List of Wireless Acronyms and Initialisms

Organizations and Programs

CCTL – Common Criteria Testing Laboratories
(<http://www.niap.nist.gov/cc-scheme/TestingLabs.html>)
CCTLs are National Information Assurance Partnership (NIAP)-approved security testing laboratories that conduct security evaluations of information technology products and protection profiles. The CCTLs use NIAP-approved test methods derived from the Common Criteria.

Centers of Academic Excellence in Information Assurance Education
(<http://www.nsa.gov/isso/programs/coeiae/index.htm>)
The National Security Agency has established the Centers of Academic Excellence in Information Assurance Education program. The objective is to reduce vulnerability in our National Information Infrastructure by promoting higher education in information systems security, and producing a growing number of professionals with INFOSEC expertise.

CERT/CC – Computer Emergency Response Team
(<http://www.cert.org>)
CERT is the Internet's official security emergency team. It monitors and responds to Internet assaults, and is a federally funded organization located at Carnegie-Mellon University in Pittsburgh.

CSRC – Computer Security Resource Center
(<http://csrc.nist.gov/>)
CSRC is an informational resource center managed by the Computer Security Division of the Information Technology Laboratory of the National Institute of Standards and Technologies. It is part of the Computer Security Division's (CSD) focus on providing wider awareness of the importance and need for information technology security. It promotes the understanding of security vulnerabilities. CSRC lists alerts related to wireless-security and other security-related vulnerabilities.

CTIA – Cellular Telecommunications and Internet Association
(<http://www.wow-com.com>)
An international organization representing the wireless industry, CTIA addresses wireless concerns related to taxation, roaming, safety, regulations, fraud, and technology. The association has published several documents on issues and technology changes related to wireless security.

DARPA – Defense Advanced Research Projects Agency
(<http://www.darpa.mil>)
DARPA is the central research and development organization for the Department of Defense. It manages research and development projects that may provide dramatic advances for traditional military roles and missions.

FCC – Federal Communications Commission
(<http://www.fcc.gov>)
An independent U.S. agency reporting directly to Congress, the FCC is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable for all 50 states, the District of Columbia, and U.S. possessions.

GSMA – GSM Association
(<http://www.gsmworld.com>)
The Global System for Mobile (communications) Association represents the interests of more than 600 GSM, satellite and 3GSM operators, key manufacturers and suppliers to the industry as well as regulatory and administrative bodies from more than 173 countries and regions throughout the world. It maintains open standards and interoperability of the mobile communications industry.

IEEE – Institute of Electrical and Electronics Engineers, Inc
(<http://www.ieee.org>)
IEEE is an international, non-profit, technical professional association that develops industry standards related to electrical engineering. The group has developed wireless standards for Local Area Networks (LANs), personal area networks (PANs), and metropolitan area networks (MANs).

IETF – The Internet Engineering Task Force
(<http://www.ietf.org>)
The IETF is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and operation. The task force has a working group addressing the subject of Internet Protocol Routing for Wireless/Mobile Hosts, which has created several Request For Comments (RFC) related to authentication and authorization in the wireless area.

IETF AAA — IETF's Authentication, Authorization and Accounting Working Group
(<http://www.ietf.org/html.charters/aaa-charter.html>)
The Working Group has developed the requirements, solicited protocol submission, and evaluated submissions for authentication, authorization, and accounting of network access. The group will focus on development of an IETF Standards track protocol based on the DIAMETER submission.

ISAC – Information Sharing and Analysis Center
(<http://www.predictive.com/solutions/units/isac.cfm>)
An ISAC is a collection of information gathering, storage, analysis, and distribution resources designed to allow individuals submit reports about information-security threats, vulnerabilities, incidents, and solutions. ISAC members share these resources and information, as well as information obtained from other sources.

ITU – International Telecommunications Union
(<http://www.itu.int>)
The ITU is an international organization within the United Nations system headquartered in Geneva, Switzerland. It provides a forum for governments and the private sector to coordinate global telecom networks and services.

MobileIP WGs
(<http://www.ietf.org/html.charters/mobileip-charter.html>)
MobileIP is an IETF Working Group dealing with Internet Protocol routing for wireless mobile hosts. The group has developed routing support to allow IP nodes to "roam" seamlessly among IP subnetworks and media types.

NIAP – National Information Assurance Partnership
(<http://www.niap.nist.gov>)
NIAP is a U.S. Government initiative formed out of the collaboration of NIST and NSA with the long-term goal of increasing consumer trust in information systems and networks through the use of efficient assessment, evaluation, and testing programs. NIAP lists several specific security vulnerabilities of wireless-communication products within their vulnerability metabase (<http://csrc.nist.gov/icat/>). The vulnerability information is provided to product developers, integrators, certifiers, accreditors, and consumers to support the processes of information technology security.

NIPC – National Infrastructure Protection Center
(<http://www.nipc.gov>)
The mission of NIPC is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response to threats or attacks against critical infrastructures. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services. NIPC has published a document on best practices for use of 802.11b wireless networking. The report is available at <http://www.nipc.gov/publications/nipcpub/bestpract.html>.

NIST – National Institute of Standards and Technologies
(<http://www.nist.gov>)
NIST is a federal agency within the U.S. Commerce Department's Technology Administration. Its mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's System and Network Security Group researches and develops security technology for advanced countermeasures, vulnerability analysis/mitigation, access control, incident response, criteria/metrics, assurance methods and Internet security. NIST and NSA support the National Information Assurance Partnership (NIAP).

NSA – The National Security Agency
(<http://www.nsa.gov>)
The NSA is the U.S. Government's cryptologic organization, which coordinates, directs, and performs highly specialized activities to protect information systems and produce foreign intelligence information. NSA and NIST support the National Information Assurance Partnership (NIAP).

NSF – National Science Foundation
(<http://www.nsf.gov>)
The NSF is an independent agency of the U.S. Government, with the mission to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense.

SFS – Scholarship for Service
(<http://www.ehr.nsf.gov/ehr/due/programs/sfs/>)
The SFS program was implemented by the NSF to increase the number of qualified students entering the fields of information assurance and computer security, as well as to increase the ability of higher education to graduate professionals in these fields.

TCPA – Trusted Computing Platform Alliance
(<http://www.trustedcomputing.org>)
TCPA was formed from a coalition of Compaq, HP, IBM, Intel and Microsoft, with the intent to collaborate with other vendors to enhance hardware and operating-system-based trusted computing platforms.

Laws

18 U.S.C. section 1030 – Computer Fraud and Abuse Act 1986
The Computer Fraud and Abuse Act defines three felonies and four misdemeanors related to unauthorized access to classified information, use of computers to defraud others, and use of computers to damage other computer systems.

DMCA, 1998 – Digital Millennium Copyright Act
(<http://www.arl.org/info/frn/copy/dmca.html>)
The DMCA was designed to implement treaties signed in December 1996 at the World Intellectual Property Organization (WIPO) Geneva conference. It also addresses additional copyright issues related to commercial software and electronic material.

UCITA – Uniform Computer Information Transactions Act
(<http://www.ucita.org>)
UCITA is a proposed contract-law statute designed to create a uniform commercial contract for what are generally known as "shrink-wrap licenses." If enacted, the law would make such licenses completely enforceable.

Models, Standards, and Protocols

AES – Advanced Encryption Standard
AES is planned to be the new cryptographic algorithm for use by the U.S. government. Based on the Rijndael Block Cipher, it was approved by NIST in October 2000.

Bluetooth
(http://www.bluetooth.com)
Bluetooth is an international short-range wireless communication specification used by mobile devices such as phones, computers and PDAs. It operates predominantly in the 2.45 GHz frequency band.

CC – Common Criteria
(<http://www.commoncriteria.org>)
The Common Criteria is a standard for information security. It defines the functional and assurance requirements of computer products within three user groups: consumers, developers, and evaluators. CC is an international project involving NIST and NSA, as well as security organizations from Canada, France, Germany, the Netherlands, the United Kingdom, and other nations. The CC project has developed a draft Protection Profile titled "Infrastructure Wireless Local Area Network for Sensitive but Unclassified Environments."

CDMA – Code Division Multiple Access
A wireless protocol used with 3G technology in which multiple channels are independently coded for transmission over a single wideband channel.

EAP – Extensible Authentication Protocol
EAP is an extension to the Point-to-Point Protocol (PPP). It provides an authentication mechanism to support schemes using token cards, one-time passwords, public key, certificates and others.

EAPOL (IEEE 802.1x) – Extensible Authentication Protocol Over LAN
The IEEE 802.1x standard defines the process of passing EAP over a wired or wireless LAN where the rest of PPP is not required or desired. The protocol in 802.1x is called EAP encapsulation over LANs (EAPOL). It is currently defined for Ethernet and token ring LANs

EAP-TLS – Extensible Authentication Protocol - Transport Layer Security
EAP-TLS is a mutual authentication method requiring both client and server to prove their identities.

EAP-TTLS – Extensible Authentication Protocol - Tunneled Transport Layer Security
EAP-TTLS is an IETF draft and is a working document of the PPP Extensions group. The purpose of the protocol is to authenticate users onto WLANs with their existing password credentials and to protect the password transmission against eavesdropping.

GSM – Global System for Mobile communications
GSM is an open system that provides international roaming capability for mobile communications. It uses digital technology and time division multiple-access transmission methods. The system allows customers to use the same number in more than 170 countries. GSM satellite roaming covers areas outside of terrestrial coverage.

IEEE 802.11b
This Institute of Electrical and Electronics Engineers standard, also known as Wi-Fi, provides a mechanism for authentication and encryption of transmissions on a wireless LAN utilizing the 2.4 gigahertz bandwidth space. Encryption and authentication is implemented via the Wired Equivalent Privacy (WEP) protocol.

IP – Internet Protocol
The Internet Protocol is one of several Internet Layer Protocols used in the TCP/IP suite of protocols. It defines how data is exchanged between Internet Layers within TCP/IP.

IPSec IP Security
IPSec is a security standard that defines several protocols to provide encryption, access control, non-repudiation and authentication of messages over an IP network. IPSec works at layer 3 and is designed to be functionally compatible with IPv6 (see next listing).

IPv6 Internet Protocol version 6
Ipv6 is a protocol designed by the IETG to fix the shortcomings of IPv4, such as data security, and to address quantity limitations. IPsec support is mandatory with IPv6.

ISO 17799 – International Organization for Standards 17799 standard
The ISO 17799 is a comprehensive and widely recognized international security standard. The standard is organized into 10 major sections covering areas such as planning, controls, maintenance and compliance. The first version of ISO 17799 was published in December 2000.

ISO/IEC standard 15408 – International Organization for Standardization & International Electrotechnical Commission
(<http://www.csrc.nist.gov/cc/ccv20/ccv2list.htm>).
ISO/IEC standard 15408 is the international standard equivalent to the Common Criteria.

OMA – Open Mobile Architecture
OMA is an initiative launched and supported by several wireless industry companies for the purpose of boosting early introduction of interoperable mobile Internet access and downloading services worldwide. This action will provide consumers with more interoperable devices and service while retaining functional diversity with in the products.

PEAP – Protected Extensible Authentication Protocol
PEAP is a protection mechanism for EAP communication between an EAP client and an EAP authenticator. The PEAP mechanism uses Transport Layer Security (TLS) to create an end-to-end encrypted channel after verifying the identity of the authenticator. The EAP protocol packets are exchanged over this encrypted channel.

PKI – Public Key Infrastructure
PKI is a standard for identifying individuals using digital signatures and certificates. It enables users to exchange data securely by use of a public and private cryptographic key pair that is obtained and shared through a common trusted authority.

SSID – Service set identifier
A unique identifier associated with an access point or group of access points.

SSL – Secure Sockets Layer
An encryption technology used for secure transmissions, SSL uses symmetric or asymmetric (public key) cryptography for peer authentication. The WAP 2.0 protocol will include SSL.

T-CMM – Trusted Capability Maturity Model
The Trusted CMM is a reference model for software process improvement and increased software assurance. Hardware and software assurance measures are required to allow simultaneous processing of a range of sensitive or classified information at the same time.

TDMA – Time Division Multiple Access
TDMA is a digital transmission technology where multiple wireless users can access the network over a single radio-frequency channel without interference. This is accomplished by allocating three unique time slots of the channel to each user.

TLS certificate – Transport Layer Security certificate
TLS, also know as Secure Sockets Layer (SSL) v3.1, utilizes public key cryptography for secure communications between Web browser and server. Certificates are issued by a Certificate Authority validating the public key is owned by the user. A certificate is a public key that has been digitally signed by a trusted third-party and packaged electronically with other related information.

WAP – Wireless Application Protocol
Cellular phones, PDAs, TVs and automotive displays that access the Internet use WAP. It functions like TCP/IP and HTML with reduced overhead to accommodate memory and processor limitations in mobile devices.

WCDMA – Wideband Code Division Multiple Access
WCDMA is a CDMA that is four times wider than the channels used for 2G networks in North America. The European Telecommunications Standards Institute (ETSI) adopted WCDMA for multiple access technique of 3G mobile communications.

WEP – Wired Equivalent Privacy
WEP is an authentication and privacy option available with the IEEE 802.11 wireless LAN standard. WEP uses a shared key between the client and access point, thereby allowing only those devices with a valid key to communicate with the access point.

WTLS – Wireless Transport Layer Security
WTLS provides authentication, privacy and integrity for the Wireless Application Protocol. It is based on TLS v1.0 and is designed to handle the requirements of the mobile networks; low bandwidth, datagram connection, limited processing power and memory capacity, and cryptography exporting restrictions.

Other Terms

3G – Third-Generation Mobile Systems
3G technology extends the capabilities of today's 2G mobile wireless network. This will be accomplished by support of both circuit and packet switched solutions, as well as data rates up to 2Mbps. The higher bandwidth will be predominantly available in populous areas.

4G – Fourth-generation mobile systems
4G technology is planned to provide an entirely packet-switched network where all elements are digital. The expected bandwidth will reach up to 100Mbps with tight network security.

AP – Access Point
A router, switch or hub device that manages multiple wireless connections to a network.

BREW – Binary Runtime Environment for Wireless
BREW is QUALCOMM's applications platform for CDMA wireless devices. It provides developers with a standard programming environment for creating wireless Internet applications and services. The platform will be provided and supported by QUALCOMM Internet Services (QIS).

CISSP – Certified Information Systems Security Professional
(<http://www.isc2.org/>).
This certification was designed to recognize mastery of an international standard for information security and understanding of a Common Body of Knowledge (CBK). Certification can enhance a professional's career and provide added information-systems credibility.

GPRS – GSM Packet Radio Service
GPRS is a packet data communications system integrated with the GSM cellular telephone system. It is a complex system that merges cellular telephone radio transmission technology and Internet information-delivery protocols. GPRS is a 2.5-generation packet based network technology for GSM networks. Data speeds for GPRS are expected to reach 100 Kbps.

iMode
iMode is a mobile Internet service that utilizes an overlay packet network for communications to the content providers on the Internet. It uses compact HTML (c-HTML), which is a subset of HTML. iMode devices display multi-color images and support navigation through hyperlinks.

ISSO – Information System Security Officer
The ISSO is the person responsible for ensuring that security is provided for and implemented throughout the life cycle of a systems-development process.

J2ME – Java 2 Micro Edition
J2ME is a modular, scalable architecture that supports the deployment of Java technology for devices with various features. It allows a developer to select a configuration and set of APIs that relate to the requirements of the device.

Since mobile devices do not need to support the entire Java 2 platform, J2ME will allow developers to select the best configuration and profile for the application.

LAN – Local Area Network
A LAN connects computers within a single geographical location, such as a building or office, thereby enabling users to share common resources such as file servers, printers, and Internet access.

MAC address – Media Access Control address
The MAC address is a 48-bit-long address that uniquely identifies each physical machine on an Ethernet local area network.

MD5
MD5 is a message-digest algorithm developed by Ronald Rivest. It takes an arbitrary length message and generates a fixed 128-bit message digest using a hash function.

NFAT – Network Forensic Analysis Tool
An NFAT product is able to record network traffic related to a security attack, and it provides the tools to perform forensic analysis of the event. The products allow a security analyst to replay, isolate and scrutinize an attack or suspicious behavior.

NIC – Network Interface Card
A NIC is a special circuit board either added to a computer or built in that allows the computer to communicate over a LAN.

PALM OS
A simple operating system for a handheld computer developed by Palm Computing in 1996. The Palm OS is relatively straightforward and is C language based, which opens it up to the widest variety of development options. Wireless data access was added to operating system in Palm OS 3.2.

PDA – Personal Digital Assistant
A PDA is small, portable computer that allows the user access to a variety of functionality. Applications for the device include Internet access, e-mail, contact management, time management and other user-specific applications.

RADIUS – Remote Authentication and Dial-In User Service
RADIUS is a centralized access-control system used by dial-up users to obtain access to a trusted network. An authentication server with dynamic passwords verifies users dialing into the network. In some cases, a callback function may be implemented.

RC4
RC4 is a stream-cipher cryptography algorithm developed by Ronald Rivest. A stream cipher encrypts all the data in real time. RC4 can use variable key-size from 40 bits to 128 bits long.

RFID – Radio Frequency IDentification
RFID is a method of identification through the use of data stored in what is called a tag and transmission of that data through transponders to receiving devices. The objective of an RFID is to provide identification or specific data about an item without requiring the read of visual information.

RIM devices – Research In Motion devices
RIM devices consist of wireless two-way communication solutions, such as the BlackBerry wireless email solution, which allow mobile professionals to send and receive emails wherever they go. These devices utilize advanced encryption technology to meet the security requirements of the public and private sector organizations.

SLA – Service Level Agreement
An SLA is an agreement between a network service provider and a customer that defines the expected service performance in measurable terms. In some cases, information systems departments have established SLAs with their user groups to help define performance expectations.

SMS – Short Message Service
SMS is a mobile messaging service that provides short messages up to 160 characters of text in a store and forward mode. SMS also provides confirmation of message delivery. Mobile messaging is evolving beyond text from SMS to EMS (Enhanced Messaging Service) to MMS (Multimedia Messaging Service).

Symbian OS
<http://www.symbian.com>
EPOC is a communication-centric operating system designed for mobile systems. It utilizes object-orientation to deliver user and developer tools using a small ROM footprint.

VPN – Virtual Private Network
A VPN is a secure private connection that operates over an unsecure public network. It employs encryption technology to ensure safe data transmission.

Windows CE
Microsoft Windows CE is a scaled-down operating system designed for small devices such as handheld computing devices, mobile phones, automobiles and industrial equipment.

WISP – Wireless Internet Service Provider
A WISP is an Internet Service Provider that provides access by use of an 802.11b wireless LAN. WISPs are actively being deployed in airports, convention centers (even restaurants), as well as some communities. There is effort under way to provide roaming capability.

WLAN – Wireless LAN
A WLAN uses radio-frequency transitions to transfer data between computers in a local area network.