified Information Systems Auditor™ (CISA®) designation—a globally respected designation for experienced IS audit, control and security professionals earned by more than 35,000 professionals worldwide since inception.
- ◆ Offers the Certified Information Security Manager® (CISM®) designation—a globally respected designation designed for leaders who manage an organization's information security. Five thousand people earned the CISM designation within the first two years of its introduction.
- ◆ Sponsors technical and management conferences on five continents to ensure consistent global professional education.
- ◆ Publishes the *Information Systems Control Journal*, research and technical professional development material.
- ◆ Advances globally applicable information systems (IS) auditing standards in addition to associated guidelines and procedures.
- ◆ Develops professional resources and networking opportunities through more than 170 local chapters in support of its members



► **The Advantages of COBIT**

COBIT provides significant advantages to those who recognize the need for internal control over their information and the systems that manage it, including:

- It is increasingly accepted internationally, based on the professional and practical experiences of experts worldwide.
- It is 100 percent compliant with ISO17799, COSO I and COSO II, and maps onto many other related standards.
- COBIT is a way to bridge the communication gap between IT functions, the business and auditors, by providing a common approach, understandable by all.
- COBIT is management-oriented, actionable and easy to use.
- COBIT provides strong support for IT audit, reduces the cost of audit risk assessment, and enables a higher quality of audit and related opinion.
- COBIT avoids reinventing wheels and shortens the time required to implement effective practices.
- COBIT is a flexible and adaptable approach to suit every organization's unique cultures, size and specific requirements.
- COBIT is complete, objective and continually evolving and is maintained by a reputable not-for-profit organization.

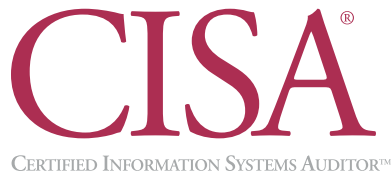
► **COBIT Components** (www.isaca.org/cobit)

- **Executive Summary**
COBIT *Executive Summary* explains COBIT key concepts and principles.
- **Framework**
COBIT *Framework* is the basis of the COBIT approach and the foundation for all the other COBIT elements. The process model is organized into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.
- **Control Objectives**
COBIT's *Control Objectives* component provides more than 300 generic control statements that define what needs to be managed in each IT process to address the business requirements of ensuring IT delivers value, risks are managed and requirements are met.
- **Control Practices**
Control Practices provides guidance on why controls are needed and what the best practices are for meeting specific control objectives. *Control Practices* helps ensure that solutions put forward are likely to be more completely and successfully implemented.
- **Management Guidelines**
COBIT *Management Guidelines* provides tools to help IT managers improve IT performance and link IT objectives to business objectives.
- **Audit Guidelines**
Audit Guidelines outlines and suggests which assessment activities should be performed for each of the 34 high-level IT control objectives, providing helpful guidance on who to interview, what questions to ask, and how to evaluate control, assess compliance and finally, substantiate the risk of the controls not being met.
- **COBIT Quickstart™** (www.isaca.org/quickstart)
COBIT *Quickstart* is specifically designed to assist in rapid and easy adoption of the most essential elements of COBIT. *Quickstart* was designed as a baseline for many SMEs but is also suitable for large organizations as a useful tool to accelerate adoption of governance best practices.

► **COBIT Online™** (www.isaca.org/cobitonline)

COBIT Online is a web-based resource where you can browse and search the very latest best practices, download customized guidance, perform benchmarking and more. A variety of subscription levels are available, each allowing different amounts and types of access and functionality. ISACA membership provides for Basic access rights and discounts on purchasing Full access.

One of the most important assets of an enterprise is its information. The integrity and reliability of that information and the systems that generate it are crucial to an enterprise's success. Faced with complex and correspondingly ingenious cyberthreats, organizations are looking for individuals who have the proven experience and knowledge to identify, evaluate and recommend solutions to mitigate IT system vulnerabilities. ISACA offers two certifications to meet these needs.



Certified Information Systems Auditor™ (CISA®)

www.isaca.org/cisa

The CISA program is designed to assess and certify individuals in the IS audit, control and security profession who demonstrate exceptional skill and judgment in information systems audit.

The CISA credential measures expertise in the areas of:

- The IS audit process
- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management

To earn the CISA designation, candidates are required to:

- Successfully complete the CISA examination*
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of five years of professional information systems auditing, control or security work experience (experience substitutions are available)
- Comply with the CISA continuing education program (after becoming certified)

*Certification exams are offered annually in June.

// ISACA's Certified Information Systems Auditor credential is one of the most popular and respected credentials in the increasingly important system audit area. //

>ED TITTEL

Certification Top 10 Lists, Certification Magazine (November 2003)



Certified Information Security Manager® (CISM®)

www.isaca.org/cism

CISM is for information security managers and those who have information security management responsibilities. It provides executive management with the assurance that those certified have the expertise to provide effective security management and consulting. It is business-oriented and focused on information risk management while addressing management, design and technical security issues at a conceptual level.

The CISM credential measures expertise in the areas of:

- Information security governance
- Risk management
- Information security program(me) development
- Information security management
- Response management

To earn the CISM designation, information security professionals are required to:

- Successfully complete the CISM examination*
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of five years of information security experience, with three years of management experience in the job practice areas (experience substitutions are available)
- Comply with the CISM continuing education program (after becoming certified)

// The CISM certification addresses a lot of what employers are telling us they are looking for in senior security managers. Enterprises need more individuals who have the expertise contained in the CISM job domains. //

>DAVID FOOTE


Foote Partners, in Certification Magazine (January 2004)

ISACA offers a full spectrum of technical and managerial conferences and education programs that are sure to meet your professional development needs. Whether you are just starting out as an IS audit, control or security professional, or are a seasoned executive, these events cover the topics and issues important to you and are presented by leading experts from around the world. No matter what your education needs, ISACA has a program that is right for you. For a complete listing of and the latest information on future conferences and educational events, please visit our web site at www.isaca.org/conferences.

Computer Audit, Control and Security Conferences (CACS)


www.isaca.org/cacs

ISACA is host to a series of annual CACS events:

 **Oceania CACS**
6-8 October 2004
Melbourne, Victoria, Australia

 **Latin America CACS**
24-27 October 2004
Mérida, Yucatán, México

 **Asia-Pacific CACS**
13-14 December 2004
Dubai, United Arab Emirates

 **North America CACS**
24-28 April 2005
Las Vegas, Nevada, USA

 **EuroCACS**
19-23 March 2006
London, UK


ISACA is also host to many other global events each year:

 **Network Security**
15-17 November 2004
Budapest, Hungary
19-21 September 2005
Las Vegas, Nevada, USA
Current Details: www.isaca.org/NetworkSecurity

 **CobIT User Convention**
4-5 November 2004
Rosemont, Illinois, USA (Chicago Area)
February 2005
Cape Town, South Africa
April 2005
Europe
Current Details: www.isaca.org/CobitUserConvention

 **Information Security Management**
19-21 September 2005
Las Vegas, Nevada, USA
Current Details: www.isaca.org/infoSecurity

 **International Conference**
19-22 June 2005
Oslo, Norway
Current Details: www.isaca.org/international

IS Audit & Control Training Week
 These intensive events, led by accomplished practitioners, offer in-depth coverage on the topics important to you.

20-24 September 2004
Amsterdam, The Netherlands

4-8 October 2004
Chicago, Illinois, USA

8-12 November 2004
Toronto, Ontario, Canada

6-10 December 2004
Atlanta, Georgia, USA

28 February - 4 March 2005
New Orleans, Louisiana, USA

7-11 March 2005
Frankfurt, Germany

6-10 June 2005
Baltimore, Maryland, USA

12-16 September 2005
Vancouver, British Columbia, Canada

October 2005
Chicago, Illinois, USA

5-9 December 2005
Phoenix, Arizona, USA

Check the web site for the most up-to-date information
www.isaca.org/TrainingWeek

TO HELP PROFESSIONALS KEEP PACE WITH THE EVER CHANGING IT ENVIRONMENT

RECENT ITGI RESEARCH PROJECTS

- COBIT and COBIT Related Products
 - COBIT Online
 - *Control Practices*
 - *COBIT Security Baseline*
- Security, Audit and Control Projects
 - *Managing Enterprise Information Integrity: Security, Control and Audit Issues*
 - *Security, Audit and Control Features PeopleSoft*
 - *Security, Audit and Control Features Oracle Applications*
 - *Oracle Database Security, Audit and Control Features*
 - *OS/390-z/OS Security, Audit and Control Features*
- Sarbanes-Oxley Projects
 - *IT Control Objectives for Sarbanes-Oxley*
 - *Sarbanes-Oxley: A Focus on IT Controls—Symposium CD-ROM*
- *IT Global Status Report*
- *Enterprise Identity Management*

PLUS TOP SELLERS FROM ITGI RESEARCH

- COBIT and Related Projects
 - COBIT 3rd Edition
 - COBIT *Quickstart*
 - *IT Governance Implementation Guide*
 - *Board Briefing 2nd Edition*
- *Security, Audit and Control Features SAP R/3*
- *Risks of Customer Relationship Management*
- *Security Provisioning: Managing Access in Extended Enterprises*
- *Virtual Private Networking—New Issues for Network Security*
- e-Commerce Security Series
 - *Business Continuity Planning*
 - *Securing the Network Perimeter*
 - *Public Key Infrastructure: Good Practices for Secure Communications*
 - *Trading Partners Identification, Registration and Enrollment*
 - *Enterprise Best Practices*
 - *A Global Status Report*

ON THE HORIZON

- Linux
- Cybercrime
- Wireless Communication

ITGI books are listed in the online bookstore under the category **Published by ISACA & ITGI.**

For additional information on these publications and others offered through the bookstore,
please visit us at www.isaca.org/bookstore

For information on research on the horizon see www.isaca.org/research



MEMBERSHIP APPLICATION

Join online and save US \$20.00

www.isaca.org/join

Please complete both sides

U.S. Federal I.D. No. 23-7067291

www.isaca.org

membership@isaca.org

MR. MS. MRS. MISS OTHER _____

Date _____

MONTH/DAY/YEAR

Name _____
FIRST MIDDLE LAST/FAMILY

PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address _____
STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE/ZIP

Residence phone _____
AREA/COUNTRY CODE AND NUMBER

Residence facsimile _____
AREA/COUNTRY CODE AND NUMBER

Company name _____

Title _____

Business address _____
STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE/ZIP

Business phone _____
AREA/COUNTRY CODE AND NUMBER

Business facsimile _____
AREA/COUNTRY CODE AND NUMBER

E-mail _____

Send mail to

- Home
- Business

Form of Membership requested

- Chapter Number (see reverse)
- Member at large (no chapter within 50 miles/80 km)
- Student (must be verified as full-time)
- Retired (no longer seeking employment)

- I do not want to be included on a mailing list, other than that for association mailings.

How did you hear about ISACA?

- 1 Friend/Coworker
- 2 Employer
- 3 Internet Search
- 4 IS Control Journal
- 5 Other Publication
- 6 Local Chapter
- 7 CISA Program
- 8 Direct Mail
- 9 Educational Event

Please note: Membership in the Association requires you to belong to a local chapter when you live or work within 50 miles/80 km of its territory. The name of the chapter is indicative of its territory. If you live further than 50 miles from the chapter territory, select member at large. This selection is subject to verification by ISACA international. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at www.isaca.org/chapters for other meeting locations.

Current field of employment (check one)

- 1 Financial
- 2 Banking
- 3 Insurance
- 4 Transportation
- 5 Retail & Wholesale
- 6 Government/National
- 7 Government/State/Local
- 8 Consulting
- 9 Education/Student
- 10 Education/Instructor
- 11 Public Accounting
- 12 Manufacturing
- 13 Mining/Construction/Petroleum
- 14 Utilities
- 15 Other Service Industry
- 16 Law
- 17 Health Care
- 99 Other _____

Level of education achieved

- (indicate degree achieved, or number of years of university education if degree not obtained)
- 1 One year or less
 - 2 Two years
 - 3 Three years
 - 4 Four years
 - 5 Five years
 - 6 Six years or more
 - 7 AS
 - 8 BS/BA
 - 9 MS/MBA/Masters
 - 10 Ph.D.
 - 99 Other _____

Certifications obtained (other than CISA/CISM)

- 1 CPA
- 2 CA
- 3 CIA
- 4 CBA
- 5 CCP
- 6 CSP
- 7 FCA
- 7 CFE
- 8 MA
- 9 FCPA
- 10 CFSA
- 11 CISSP
- 99 Other _____

Work experience

- (check the number of years of Information Systems work experience)
- 1 No experience
 - 2 1-3 years
 - 3 4-7 years
 - 4 8-9 years
 - 5 10-13 years
 - 6 14 years or more

Current professional activity (check one)

- 1 CEO
- 2 CFO
- 3 CIO/IS Director
- 4 Audit Director/General Auditor
- 5 IS Security Director
- 6 IS Audit Manager
- 7 IS Security Manager
- 8 IS Manager
- 9 IS Auditor
- 10 External Audit Partner/Manager
- 11 External Auditor
- 12 Internal Auditor
- 13 IS Security Staff
- 14 IS Consultant
- 15 IS Vendor/Supplier
- 16 IS Educator/Student
- 99 Other _____

Date of Birth _____
MONTH/DAY/YEAR

Payment due

- Association dues † \$ 120.00 (US)
 - Chapter dues (see reverse) \$ _____ (US)
 - New member processing fee \$ 30.00 (US)*
- PLEASE PAY THIS TOTAL \$ _____ (US)

† For student membership information please visit www.isaca.org/student

* Membership dues consist of association dues, chapter dues and new member processing fee. Join online and save US \$20.00.

Method of payment

- Check payable in US dollars, drawn on US bank
- Send invoice (Applications cannot be processed until dues payment is received.)
- MasterCard VISA American Express Diners Club

All payments by credit card will be processed in US dollars

ACCT # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

Cardholder billing address if different than address provided above:

By applying for membership in the Information Systems Audit and Control Association, members agree to hold the Association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the Association and the Institute as set forth in their respective bylaws, and they certify that they will abide by the Association's Code of Professional Ethics (www.isaca.org/ethics).

Initial payment entitles new members to membership beginning the first day of the month following the date payment is received by International Headquarters through the end of that year.

No rebate of dues is available upon early resignation of membership.

Contributions, dues or gifts to the Information Systems Audit and Control Association are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

Make checks payable to:

Information Systems Audit and Control Association

Mail your application and check to:

Information Systems Audit and Control Association
1055 Paysphere Circle
Chicago, IL 60674 USA
Phone: +1.847.253.1545 x475
Fax: +1.847.253.1443

US dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.

For current chapter dues, or if the amount is not listed below, please visit the web site www.isaca.org/chapdues or contact your local chapter at www.isaca.org/chapters.

Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues
ASIA			Kenya	158	\$40	New Jersey	30	\$40	Boise, ID	42	\$30
Hong Kong	64	\$40	Latvia	139	\$10	Central New York (Syracuse)	29	\$15	Willamette Valley, OR (Portland)	50	\$30
Bangalore, India	138	\$15	Lithuania	180	\$20	Hudson Valley, NY (Albany)	120	\$0	Utah (Salt Lake City)	04	\$30
Cochin, India	176	\$10	Netherlands	97	\$50	New York Metropolitan	10	\$50	Mt. Rainier, WA (Olympia)	129	\$20
Coimbatore, India	155	\$10	Lagos, Nigeria	149	\$20	Western New York (Buffalo)	46	\$30	Puget Sound, WA (Seattle)	35	\$25
Hyderabad, India	164	\$17	Norway	74	\$50	OCEANIA					
Kolkata, India	165	\$20	Warsaw, Poland	151	\$30	Harrisburg, PA	45	\$25	Adelaide, Australia	68	\$0
Chennai, India	99	\$10	Moscow, Russia	167	\$0	Lehigh Valley (Allentown, PA)	122	\$35	Brisbane, Australia	44	\$16
Mumbai, India	145	\$21	Romania	172	\$50	Philadelphia, PA	06	\$40	Canberra, Australia	92	\$0
New Delhi, India	140	\$15	Slovenia	137	\$50	Pittsburgh, PA	13	\$20	Melbourne, Australia	47	\$25
Pune, India	159	\$17	Slovak Republic	160	\$55	National Capital Area, DC	05	\$40	Perth, Australia	63	\$5
Indonesia	123	\$45	South Africa	130	\$35	Southeastern United States					
Nagoya, Japan	118	\$60	Barcelona, Spain	171	\$110	North Alabama (Birmingham)	65	\$30	Sydney, Australia	17	\$30
Osaka, Japan	103	\$85	Madrid, Spain	183	\$95	Jacksonville, FL	58	\$30	Auckland, New Zealand	84	\$30
Tokyo, Japan	89	\$100	Valencia, Spain	182	\$30	Central Florida (Orlando)	67	\$35	Wellington, New Zealand	73	\$24
Korea	107	\$30	Sweden	88	\$45	South Florida	33	\$40	Papua New Guinea	152	\$0
Lebanon	181	\$35	Switzerland	116	\$35	West Florida (Tampa)	41	\$35			
Malaysia	93	\$10	Tanzania	174	\$40	Atlanta, GA	39	\$35			
Muscat, Oman	168	\$40	London, UK	60	\$60	Charlotte, NC	51	\$35			
Karachi, Pakistan	148	\$15	Central UK	132	\$55	Research Triangle (Raleigh, NC)	59	\$25			
Manila, Philippines	136	\$20	Northern England, UK	111	\$50	Piedmont/Triad (Winston-Salem, NC)	128	\$0			
Jeddah, Saudi Arabia	163	\$0	Scotland, UK	175	\$45	South Carolina Midlands (Columbia, SC)	54	\$30			
Riyadh, Saudi Arabia	154	\$0	NORTH AMERICA			Memphis, TN	48	\$45			
Singapore	70	\$10	Canada			Middle Tennessee (Nashville)	102	\$45			
Sri Lanka	141	\$15	Calgary, AB	121	\$0	Virginia	22	\$30			
Taiwan	142	\$50	Edmonton, AB	131	\$25	Southwestern United States					
Bangkok, Thailand	109	\$10	Vancouver, BC	25	\$20	Central Arkansas (Little Rock)	82	\$60			
UAE	150	\$10	Victoria, BC	100	\$0	Central Mississippi (Jackson)	161	\$0			
			Winnipeg, MB	72	\$20	Denver, CO	16	\$40			
			Nova Scotia	105	\$0	Greater Kansas City, KS	87	\$0			
			Ottawa Valley, ON	32	\$10	Baton Rouge, LA	85	\$25			
			Toronto, ON	21	\$25	Greater New Orleans, LA	61	\$20			
			Montreal, PQ	36	\$20	St. Louis, MO	11	\$25			
			Quebec City, PQ	91	\$35	New Mexico (Albuquerque)	83	\$25			
			Islands			Central Oklahoma (OK City)	49	\$30			
			Bermuda	147	\$0	Tulsa, OK	34	\$25			
			Trinidad & Tobago	106	\$25	Austin, TX	20	\$25			
			Midwestern United States			Greater Houston Area, TX	09	\$40			
			Chicago, IL	02	\$50	North Texas (Dallas)	12	\$30			
			Illini (Springfield, IL)	77	\$30	San Antonio/So. Texas	81	\$25			
			Central Indiana (Indianapolis)	56	\$30	Western United States					
			Michiana (South Bend, IN)	127	\$25	Anchorage, AK	177	\$20			
			Iowa (Des Moines)	110	\$25	Phoenix, AZ	53	\$30			
			Kentuckiana (Louisville, KY)	37	\$30	Los Angeles, CA	01	\$25			
			Detroit, MI	08	\$35	Orange County, CA (Anaheim)	79	\$30			
			Western Michigan	38	\$25	Sacramento, CA	76	\$20			
			Minnesota	07	\$30	San Francisco, CA	15	\$45			
			Omaha, NE	23	\$30	San Diego, CA	19	\$25			
			Central Ohio (Columbus)	27	\$25	Silicon Valley, CA (Sunnyvale)	62	\$30			
			Greater Cincinnati, OH	03	\$20	Hawaii (Honolulu)	71	\$40			
			Northeast Ohio (Cleveland)	26	\$30						
			Kettle Moraine, WI (Milwaukee)	57	\$30						
			Quad Cities	169	\$0						
			Northeastern United States								
			Greater Hartford, CT	28	\$40						
			Central Maryland (Baltimore)	24	\$25						
			New England	18	\$25						

To receive your copy of the Information Systems Control Journal, please complete the following subscriber information:

Size of organization (at your primary place of business)

① Fewer than 50 employees
 ② 50-100 employees
 ③ 101-500 employees
 ④ More than 500 employees

Size of your professional audit staff (local office)

① 1 individual
 ② 2-5 individuals
 ③ 6-10 individuals
 ④ 11-25 individuals
 ⑤ More than 25 individuals

Your level of purchasing authority

① Recommend products/services
 ② Approve purchase
 ③ Recommend and approve purchase

Education courses attended annually (check one)

① None
 ② 1
 ③ 2-3
 ④ 4-5
 ⑤ More than 5

Conferences attended annually (check one)

① None
 ② 1
 ③ 2-3
 ④ 4-5
 ⑤ More than 5

Primary reason for joining the association (check one)

① Discounts on association products and services
 ② Subscription to *IS Control Journal*
 ③ Professional advancement/certification
 ④ Access to research, publications and education
 ⑤ Other _____

*Call chapter for information



Wireless LAN Risks and Vulnerabilities

by
Richard A. Stanley, Ph.D., PE, CISSP

Disclaimer

The Information Systems Audit and Control Foundation and the author of *Wireless LAN Risks and Vulnerabilities* have designed the white paper primarily as an educational resource for control professionals. ISACF makes no claim that use of this product will assure a successful outcome. The product should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed towards obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his or her own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2002 Information Systems Audit and Control Foundation. Reproduction for any purpose is not permitted without ISACF prior written permission. No other right or permission is granted with respect to this work. All rights reserved.

A scan of today's network marketplace indicates that wireless networking is ready for deployment in businesses, even in preference to the wired networks that are now commonplace. The ability to install a local area network (LAN) and to move network stations without the cost of installing or modifying cabling in already-built facilities is a major benefit of this technology. Since the mid-1990s, the technical standards underlying these networks have evolved from multiple proprietary specifications into a few generally agreed-upon international standards. This, in turn, has provided the ability to construct networks comprised of products from more than a single vendor. Network speeds have risen from a few hundred kilobits per second to several megabits per second, rates that are fully competitive with wired 10BaseT Ethernet networks. This has made use of wireless LANs (WLANs) by those traveling from place to place (often referred to in documents as itinerant or peripatetic users) not only possible but also feasible, and WLANs can now be found in many airport clubs, hotels and even Starbucks coffee shops.^{1,2} More importantly, WLANs are becoming common in business settings. Gartner Group predicts that by the end of 2002, 75 percent of American businesses will either have planned for or already installed wireless LANs.³ "The number of business wireless data users [is expected] to grow from 6.6 million at the end of 2001, to more than 39 million in 2006," according to InStat/MDR.⁴ This corresponds to a growth in WLAN equipment sales from US \$1.3 million to US \$3.5 billion over the period from the beginning of 2002 to the end of 2005, according to one study.⁵ Another study finds almost everywhere in the world except South America and Africa to be strong WLAN markets.⁶ One survey predicts that 21 million Americans will be using public WLANs by 2007, generating over US \$3 billion in revenue from services offered.⁷ In addition, there is little evidence that this growth is fueled by WLAN replacement of fixed facilities, but rather, by WLAN growth to extend fixed networks. By just about any measure, wireless LAN usage is growing at a rapid pace worldwide.

Wireless LANs, however, still have their problems. Connecting network elements by radio waves instead of wires presents many challenges. From the reliability standpoint, it is difficult to predict a priori the dependable coverage of a wireless network radio inside a building. This is largely because building construction varies widely, and things like steel beams and heavily plastered walls severely attenuate (weaken) radio waves. Even outside of structures, predicting coverage accurately and dependably is difficult, owing to radio propagation issues such as multipath fading, which are probabilistic and nondeterministic. (Multipath fading is defined in the glossary at the end of this paper.) Perhaps more troubling is that, by their very nature, wireless LANs broadcast their data into space, where they can be intercepted by anyone with the ability to listen in at the appropriate frequency. Worse, the very features that facilitate itinerant use of wireless LANs also enable interlopers to easily enter such networks with the same privileges as authorized users unless measures are taken to mitigate those threats.⁸ That presents a major security risk. In addition, although backbone speeds are comparable to 10BaseT Ethernet, they are still much slower than 100BaseT Fast Ethernet.

Not all networks, and certainly not all wired networks, are secure. Nor must all networks be secure. In the case of a local area network, operating over cables within a relatively secure physical perimeter, the level of security provided by the physical construction usually is sufficient. Adding wireless transmission, however, also adds vulnerabilities with which wired networks often are not required to cope, such as the need to authenticate every network user. To the extent that security is desired, the following characteristics must be provided, as they are required by the specific application:

- Confidentiality—Assurance that the message sent is readable only by the intended recipient (i.e., protection against interception, or eavesdropping)
- Authenticity—Assurance that the message originates from the claimed entity (i.e., protection against spoofing, or impersonation)
- Integrity—Assurance that the message has not changed in transmission (i.e., protection from transmission errors and/or willful modification of the message)
- Availability—Assurance that the data will be available to us when and where it is required (i.e., protection against denial of service or poor reliability)

This white paper provides an overview of how wireless LANs work, along with a review of the risks, vulnerabilities, and threats that affect wireless networks differently than their wired brethren.

Wireless LAN Technology

At root, all LANs are no more than radio networks. The signals traveling between the network stations are high-frequency signals in the range of 10 MHz to 300 MHz or higher. (Hertz [Hz] is defined in the glossary at the end of this paper.) What distinguishes wireless LANs from their wired kin is that wired networks attempt to confine these signals to cables and view signal emanation from the network cables as a problem. Wireless networks deliberately broadcast their data as radio waves and then receive them out of the air to complete the network connection. As with entertainment radio and television, it is not practical to broadcast the network baseband signals directly, so a process known as modulation impresses them onto another radio frequency known as the carrier. (Baseband signals and modulation are defined in the glossary at the end of this paper.)

The types of modulation used for wireless LANs fall into the category known as spread spectrum. Spread spectrum signals occupy a large portion of the assigned radio spectrum, rather than being narrowly centered on the carrier frequency, as is customary with radio and television stations. Military applications drove the development of spread spectrum technology. One advantage of spread spectrum is that it is more tolerant of interference from narrow-band signals (like those radio and television stations) than are narrow-band modulation techniques. This advantage is achieved at the cost of increased complexity. Fortunately, very large-scale integration (VLSI) integrated circuit technology makes it possible to realize a practical and affordable spread spectrum system on just a few, or even a single, integrated circuit.

There are two primary types of spread spectrum modulation used for current wireless LANs:⁹

- Frequency hopping spread spectrum (FHSS) is a system wherein the transmitter constantly changes frequency within an assigned range, remaining only a short time on each frequency visited. Clearly, the transmitter and receiver must shift frequencies (hop) in step, which requires that they share a key containing the hop sequence. US Federal Communications Commission rules require that, in the most-used bands, the hop sequence using channels spaced at 1 MHz intervals must cover at least 75 channels in the assigned band and not remain on any single channel for longer than 400 milliseconds in any 30-second period.¹⁰
- Direct sequence spread spectrum (DSSS) achieves the spreading of the signal by modulating the data with a key sequence known as the chipping code. The result of this operation is a signal spread across the desired frequency band, as is achieved with FHSS. DSSS can generally support higher data rates than FHSS and is more tolerant of many types of interference. Like FHSS, it requires that transmitter and receiver share a secret, in this case, the chipping code.

It is important to note that wireless networks, as a direct result of the type of modulation they employ, are private key (symmetric key) systems. All stations on a given network share a common key. This facilitates key distribution and management, but causes security problems.

A third type of modulation, orthogonal frequency division multiplexing (OFDM), is used by high-speed wireless LANs. In essence, OFDM involves splitting the input data into several parallel streams, modulating each stream onto a separate carrier frequency, then demodulating all the carriers at the distant end and recombining the data into a replica of the original. Each of these streams is modulated onto the carrier using one of the spread spectrum techniques.

At the time this paper was written, available and planned wireless LANs operate in one of three radio bands designated as industrial, scientific and medical (ISM). These bands are located at 900 MHz (902-928 MHz), 2.4 GHz (2400-2483.5 MHz) and 5.8 GHz (5725-5850 MHz).¹¹ Commonly used devices that

also operate in these bands are microwave ovens (in the 2.4 GHz band) and cordless telephones (in both the 900 MHz and 2.4 GHz bands). The 5.8 GHz band is not yet in wide use, but that is expected to change before long, if only because of the growing congestion of the 2.4 GHz band.¹² However, much of the 5.8 GHz band is subject to increased regulation, as compared to the lower frequency bands. The attraction of the ISM bands is that under Part 15 of the FCC Rules, the equipment operator requires no license to operate radio equipment at those frequencies.¹³ The only requirement is that the equipment has been certified by the manufacturer to the licensing authority (a government agency, such as the FCC in the US, the Register of Radio Frequencies in New Zealand, the Post and Telecommunications authority in Japan, Industry Canada in Canada and many other nations, etc.) as meeting the technical requirements established by the agency for operation within the ISM band. Those requirements include specifying modulation type, power output and assurance that the device does not put the operator at risk.

This attraction has an ugly side, however. Equipment that operates under the Part 15 Rules must share this spectrum on a noninterference basis with licensed users in the same band.¹⁴ Simply put, wireless LANs must not cause interference to licensed users in the ISM frequency band and must accept any interference they encounter. Governments in most of the world have provided for this sort of usage to allow people to buy and use devices such as microwave ovens and cordless telephones without having to apply for and obtain a radio operator’s permit from the radio licensing authority. Although unlicensed operation has been a boon for consumer electronics, it presents to the equipment manufacturers a significant design and operational challenge, which is complicated by the fact that the Part 15 rules make no effort to separate users of this band by the power output of the devices used. Permitted power levels range from as much as one watt to only a few milliwatts.¹⁵ It is a testament to the state of modern technology that these systems operate at all, much less at high data rates in critical applications.

A recent alternative is the addition of an Unlicensed National Information Infrastructure (UNII) 5 GHz band, which supports high data rates and promises less interference than the ISM bands. As implemented in the US, the UNII band consists of two bands—one extending from 5.15 to 5.35 GHz and the second extending between 5.725 and 5.825 GHz.¹⁶ Within the UNII bands, devices are segregated into sub bands, largely on the basis of output power.¹⁷ This is a much better arrangement than the “wild west” that has developed in the other Part 15 unlicensed bands and should make the deployment of future wireless LANs somewhat more straightforward. The regulations also require that the usage of the UNII band be restricted to high data rate devices, which should prevent the migration of cordless telephones, infant monitors, microwave ovens, etc., into the new band.¹⁸ What these regulations will not do, however, is eliminate the problem of interference or the inability to operate the WLAN in a protected, licensed frequency band.

Complicating the picture somewhat is the fact that UNII band implementation is not uniform. In Europe the entire band from 5.15 to 5.825 GHz is available; in the US and Japan, only portions of this spectrum are assigned to UNII devices. **Table 1** illustrates the band structure and power level assignments in those regions of the world.¹⁹ (In **table 1**, EIRP refers to Effective Isotropic Radiated Power, which is simply a measure of the power leaving the antenna as compared to a point source that radiates in all directions at once.) A quick review of **table 1** reveals that the selections for powers in the sub bands are not congruent. In particular, the power restrictions on the highest of the UNII sub bands in the US and Europe are diametrically opposed. In the US, this band is reserved for the highest power output devices; in Europe, it is for the lowest power devices. This dichotomy will make it difficult for manufacturers to develop a single product that is usable out of the box in any of the markets, except in the 5.15-5.25 GHz sub band. As a result, one may expect the initial UNII deployments to migrate to this band with concomitant interference problems.

Table 1—UNII Bands and Permitted Powers, by Region

	5.15-5.25 GHz	5.25-5.35 GHz	5.470-5.725 GHz	5.725-5.825 GHz
--	---------------	---------------	-----------------	-----------------

Europe	200 mW (EIRP)	200 mW (EIRP)	1 W (EIRP)	25 mW (EIRP)
US	50 mW (max) 200 mW (EIRP)	250 mW (max) 1 W (EIRP)	Not available	1 W (max) 4 W or 200 W (EIRP)
Japan	200 mW (EIRP)	Not available	Not available	Not available

Like cordless telephones, wireless LANs are used primarily as extensions of fixed, wired networks. WLANs are connected to the fixed network by means of an access point, which functions as a bridge between the fixed and wireless portions of the network. An access point is essentially a radio transmitter/receiver combined with a network bridge. Although wireless LANs are basically Ethernets, another protocol suite is required to ensure interoperability, as the Ethernet standards (more correctly, the Institute of Electrical and Electronics Engineers [IEEE] 802.3 standard commonly referred to as Ethernet; the standard for true Ethernet is 802.2, although it is relatively unused now) require a wired network.

Table 2 shows the predominant wireless LAN standards. It is important to note that the 802.11 standards family basically adds wireless functionality to the protocol structure of 802.3; it does not develop a new network layer protocol. For this reason, the 802.11 standards are sometimes called wireless Ethernet.

Bluetooth is included in **table 2** for the sake of completeness, as it is receiving much attention in both the trade and popular press. Bluetooth, however, is essentially a protocol developed to replace wires in local digital device interconnections, such as, the link between the computer and a printer, but it is not a comparable networking protocol to the 802.11 series. Bluetooth is, rather, “a global de facto standard for wireless connectivity.”²⁰ Nevertheless, Bluetooth devices operating in the 2.4 GHz band will be sources of interference to other networks in that band, and vice versa. The rapid population of the 2.4 GHz band will almost certainly drive the WLAN market to the UNII bands sooner rather than later, assisted by the rapidly falling costs of operating at those frequencies.

Table 2—Most Common Wireless Local Area Network Standards

Protocol	Author	Frequency	Modulation	Data Rate	Comments
802.11	IEEE	900 MHz ISM	FHSS	~ 300 Kbps	Original standard of the series <i>Obsolescent</i>
802.11a	IEEE	5 GHz UNII	OFDM	Up to 54 Mbps	Emerging Standard Not backward compatible with 802.11
802.11b	IEEE	2.4 GHz ISM, 900MHz legacy	DSSS FHSS legacy	1 to 11 Mbps	Most popular as of this writing
802.11e	IEEE	5 GHz UNII	OFDM	Up to 54 Mbps	Adds QoS capability to 802.11h <i>(Not yet available)</i>
802.11g	IEEE	2.4 GHz ISM,	DSSS FHSS	Up to 54 Mbps	Intended to maintain backward compatibility with 802.11b. <i>(Not yet available)</i> expected to be ratified third quarter 2002)
802.11h	IEEE	5 GHz UNII	OFDM	Up to 54 Mbps	Adds transmit power control dynamic freq. selection to 802.11a, to counter EU area interference issues
802.11i	IEEE	5 GHz UNII	OFDM	54 Mbps or	Intended to specifically

Wireless LAN Risks and Vulnerabilities

				beyond	include security and authentication (<i>In process; probably years in future</i>)
802.11j (5UP-2003)	IEEE, ETSI ²¹	5 GHz UNII	OFDM, GMSK	54 Mbps or beyond	Effort to converge 802.11 and HiperLAN standards to permit interoperation in the 5 GHz band. ²² (<i>Committee forming</i>)
HiperLAN	ETSI	5.15-5.30 GHz or 17.1-17.3 GHz	GMSK	23.529 Mbps	European Community backed standard, expected to appear by mid-2002
HiperLAN/2	ETSI	5.15-5.30 GHz or 17.1-17.3 GHz	GMSK	54 Mbps	European Community developed standard, expected to appear in 2002
HomeRF™	HomeRF™ Industry group	2.4 GHz	FHSS	Up to 10 Mbps	Integrated voice, data and entertainment for home networking
Bluetooth	Bluetooth Consortium	2.4 GHz	FHSS	1 Mbps	Cable replacement, not comparable to 802.11 or HiperLAN

The other major WLAN standards issue is the perennial difference in approach to standards development in North America and the European Union. The benefit from these differing approaches is a healthy competition that tends to bring the best products to market. The downside is that when the resulting standards are incompatible, higher end user costs result because of market fragmentation. The existing standards for WLANs within the European community are HiperLAN and HiperLAN/2, summarized in **table 2**. It can be argued that the ETSI HiperLAN standards are technically superior to 802.11, but the 802.11 family market share continues to grow, possibly owing to the 5 to 15 percent price premium for HiperLAN/2. The IEEE has introduced a new variant of 802.11a, named 802.11h, which adds transmit power control (TPC) and dynamic frequency selection (DFS) to the 802.11a standard to deal with particular interference problems found in Europe, where the 5 GHz band is shared with defense establishment and NATO radars and satellites.²³ At least one vendor, Philips, has decided that the future lies with the 802.11h standard, and is tooling its silicon foundry to produce chips solely to implement that standard, to the exclusion of HiperLAN.²⁴ However, IEEE and ETSI have established a working group (called 802.11j or 5UP, respectively) to harmonize the 802.11 5GHz standards with HiperLAN/2, to permit both to interoperate in the 5GHz band. If this effort succeeds, it should significantly reduce end-user equipment prices and make worldwide WLAN interoperation feasible.

There are still issues with interoperability among devices of different makes that implement the same technical standard, but these are slowly being resolved as a result of market pressures. However, it is important to note that with the exception of backward compatibility from 802.11b to 802.11, devices using the standards above are noninteroperable (802.11a and 802.11h interoperability is yet to be resolved). Caution should also be exercised when mixing hardware from different manufacturers. As in many cases where devices are built to an open standard, some vendors have implemented the standard with added features that may require adjustment to achieve interoperation with devices of other manufacturers. However, the existence of a body of WLAN standards has enabled the design and deployment of practical networks with reasonably predictable results. This was not the case as recently as

the mid-1990s; when systems built to mutually incompatible proprietary standards were the only choice for would-be wireless LAN designers.

Wireless LAN Vulnerabilities and Risks

In addition to all the vulnerabilities common to wired networks, wireless LANs introduce a new series of risks. The critical vulnerabilities are eavesdropping, illicit entry into the network (enabled by a failure of user authentication) and denial of service. The basic IEEE 802.3 Ethernet protocol that underlies the 802.11 standards does a reasonable job of ensuring data integrity using a 4-byte Cyclic Redundancy Check (CRC) computed over the data. But as the data on wireless networks is exposed to outsiders, true network security argues for cryptographic integrity checks. Another risk is some users may perceive they are at risk from being exposed to radio wave energy, but there is no credible research supporting this thesis, and Part 15 certification requires that devices meet the government standard for exposure to radio emissions. This topic will not be considered further here, but will be discussed in additional detail in the wireless LAN technical perspective that is being developed by ISACF research.

Because it is by far the most popular wireless LAN standard at this time, the following discussion will be limited to the variants of the IEEE 802.11 standard. The specifics related to vulnerabilities and performance discussed herein are pertinent only to the 802.11 series of networks, while the modalities of risk are the same for all types of wireless LANs. In other words, all wireless LANs face the same population of risks to message confidentiality, integrity, authenticity and denial of service as are faced by the 802.11 series. Only the technical details of vulnerabilities and dealing with the threats differ from standard to standard.

Eavesdropping (Compromising Confidentiality)

By their nature, wireless LANs intentionally radiate network traffic into space. Once that is done, it is impossible to control who can receive the signals. So it must be assumed in any wireless LAN installation that the network traffic is subject to interception and eavesdropping by third parties. The obvious solution to this problem is to encrypt the data stream, and the 802.11 standards provide for doing that. Unfortunately, the implementation of this solution is less than perfect.

To provide security on wireless LANs, the 802.11 standards (other than the original) provide for wired equivalent privacy (WEP). Basic WEP uses 40-bit static keys and RC4 encryption.²⁵ There are several problems with the implementation of this approach. First, WEP is an option. It is not activated by default in shipped products, and it reduces raw throughput by as much as 50 percent. Furthermore, it is widely believed that many network administrators are unaware the feature even exists. Consequently, most operating networks have not enabled WEP.²⁶ In such a situation, the network is broadcasting all traffic in the clear for the benefit of all who can intercept it. Moreover, it broadcasts a beacon that announces its presence, so those itinerant WLAN users can find the access point and connect to the network. That is one of the most attractive features of wireless networks—they facilitate rapid communications by highly mobile users. However, this is hardly a secure mode of operation. Worse, it turns out that WEP itself is fatally flawed.

The WEP approach to cryptography sounds secure: WEP encrypts every packet with a different key. However, WEP does not properly implement the RC4 initialization vector. Instead it uses a straightforward and predictable approach to incrementing the vector from one packet to the next. Coupled with weak key scheduling and a restricted key space, WEP is demonstrably insecure. Early in 2001, researchers at the University of California, Berkeley, USA, provided theoretical proof that the WEP security scheme could be broken.²⁷ Recent efforts by other researchers using those techniques succeeded in breaking the key on an actual network in a few hours the first time they tried, and in much less time on subsequent attempts.²⁸ One group was able to break the network key in less than 15 minutes and also demonstrated that the work factor to break the key scales linearly.²⁹ Although the 802.11a protocol allows

for keys up to 152 bits long,³⁰ the practical effect of the discovery about linear scaling of the work factor is that simply expanding the key to 152 bits will not notably improve the situation. At best, it might then take an hour to recover the network key. Researchers have also shown that it is possible to listen to packets, inject packets and alter packets on wireless LANs using WEP.³¹ As if these findings were not troubling enough, the WEP password scheme has also been found to be flawed, with the result that an intruder can gain access to some WEP-protected networks in as little as 30 seconds.³²

The root cause of this problem has been reported as being solely the RC4 encryption scheme. However, a more accurate description is that WEP was created without a thorough understanding and public review of the cryptographic primitives that were combined to create WEP. Also, many of the things that would enhance the security of WEP—such as changing the initialization vector after every packet—are merely recommendations in the standard and not requirements.³³ The WEP standard does not even address the issue of key management.

WEP is expected to perform several security functions simultaneously: authentication, integrity and confidentiality.³⁴ Unfortunately, the result is that WEP alone—as it exists at this writing—cannot be relied upon to secure the wireless network.

The proposed, quick fix to the WEP security problem “...uses a technique called fast-packet keying to rapidly generate unique encryption keys for each data packet transmitted.”³⁵ However, this change to the algorithm merely makes it somewhat harder for eavesdroppers to determine the keys; it does not make it impossible. Thus, the fast packet keying approach must be viewed only as a stopgap measure.

The IEEE has proposed an updated standard, WEP2, to address the WEP shortcomings. WEP2 uses 128-bit encryption and a 128-bit initialization vector. However, it still relies on RC4 encryption and is still assessed as being vulnerable to the attacks described above.³⁶ One of the authors of the RSA public key encryption algorithm, Ron Rivest, has stated, “Those who are using the RC4-based WEP or WEP2 protocols to provide confidentiality of their 802.11 communications should consider these protocols to be broken ...”³⁷ The IEEE has further undertaken to define an enhanced security network standard that will use the newly adopted Advanced Encryption Standard (AES),³⁸ which replaces the Digital Encryption Standard (DES)³⁹ in use since the mid-1970s. However, this new standard is unlikely to debut in many commercial products before late 2002 and compatibility issues remain.⁴⁰

There clearly are technologies that can be employed to provide cryptographic level confidentiality beyond what is offered by WEP.⁴¹ The researchers, who broke WEP recommend treating all wireless networks as being outside the firewall and using higher-level protocols, such as SSH or IPSec, to provide security. Another approach is an overlaid proprietary cryptographic schema based on the MD5 algorithm from NextComm.⁴² Yet another way is to establish a virtual private network (VPN) connection between the wireless client and the wired network server to which it is connecting. There will doubtless be other approaches in the near future. The problem is that these further reduce throughput, increase complexity, potentially add proprietary hardware and/or software and reduce ease of network use for the end users.

In the midst of all this dreary news about wireless security, one should realize that absolute security was never the goal of WEP. Of course, absolute security is impossible. The goal of WEP was to provide a level of security commensurate with that found on wired LANs. One can argue that, despite its cryptographic problems, WEP has achieved that goal. Wired networks are not generally very secure unless protected by measures beyond those provided by the network layer protocols. Many people have surreptitiously connected a computer to a wired LAN and have been able, as a result, to access resources to which they had no right.⁴³ This is a common problem, usually controlled by limiting which computers may connect to the wired LAN. That limitation is more often than not enforced by physical access restrictions. However, in the wireless domain, it is more difficult to limit who can connect to the LAN, so

WEP—despite its shortcomings—is an important tool in the overall management of network security. It is simply not a sufficient tool, as the above discussion illustrates.

Message Integrity

Another function of WEP within the 802.11 framework is to ensure message integrity. This is accomplished by computing a 32-bit long CRC over the packet data. The CRC is added to the end of the data, and the result is encrypted using the RC4 algorithm. The output of this process is added bit by bit to the plaintext message and the CRC. The initialization vector is then added to the data stream ahead of this encrypted output to produce the data that is transmitted over the radio link. The security of this method rests solely with the security of the secret key. This is typical of modern cryptographic systems that conform to Kerckhoff's assumption.⁴⁴ Unfortunately, this specific algorithm has problems that compromise its security.

First, if an attacker is able to find two identical messages enciphered with the same initialization vector and secret key, the then adding those two messages together bit by bit will cancel out the enciphered keystream component. Since most IP messages contain highly predictable portions, this line of attack enables an intruder to gain substantial knowledge about the messages. Put differently, the system is vulnerable to a known plaintext attack. A known plaintext attack is not so difficult to arrange; the attacker need only send an e-mail to a client on the wireless network and then wait for the client to read the e-mail using WEP.⁴⁵

Second, the CRC check performed on the data is not a hash function. Hash functions are especially constructed so that it is computationally infeasible, knowing the hash value of some data, x , to find some other data, y , that produces the same hash output. Conversely, a CRC algorithm is deterministic and it is not too difficult to construct a data stream that is different from the original but will produce the same CRC result. When such a modification is made, it is impossible by using a CRC check to determine that the message has been altered, as both the original message and the altered message have the same CRC result.

Finally, the initialization vector is only 24 bits long, which means that it must repeat every 2^{24} packets (less than 16.8 million packets or about half a day's traffic on a busy 5 Mbps network). This in turn provides yet another chance for attackers to ferret out details of the messages and offers the opportunity to alter messages without that alteration being detected. That constitutes a major failure of any integrity-checking scheme.

As a result, although WEP purports to provide data integrity checking for wireless packets, it does not do an adequate job of it.

Illicit Entry into the Network (Exploiting Poor Authentication)

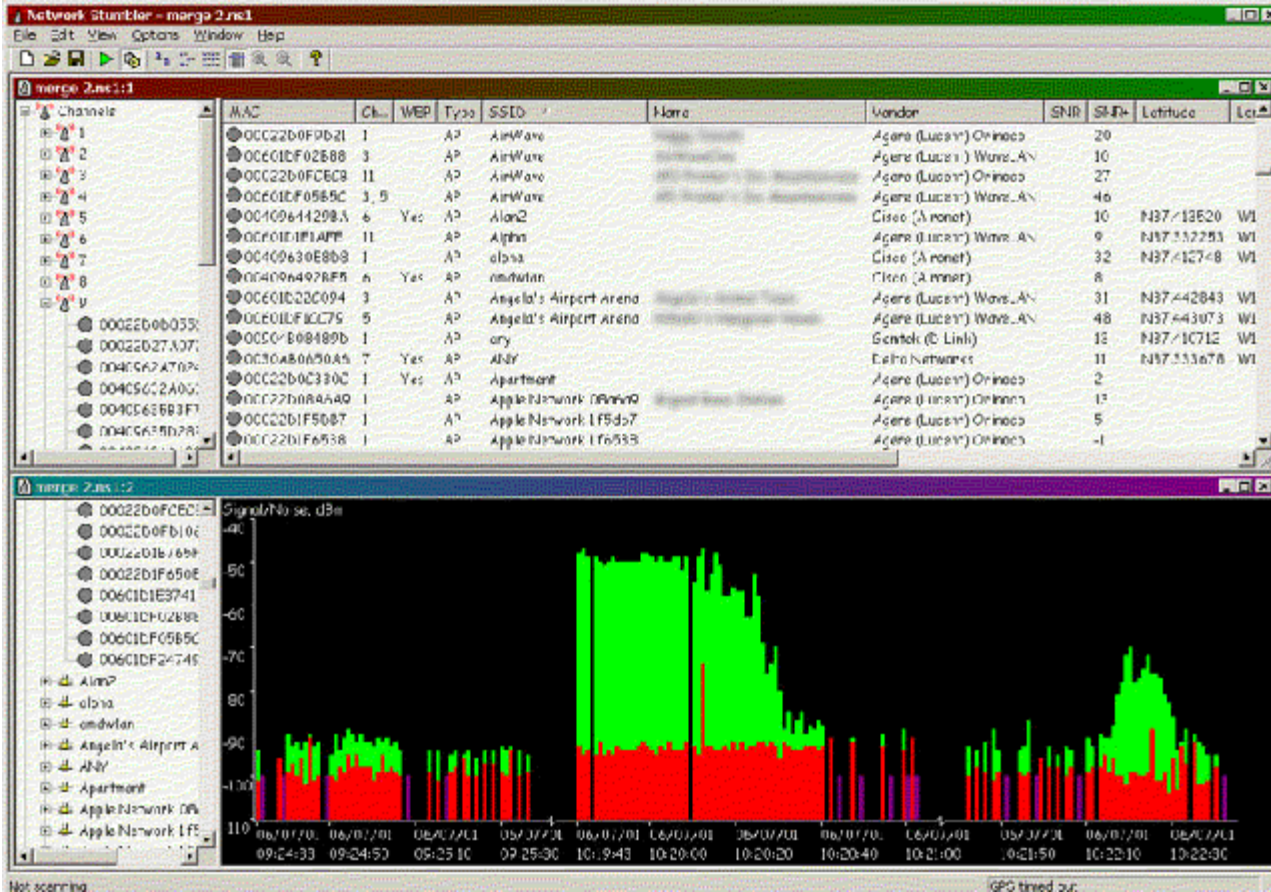
Wireless LANs could be used only to network fixed computers, thereby avoiding the costs of cabling. Usually, however, they are used to interconnect highly mobile user populations provisioned with laptop computers, PDAs and other mobile devices. WEP is intended to ensure the authenticity of network users by rejecting non-WEP packets. But the very nature of the wireless protocol is to make the network user friendly by facilitating connection to an access point—and thus the entire network—as the user moves about. Access points, unless configured to do otherwise, broadcast a beacon signal that announces their availability to potential users. If the beacon did not exist, it would not be nearly as straightforward for users to connect to a network. This is analogous to the cellular telephone network. The cellular network would not be nearly as useful as it is if users could not move about freely in both their home areas and away from home. However, it was not until after suffering high financial losses directly attributable to poor authentication in the cellular protocols that the industry adopted strong cryptographic authentication for cell phones. Unfortunately, the wireless LANs many find so useful have a major security hole,

because they have weak authentication. Weak authentication provides a way for unauthorized users to enter the network.

Wireless network equipment, as configured out of the box, is generally set so that the network name is a default name for public access, and all network interface cards that conform to the standard of the network (e.g., 802.11b) can readily connect to the system. Furthermore, equipment from most vendors broadcasts its IP address by default.⁴⁶ Few network administrators bother to change the level of access to something more restrictive than the default. As a result, the wireless access point advertises its address and its network name, so that when a wireless client senses the access point, the client will attempt to connect to the network. Unless the ability for clients to connect is somehow restricted (such as by MAC address—discussed at the end of this section), the connection attempt will succeed, and another user will be added to those already supported. As wireless LANs primarily serve to extend wired networks, the view this newcomer has of the network may be quite extensive, and the resources available may include many not intended for casual visitors. As discussed above, this is virtually identical to the situation with wired networks. The difference is that one must gain physical access to a wired network to connect to it. With a wireless LAN, one only has to be in the vicinity. As it happens, the vicinity may cover a rather large area.

Depending on the structural elements in the path, a wireless LAN signal may be usable for distances of approximately 500 meters. While this is helpful from a coverage standpoint, it is not helpful from a security standpoint. Using directional antennas, one can detect wireless network signals at distances up to eight miles (12.8 km) from the network node.⁴⁷ In such a situation, someone can connect to the network from outside the perimeter of the place of business, and probably without the organization's knowledge. The ability of unauthorized users to join wireless networks without detection has been demonstrated repeatedly, and has even appeared in the mainstream media.⁴⁸ One researcher has stated publicly that, “[h]ackers can travel the entire length of Market Street in San Francisco ‘and basically not lose 802.11 coverage’ while picking up wireless LAN signals in their cars.”⁴⁹ Software, such as NetStumbler,⁵⁰ which is freely available on the Internet readily turns a laptop computer with a wireless network card into a tool that detects wireless networks, presents the user with the network identification and information about encryption being used, and then allows the user to log into unprotected wireless networks. One self-described “drive-by hacker” found that between Pasadena and San Francisco, California, USA, fewer than half of the wireless networks he detected even had WEP enabled.⁵¹ **Figure 1** shows a screenshot of a NetStumbler data collection session that includes location detail produced by linking NetStumbler with a global positioning system (GPS) receiver.⁵² Note the level of detail available about the networks intercepted. This provides a would-be interloper with all the information necessary to enter the network illicitly. Notice also that only 25 percent (4 of 16) of the networks shown on the screenshot have WEP enabled. WEP, imperfect though it is, cannot provide any security at all if it is shut off.

Figure 1—NetStumbler Screen Shot Showing Details of Intercepted WLANs



Large networks that cater to highly mobile users are more or less forced to accept the poor authentication provided by WEP. It would not do if one had to register in advance to use a network in a public airport space, for instance. However, smaller networks have an option that can help. It is possible to restrict access to the network to those network nodes whose MAC (media access control) addresses are known in advance by the access point. For a small wireless network with a stable user population, this is an attractive option. Although this will make it harder for interlopers to join the network, it will remain possible. Moreover, it will do nothing about the eavesdropping risk.

Not mentioned previously is perhaps the largest risk to network integrity. If a legitimate user loses a network card, either by carelessness or through theft, the entire network cryptographic system has been compromised and new keys must be provisioned immediately for all remaining legitimate users. This is logistically a daunting task. Furthermore, it is highly likely that the lost network card will not be reported in a timely manner because either its loss is not discovered in a timely manner or the user is embarrassed by the loss and spends time searching for the card in the hope that it was merely misplaced.

A WEP Solution?

In an attempt to deal with the shortcomings of WEP, some WLAN vendors have embraced the 802.1x Extensible Authentication Protocol (EAP) and the Remote Access Dial-In User Protocol (RADIUS).⁵³ RADIUS is already used by many corporations to provide strong authentication for users who access the network over dial-up or Internet connections while they are on business travel or otherwise from their home network connection. This solution claims to provide the following features:⁵⁴

- Unique encryption keys for each user and each communications session, rather than the common key used across the network by WEP
- Key renewal on a periodic basis, as is done with high-security government communications links
- Authentication of users rather than authentication of the network access device
- Centralized authentication and key renewal
- Mutual authentication between client and authentication agent

The proponents of this approach—such as Cisco, Agere and LXE—maintain that implementing the combination of dynamic WEP and EAP would produce a computationally secure wireless LAN cryptosystem that would defeat all known attacks against WEP, comply with existing standards and not significantly affect network throughput. It appears that CiscoSecure ACS 2.6 for Windows 2000 and NT implements this approach successfully.⁵⁵

Denial of Service (Attacking Network Availability)

A denial-of-service (DoS) attack is one wherein the attacker attempts to render the target network unable to serve its legitimate users. In the wired domain, protocol-based attacks such as SYN flooding and the Ping of Death, which seek to overwhelm the target network with traffic and force the network servers to crash, have become customary. This type of attack is also effective against wireless networks.

In addition to protocol-based DoS attacks, wireless networks are vulnerable to a denial-of-service attack that is not viable against their wired brethren. Because their signals must travel through the public airwaves rather than in protected cables, wireless networks are extremely susceptible to radio interference, either deliberate or accidental. Accidental interference occurs all too often, owing to the shared, unlicensed nature of the bands in which these networks operate. It is common for a wireless network, or a portion of it, to become unusable when a cordless telephone is operating in the same radio band and in physical proximity to the wireless node. It is also common for one wireless network to interfere with another close by, frequently rendering both useless.

Deliberate jamming attacks are not yet as common as accidental interference, but they are certainly straightforward. All that is needed is to set up a transmitter covering the band where the wireless LAN operates and ensure that the transmitter has sufficient power to overwhelm the relatively weak LAN nodes. As it happens, the most ubiquitous occupant of the 2.4 GHz ISM band is the microwave oven. Microwave ovens are supposed to operate at a single frequency in that band, but their frequency stability is poor. A devious user can make the frequency stability deliberately worse, so that the oven frequency covers many of the channels assigned for use by the wireless LAN. Wireless network nodes operate at power outputs of no more than a watt, and usually less. With minor modification, the typical microwave oven—which operates at power output levels of around 600 watts—can become a practical jammer for wireless LANs operating at levels of tens or hundreds of milliwatts. When designing a wireless LAN, the involvement of a competent radio engineer to do a survey of existing signals in the frequency band of interest and assessing the likelihood of physically introducing jammers into the vicinity is usually money well spent. Periodic resurveys are also a wise precaution. Wireless LAN users must be sensitive to the potential for both deliberate and accidental interference and have a plan for dealing with the interruptions this may cause.

Battery exhaustion in the portable wireless clients is another means of denying service. This can be forced by placing software in the client that disables or otherwise interferes with the power management functions. In turn, such disruption can cause the device to drain its battery much faster than anticipated, with the result that the user is stranded, out of touch with the network and away from a convenient charging location. This type of attack is difficult to discern from a simple case of a dying battery or a user who did not pay sufficient attention to charging protocols before setting out on their journey. It is thus a tempting attack for one who wishes not to be discovered. For those users whose WLANs must operate

irrespective of external problems, such as emergency services, serious consideration should be given to providing backup to the main power used to power the wired network and the wireless access points, and to charge the portable unit batteries.

Summary

It is impossible in a white paper of this length to exhaustively cover all the risks and vulnerabilities pertaining to wireless LANs. The most severe and most common vulnerabilities have been covered, namely eavesdropping, faulty message integrity, illicit entry of outsiders into the network and radio interference—both accidental and deliberate.

Protecting a wireless network requires forethought and planning, just as protecting a wired network does. Among the key protective measures to be undertaken are:

- Do not rely on WEP alone to provide security for the network.
- Limit, as much as is possible, who can attach to your network.
- Survey the interference and jamming environment for a planned wireless LAN before it is installed, and continuously monitor the environment after installation.

By understanding and dealing properly with the risks and threats unique to the wireless domain, a wireless LAN can be a valuable, and appropriately secure, addition to a wired enterprise network. ISACF is currently conducting a research project on wireless communications. Because wireless communications transcend traditional and regulatory boundaries, they pose significant technical challenges, as well as greater challenges in the areas of control, security, and audit. This project will provide both a technical and functional assessment and will be written from a business and risk management perspective. Completion is scheduled for September 2002.

End Notes

¹ Marsan, Carolyn Duffy, "Starbucks wireless network a sweet deal for MobileStar," *Network World*, 25 June 2001

² Meeks, Fleming, "The Next Big Thing," *Barrons*, Vol. LXXXI, No. 46 (12 November 2001), pp. 29-30

³ "Services Web et 802.11: conjonction favorable," *LeMonde Informatique*, No. 932, 29 March 2002

⁴ "Wireless Data Services Grows Despite Industry Downturn," *CommWeb.com*, 6 March 2002

⁵ Hilton, Isaac, "Beware the Expanding WLAN," *CommWeb.com*, 10 December 2001

⁶ Cahners In-Stat Staff writer, "Business WLAN market exceeds expectations in 2001," January/February 2002

⁷ "Public Wireless LAN Access: US Market Forecasts 2002-2007"

⁸ Gomes, Lee, "Many wireless networks open to attack," *The Wall Street Journal Online*, 27 April 2001

⁹ Williams, Gerald, op. cit.

¹⁰ Code of Federal Regulations, Title 47, Section 15.247(a)(1)(iii), United States Government Printing Office, Revised as of 1 October 2000. [Citation: 47 CFR § 15.247(a)(1)(iii)]

¹¹ 47 CFR § 15.247

¹² Cox, John, "High-speed wireless LANs are coming," *Network World*, 9 April 2001

¹³ 47 CFR § 15.1

¹⁴ 47 CFR § 15.247(h)

¹⁵ 47 CFR § 15.247(b)(1)

¹⁶ 47 CFR § 15.403(i)

¹⁷ 47 CFR § 15.407(a)

¹⁸ James C. Chen, "Wireless LANs Move to 5 GHz," *EE Times*, 5 January 2002

¹⁹ Ibid.

²⁰ "What is Bluetooth," *Nokia and Bluetooth*, www.nokia.com/bluetooth/whatis.html

²¹ European Telecommunications Standards Institute (ETSI)

²² "Etat des travaux de l'IEEE sur les normes issues de 802.11," *Fondation Internet Nouvelle Génération*, Paris,

France, 13 Dec 2001

- ²³ Joris Evers, “Too Many Standards Spoil Wireless LAN Soup,” *IDG News Service*, 2 January 2002
- ²⁴ Nolan Fell, “Philips Sees No Future in HiperLAN/2 chips,” *EE Times UK*, 29 October 2001
- ²⁵ Andrew Garcia, “WEP Remains Vulnerable,” *eWEEK*, 26 March 2001
- ²⁶ Wes Simonds, “Bad Packets: WLAN In, WEP Out,” *SearchNetworking*, 17 September 2001
- ²⁷ S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” *Eighth Annual Workshop on Selected Areas in Cryptography*, August 2001
- ²⁸ Adam Stubblefield, John Ioannidis, Aviel D. Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP,” AT&T Labs - Research, Florham Park, NJ, USA, 6 August 2001
- ²⁹ Patrick Mannion, “Cipher attack delivers heavy blow to WLAN security,” *EE Times*, 6 August 2001
- ³⁰ John Taschek, “Is 802.11a Dead Before It Even Begins?” *eWeek*, 9 February 2002
- ³¹ Dan Verton, “Flaws in Wireless Security Detailed,” *Computerworld*, 16 July 2001
- ³² Robert Lemos, “Wireless Networks Wide Open to Hackers,” CNET News.com, 12 July 2001
- ³³ Larry Loeb, “What’s Up with WEP?” *IBM developerWorks*, April 2001
- ³⁴ Simonds, op. cit.
- ³⁵ Peter Sayer, “Wireless LAN Security Fix on Tap from IEEE group,” *Network World*, 7 January 2002
- ³⁶ Dan Verton and Bob Brewin, “New Wireless LAN Vulnerabilities Uncovered,” *Computerworld*, 9 August 2001
- ³⁷ R. Rivest, “RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4,” www.rsa.com/rsalabs/technotes/wep.html, 2001
- ³⁸ US National Institute of Standards and Technology, FIPS PUB 197
- ³⁹ US National Institute of Standards and Technology, FIPS PUB 46-3
- ⁴⁰ Garcia, op. cit.
- ⁴¹ Brian Fonseca and Ephraim Schwartz, “Guardent, SafeNet Respond to WLAN Security Hole,” *Infoworld*, 20 August 2001
- ⁴² Ted Stevenson, “New Encryption Technology Closes WLAN Security Loopholes,” *Internet News*, 13 September 2001
- ⁴³ Larry Mittag, “Hacker’s Delight,” *Communication Systems Design*, 2 April 2001
- ⁴⁴ Bruce Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996, p. 7
- ⁴⁵ Loeb, op. cit.
- ⁴⁶ Jacqueline Emigh, “Driveby Hacking on the Go,” *CIO Information Network*, 8 January 2002
- ⁴⁷ Verton, op. cit.
- ⁴⁸ Nikita Borisov, “Intercepting Mobile Communications: The Insecurity of 802.11,” University of California Berkeley, 2001
- ⁴⁹ Verton, op. cit.
- ⁵⁰ www.netstumbler.com
- ⁵¹ Emigh, op. cit.
- ⁵² home.pacbell.net/mariusm/
- ⁵³ IETF RFC 2865
- ⁵⁴ Dick Sorenson, “Wireless Insecurity,” *isitWireless.com*, 9 February 2002.
- ⁵⁵ Jim Warner, e-mail “Re: LEAP/RADIUS Authentication with Dynamic WEP,” warner@cats.UCSC.EDU, 20 April 2001 18:16:04

Glossary

Baseband Signals—All communication begins with a signal that the communicators can understand naturally. When speaking, people use a signal—their voice—that other humans can understand. If speech needs to travel over a long distance, they must find a way to impress it onto a radio wave, for example, and then remove it from the radio wave at the distant end. This is done because radio waves can travel longer distances than can voices. A similar problem exists with networks. The natural network signals, or baseband signals, are radio signals of relatively low frequency. To be useful for wireless networking, these baseband signals need to be impressed onto another radio wave, the carrier, that will carry them

over the necessary distance.

Hertz (Hz)—The frequency of an electromagnetic wave, such as a radio wave, is measured in Hertz, abbreviated Hz, where one Hertz represents a complete cycle of the wave from maximum through minimum and back to maximum in one second. The alternating current that is used to power household appliances in North America, parts of South America and in Southern Japan has a frequency of 60 Hertz. In most of the rest of the world, house current has a 50-Hertz frequency. Until the late 1960s frequency was denominated in cycles per second, which is perhaps more descriptive, but that terminology is no longer used. Since radio waves have much higher frequencies than power waves, they use multiplier prefixes to avoid writing lots of zeros. Thus, a Kilohertz (KHz) is a thousand Hertz, one Megahertz (MHz) represents a frequency of one million Hertz, and one Gigahertz (GHz) is one billion Hertz. Although specifics vary by country, FM radio stations generally operate in the 76-108 MHz band, television from about 50 to 800 MHz, PCS telephones like GSM 1900 near 2 GHz, and so on.

Modulation—As it happens, the frequencies of waves that can be directly perceived do not travel for long distances. A loud noise can travel for a few thousand feet at most, and usually less. Any solid object can block light. To send messages that are themselves composed of electromagnetic waves—for example, listening to a symphony played in Boston while sitting in Delhi, the signal must somehow be impressed onto another signal that enables it to travel the distance required. Radio, for example, makes it possible to hear things at a great distance from their source by impressing the sound signals onto a wave of much higher frequency that is able to travel from the radio-transmitting site to the receiver. Radio receivers then extract the sound from the signal, and generate sound waves that can be heard. This process of impressing a signal carrying information onto another signal is called modulation. The recovery process performed by the radio receiver in the example is known as demodulation. When a radio is tuned to 1030 Hz, the frequency of the carrier signal is being selected. Circuits in the radio choose that frequency distinctly from the others, so only the desired signal is heard, and then demodulate the signal so people can hear the program.

Modulation requires the carrier signal to be of much higher frequency than the information signal that it will carry. A carrier wave can be modulated by varying any of its defining characteristics—frequency, amplitude, or phase—as a function of time. WLANs use modulation that varies the frequency of the signal in special ways to make the signal wider. Some of these are known as Direct Sequence Spread Spectrum (DSSS), Frequency Hopped Spread Spectrum (FHSS), Orthogonal Frequency Division Modulation (OFDM), and Gaussian Minimum Shift Keying (GMSK). There is no need to delve into the details of modulation here, but it is important to know that the carrier signal is only a means of getting the information signal from one place to another—it is not an end in itself.

Multipath Fading—There are many possible paths a radio signal may take from the transmitter to the receiver, because the signal radiates in many directions from the transmitting antenna. As result, some components of the signal arrive at the receiver after having been reflected from surfaces along the way. A reflected signal travels a longer path than does the direct signal. Each of these signals left the transmitter at the same instant, or in phase. The reflected signal components take longer to arrive at the receiver than does the direct signal. A signal that took a path exactly one-half of a wavelength longer than the direct wave, if it is of the same amplitude as the direct wave, will cancel the direct wave entirely at the receiver, even if each of the two components were separately quite strong. If the two signals are not quite of the same amplitude, or not exactly a half-wavelength apart, they will add in such a way as to either increase or decrease the received signal. This phenomenon is known as multipath fading. Even if the transmitter and receiver are motionless, some of the reflecting surfaces along the paths are not, so the received signal

strength constantly varies over time. The excursions from peak to trough of signal strength often cause a change in signal power level of as much as 10 million to one in the space of a tiny fraction of a second.

Richard A. Stanley, Ph.D., PE, CISSP is vice president of Wheeler Associates, Limited, a technology and educational consulting firm outside Boston, which specializes in custom security solutions. He has over 35 years experience with telecommunications and security systems and has directed research in those areas for the US government and in the private sector. He is a Registered Professional Electrical Engineer in the Commonwealth of Massachusetts, USA and a Certified Information Systems Security Professional. Dr. Stanley is a member of the New York Electronic Crimes Task Force. He often speaks at professional gatherings, and holds appointments as an adjunct professor at Worcester Polytechnic Institute, Suffolk University, and the University of Massachusetts-Boston, where he teaches security-related topics in electrical engineering and computer science.

To learn more about wireless and its key components, risk management methodologies and risks and controls, look for the full research results which will be published in September 2002 by ISACF in the book: *Wireless LAN Risks and Vulnerabilities*. The book contains an overview of wireless, provides a risk management methodology, explores wireless risk areas and provides a comprehensive audit work program to address the key risks. Some of the content areas include: wireless security issues, telecommunications architectures, data networks, history of architectures and how wireless systems extend these architectures, typical wireless architecture and protocols, wireless technology including wireless LAN, regulatory issues and world zones, monitoring and intrusion detection, risks and control, vulnerabilities, countermeasures, system design, due diligence requirements, customer expectations, legal and ethical concerns, overview of pertinent legislation including international legal requirements, auditing issues, privacy and regulatory issues.

Information Systems Audit and Control Foundation
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008, USA
Phone +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org