National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Interagency Report 7581
September 2009

System and Network Security Acronyms and Abbreviations

Karen Scarfone
Victoria Thompson

NIST Interagency Report 7581
September 2009

System and Network Security Acronyms and Abbreviations

Karen Scarfone
Victoria Thompson

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2009

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7581
32 pages (Sep. 2009)

Acknowledgments

The authors, Karen Scarfone of the National Institute of Standards and Technology (NIST) and Victoria Thompson of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this report, particularly Liz Lennon and Tim Grance of NIST. Thanks also go to individuals and organizations that submitted suggestions, particularly Tim Kramer, Mark Seecof, Janine Paris, the U.S. Department of Energy, and the U.S. Department of State. The authors also thank their colleagues who created acronym and abbreviation lists for their publications that were subsequently used as sources of information for this report.

Trademark Information

Note to Reviewers

Reviewers are encouraged to submit additional acronyms and abbreviations related to system and network security, particularly for emerging technologies, for consideration as additions to this report. All suggestions and corrections should be sent to securityacronyms@nist.gov.

Table of Contents

1. Introduction

This report contains a list of selected acronyms and abbreviations for system and network security terms with their generally accepted or preferred definitions. It is intended as a resource for federal agencies and other users of system and network security publications.

The capitalization, spelling, and definitions of acronyms and abbreviations frequently vary among publications. It is easy to understand why this happens. While some acronyms and abbreviations (e.g., WWW*)* have one universally recognized and understood definition within the domain of system and network security, others (e.g., IA, MAC) have multiple valid definitions depending upon the context in which they are used. Some acronyms bear little resemblance to their definitions, such as Modes of Operation Validation System for the Triple DES Algorithm (TMOVS). Others use unexpected capitalization or spelling (e.g., Electronic Business using eXtensible Markup Language [ebXML] and Organisation for Economic Co-operation and Development [OECD]). As a result, acronyms, abbreviations, and their definitions may be inaccurately or inconsistently defined by authors, perpetuating errors and confusing or misleading readers.

This report is meant to help reduce these errors and confusion by providing the generally accepted or preferred definitions of a list of frequently used acronyms and abbreviations. The list does not include *all* system and network security terms, nor is it a compendium of every acronym and abbreviation found in system and network security documents published by NIST. Readers should refer to each document's list of acronyms and abbreviations (typically found in an appendix) for definitions applicable to that particular document.

The following conventions have been used in the preparation of the list of acronyms and abbreviations in this report.

- Abbreviations and acronyms generally appear in all capital letters, although there are occasional exceptions—for example, meter (m) and decibels referenced to one milliwatt (dBm).
- Technical terms are not capitalized unless they are proper nouns. Names of people, places, and groups, and the titles of protocols, standards, and algorithms are considered proper nouns. For example, certification and accreditation (C&A) is not capitalized, but Advanced Encryption Standard (AES) is capitalized.
- Collective nouns are not capitalized (e.g., wide area network [WAN]).
- When two or more definitions of the same acronym or abbreviation are given, the acronym or abbreviation is italicized and repeated for each definition. Definitions are listed alphabetically.

2. Acronym and Abbreviation List

This section consists of a list of selected system and network security acronyms and abbreviations, along with their generally accepted definitions. When there are multiple definitions for a single term, the acronym or abbreviation is italicized and each definition is listed separately.

Numeric

1xRTT	one times radio transmission technology
3DES	Triple Data Encryption Standard
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

A

A	address resource record type
AA	ABAC attribute authority
AAA	authentication, authorization, and accounting
AAAK	authentication, authorization, and accounting key
AAD	additional authenticated data
AAR	after action report
AAS	adaptive antenna system
ABAC	attribute-based access control
ACE	access control entry
ACL	access control list
ACM	Association for Computing Machinery
ACO	authenticated cipher offset
AD	Active Directory
AD	authenticated data
ADS	alternate data stream
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Block Chaining
AES-CTR	Advanced Encryption Standard-Counter Mode
AFH	adaptive frequency hopping
A-GPS	assisted global positioning system
AH	Authentication Header
AIDC	automatic identification and data capture
AIM	Association for Automatic Identification and Mobility
AIT	automatic identification technology
AJAX	Asynchronous JavaScript and XML
AK	authorization key
AKID	authorization key identifier
AKM	authentication and key management
ALG	application layer gateway
ANSI	American National Standards Institute
AP	access point
API	application programming interface

APWG	Anti-Phishing Working Group
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	authentication server
AS	authentication service
AS	autonomous system
ASC	Anti-Spyware Coalition
ASC X9	Accredited Standards Committee X9
ASCII	American Standard Code for Information Interchange
ASLR	address space layout randomization
ASN	autonomous system number
ASN.1	Abstract Syntax Notation 1
ASP	active server pages
ATA	Advanced Technology Attachment
ATIM	Announcement Traffic Indication Message
ATM	asynchronous transfer mode
ATM	automated teller machine
AV	antivirus
AVIEN	Anti-Virus Information Exchange Network
AVP	attribute-value pair

B

B2B	business-to-business
BCP	best current practice
BCP	business continuity plan
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol 4
BIA	Bump-in-the-API
BIA	business impact analysis
BioAPI	Biometric Application Programming Interface
BIOS	basic input/output system
BITS	Bump-in-the-Stack
BPML	Business Process Modeling Language
BPSS	Business Process Specification Schema
BRP	business recovery (resumption) plan
BS	base station
BSC	base station controller
BSI	British Standards Institution
BSIA	British Security Industry Association
BSP	best security practice
BSS	basic service set
BSSID	basic service set identifier
BTNS	better-than-nothing-security
BTS	base transceiver station
BU	binding update
BUA	binding update acknowledgement

C

C&A	certification and accreditation
CA	certificate authority
CA	certification agent
CA	certification authority
CAC	common access card
CAIDA	Cooperative Association for Internet Data Analysis
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CARO	Computer Antivirus Research Organization
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CBEFF	Common Biometric Exchange File Format
CC	Common Criteria
CCE™	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIPS	Computer Crime and Intellectual Property Section
CCK	complementary code keying
CCM	Counter Mode with CBC-MAC
CCMP	Counter Mode with CBC-MAC Protocol
CCRA	Common Criteria Recognition Arrangement
CCSS	Common Configuration Scoring System
ccTLD	country code top-level domain
CD	checking disabled
CD	compact disc
CDFS	compact disc file system
CDMA	code division multiple access
CD-R	compact disc-recordable
CD-ROM	compact disc-read only memory
CD-RW	compact disc-rewritable
CEO	chief executive officer
CERIAS	Center for Education and Research in Information Assurance and Security
CERT	computer emergency response team
CERT®/CC	CERT® Coordination Center
CF	CompactFlash®
CFAA	Computer Fraud and Abuse Act
CFB	Cipher Feedback
CFI	computer and financial investigations
CFR	Code of Federal Regulations
CFTT	computer forensics tool testing
CGA	cryptographically generated addresses
CGI	Common Gateway Interface
CHAP	Challenge-Handshake Authentication Protocol
CHUID	cardholder unique identifier
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CIO	chief information officer
CIP	critical infrastructure protection
CIPC	Critical Infrastructure Protection Committee

CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIRC	computer incident response capability
CIRC	computer incident response center
CIRDB	CERIAS Incident Response Database
CIRT	computer incident response team
CIS	Center for Internet Security
CISO	chief information security officer
CLF	common log format
CLI	command line interface
CLR	common language runtime
cm	centimeter
CMA	Certificate Management Authority
CMAC	Cipher-based Method Authentication Code
CME	Common Malware Enumeration
CMOS	complementary metal oxide semiconductor
CMS	Centers for Medicare and Medicaid Services
CMS	Cryptographic Message Syntax
CMSS	Common Misuse Scoring System
CMVP	Cryptographic Module Validation Program
CN	common name
CN	correspondent node
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CoA	care-of address
codec	coder/decoder
COI	conflict of interest
COM	Component Object Model
COOP	continuity of operations
COPPA	Children's Online Privacy Protection Act
CORBA®	Common Object Request Broker Architecture
COTS	commercial off-the-shelf
CP	certificate policy
CP	contingency plan
CPE™	Common Platform Enumeration
CPI	compression parameter index
CPNI	Centre for the Protection of National Infrastructure
CPS	certification practice statement
CPU	central processing unit
CRAM	challenge-response authentication mechanism
CRC	cyclic redundancy check
CRL	certificate revocation list
CS	client/server
CSIA	Cyber Security Industries Alliance
CSIRC	computer security incident response capability
CSIRT	computer security incident response team
CSO	chief security officer
CSO	computer security object
CSP	Credentials Service Provider
CSR	certificate signing request
CSRC	Computer Security Resource Center
CSRDA	Cyber Security Research and Development Act of 2002

CSS cascading style sheet
CSV comma-separated values
CTO chief technology officer
CTR counter mode encryption
CVE Common Vulnerabilities and Exposures
CVSS Common Vulnerability Scoring System
CWE Common Weakness Enumeration

D

DA destination address
DAA designated accrediting authority
DAA designated approving authority
DAC discretionary access control
DAD duplicate address detection
DAML DARPA Agent Markup Language
D-AMPS Digital Advanced Mobile Phone Service
DAO Data Access Object
DARPA Defense Advanced Research Projects Agency
dBm decibels referenced to one milliwatt
DBMS database management system
DC domain controller
DCE Distributed Computing Environment
DCOM Distributed Component Object Model
DCS distributed control system
DDMS Department of Defense Metadata Specification
DDoS distributed denial of service
DEA Data Encryption Algorithm
DEP Data Execution Prevention
DES Data Encryption Standard
DFS Distributed File System
DFS dynamic frequency selection
DH Diffie-Hellman
DHAAD Dynamic Home Agent Address Discovery
DHCP Dynamic Host Configuration Protocol
DHCPv6 Dynamic Host Configuration Protocol for Internet Protocol v6
DHS U.S. Department of Homeland Security
DIMS Digital Identity Management Service
DISA U.S. Defense Information Systems Agency
DLL dynamic link library
DMA direct memory access
DMZ demilitarized zone
DN distinguished name
DN domain name
DNP Distributed Network Protocol
DNS domain name system
DNSBL Domain Name System Blacklist
DNSSEC Domain Name System Security Extensions
DOC U.S. Department of Commerce
DoD U.S. Department of Defense

DOE	U.S. Department of Energy
DOI	domain of interpretation
DOJ	U.S. Department of Justice
DOM	Document Object Model
DoS	denial of service
DPA	differential power analysis
DRA	data recovery agent
DRM	digital rights management
DRP	disaster recovery plan
DS	Delegation Signer
DS	distribution system
DS Field	differentiated services field
DSA	Digital Signature Algorithm
DSL	digital subscriber line
DSML	Directory Services Markup Language
DSN	delivery status notification
DSOD	dynamic separation of duty
DSS	Digital Signature Standard
DSTM	Dual Stack Transition Mechanism
DTC	Distributed Transaction Coordinator
DTD	Document Type Definition
DTR	derived test requirement
DUID	DHCP unique identifier
DVD	digital video disc
DVD-R	digital video disc - recordable
DVD-ROM	digital video disc - read only memory
DVD-RW	digital video disc - rewritable

E

EAL	evaluation assurance level
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAPOL	Extensible Authentication Protocol Over LAN
EAPOL-KCK	Extensible Authentication Protocol Over LAN Key Confirmation Key
EAPOL-KEK	Extensible Authentication Protocol Over LAN Key Encryption Key
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
EBGP	Exterior Border Gateway Protocol
ebXML	Electronic Business using eXtensible Markup Language
EC2N	Elliptic Curve over G[2N]
ECB	Electronic Codebook (mode)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECM	Enterprise Configuration Manager
ECP	Encryption Control Protocol
ECPA	Electronic Communications Privacy Act
EDGE	Enhanced Data rates for GSM Evolution
EDI	electronic data interchange

EDR	enhanced data rate
EEPROM	electronically erasable programmable read-only memory
EFI	Extensible Firmware Interface
EFS	Encrypting File System
EGP	Exterior Gateway Protocol
EH	extension header
EICAR	European Institute for Computer Antivirus Research
EIGRP	Enhanced Interior Gateway Routing Protocol
EIK	EAP Integrity Key
email	electronic mail
EMS	energy management system
EMS	Enhanced Messaging Service
EMSK	Extended Master Session Key
EPAL	Enterprise Privacy Authorization Language
EPC	electronic product code
EPCIS	Electronic Product Code Information Services
EPHI	electronic protected health information
EPS	events per second
ERP	enterprise resource planning
ESMS	enterprise security management system
ESMTP	Extended Simple Mail Transfer Protocol
ESN	electronic serial number
ESP	Encapsulating Security Payload
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
EU	European Union
EUI-64	Extended Unique Identifier 64 bit
EV-DO	Evolution-Data Optimized
ext2fs	Second Extended Filesystem
ext3fs	Third Extended Filesystem

F

FAQ	frequently asked questions
FAR	Federal Acquisition Regulation
FASC-N	Federal Agency Smart Credential Number
FASP	Federal Agency Security Practices
FAT	file allocation table
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FBI CJIS	Federal Bureau of Investigation Criminal Justice Information Services Division
FCC	Federal Communications Commission
FCC ID	Federal Communications Commission Identification number
FCL	final checklist list
FCPF	Federal PKI Common Policy Framework
FCRA	Fair Credit Reporting Act
FCS	frame check sequence
FDA	Food and Drug Administration
FDCC	Federal Desktop Core Configuration
FDCE	Federated Development and Certification Environment

FDE	full disk encryption
FDIC	Federal Deposit Insurance Corporation
FEA	Federal Enterprise Architecture
FEK	file encryption key
FFMIA	Federal Financial Management Improvement Act
FHSS	frequency hopping spread spectrum
FIB	forwarding information base
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standards
FIRST™	Forum of Incident Response and Security Teams
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FISSEA	Federal Information Systems Security Educators' Association
FLETC	Federal Law Enforcement Training Center
FMR	false match rate
FMS	Fluhrer-Mantin-Shamir
FNMR	false non match rate
FOIA	Freedom of Information Act
FPC	Federal Preparedness Circular
FPKI	Federal Public Key Infrastructure
FPKIA	Federal Public Key Infrastructure Architecture
FPKIPA	Federal Public Key Infrastructure Policy Authority
FQDN	fully qualified domain name
FRR	false rejection rate
FSO	field security office
FTC	Federal Trade Commission
FTCA	Federal Trade Commission Act
FTP	File Transfer Protocol
FUS	Fast User Switching
FY	fiscal year

G

GAO	U.S. Government Accountability Office
GB	gigabyte
GFAC	generalized framework for access control
GFIRST	Government Forum of Incident Response and Security Teams
GHz	gigahertz
GIG	Global Information Grid
GINA	graphical identification and authentication
GKEK	Group Key Encryption Key
GLB *or* **GLBA**	Gramm-Leach-Bliley Act
GMK	Group Master Key
GnuPG	GNU Privacy Guard
GOTS	government off-the-shelf
GPL	general public license
GPMC	Group Policy Management Console
GPO	Group Policy Object
GPRS	general packet radio service
GPS	global positioning system

GR graceful restart
GRE Generic Routing Encapsulation
GRS General Records Schedule
GS1 Global Standards One
GSA U.S. General Services Administration
GSM Global System for Mobile Communications
GTC Generic Token Card
GTEK group traffic encryption key
GTK group temporal key
gTLD generic top-level domain
GTSM Generalized TTL Security Mechanism
GUI graphical user interface

H

HA high availability
HA home agent
HAG high assurance guard
HCI host controller interface
HERF hazards of electromagnetic radiation to fuel
HERO hazards of electromagnetic radiation to ordnance
HERP hazards of electromagnetic radiation to personnel
HF high frequency
HFS Hierarchical File System
HHS U.S. Department of Health and Human Services
HINFO host information
HIP Host Identity Protocol
HIPAA Health Insurance Portability and Accountability Act
HIPERLAN high-performance radio local area network
HKLM HKEY_Local_Machine
HL7 Health Level Seven
HMAC keyed-hash message authentication code
HMI human-machine interface
HPA host protected area
HPFS High-Performance File System
HR human resources
HSARPA Homeland Security Advanced Research Projects Agency
HSPD Homeland Security Presidential Directive
HTCIA High Technology Crime Investigation Association
HTCP Hyper Text Caching Protocol
HTML Hypertext Markup Language
HTTP Hypertext Transfer Protocol
HTTPS Secure Hypertext Transfer Protocol
Hz hertz

I

I&A	identification and authentication
I/O	input/output
I3P	Institute for Information Infrastructure Protection
IA	information assurance
IAB	Internet Architecture Board
IACIS®	International Association of Computer Investigative Specialists
IAIP	Information Analysis and Infrastructure Protection
IANA	Internet Assigned Numbers Authority
IAO	information assurance officer
IATF	Information Assurance Technical Framework
IBC	iterated block cipher
IBE	identity-based encryption
iBGP	Internal Border Gateway Protocol
IBMJSSE	IBM Java Secure Socket Extension
IBSS	independent basic service set
IC3	Internet Crime Complaint Center
ICAMP	Incident Cost Analysis and Modeling Project
ICANN	Internet Corporation for Assigned Names and Numbers
ICCID	Integrated Circuit Card Identification
ICCP	Inter-control Center Communications Protocol
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICP	Internet Cache Protocol
ICS	industrial control system
ICS	Internet Connection Sharing
ICSA	International Computer Security Association
ICV	integrity check value
ID	identification
IDART™	Information Design Assurance Red Team
IDE	integrated development environment
IDE	Integrated Drive Electronics
IDEA	International Data Encryption Algorithm
iDEN	Integrated Digital Enhanced Network
ID-FF	Identity Federation Framework
IDMEF	Intrusion Detection Message Exchange Format
IDMS	identity management system
IDPS	intrusion detection and prevention system
IDS	intrusion detection system
ID-SIS	Identity Service Interface Specifications
ID-WSF	Identity Web Services Framework
ID-WSF DST	Identity Web Services Framework Data Services Template
IE	Internet Explorer
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE-SA	IEEE Standards Association
IESG	Internet Security Steering Group
IETF	Internet Engineering Task Force
IETF BCP	Internet Engineering Task Force Best Current Practice
IETF RFC	Internet Engineering Task Force Request for Comments

IGMP Internet Group Management Protocol
IGP interior gateway protocol
IID interface identifier
IIF information in identifiable form
IIHI individually identifiable health information
IIS Internet Information Services
IKE Internet Key Exchange
IM instant messaging
IMAP Internet Message Access Protocol
IMEI International Mobile Equipment Identity
IMSI International Mobile Subscriber Identity
INCITS InterNational Committee for Information Technology Standards
IP Internet Protocol
IPA initial privacy assessment
IPComp Internet Protocol Payload Compression Protocol
IPng Internet Protocol Next Generation
IPS intrusion prevention system
IPsec Internet Protocol Security
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
IPX Internet Packet Exchange
IR infrared
IR interagency report
IRC Internet Relay Chat
IrDA® Infrared Data Association®
IRQ interrupt request line
IRS Internal Revenue Service
IRTF Internet Research Task Force
IS information system
ISA interconnection security agreement
ISA International Society of Automation
ISAC information sharing and analysis center
ISAKMP Internet Security Association and Key Management Protocol
ISAP Information Security Automation Program
ISAPI Internet Server Application Programming Interface
ISATAP Intra-Site Automatic Tunnel Addressing Protocol
ISF Information Security Forum
ISID Industrial Security Incident Database
IS-IS Intermediate System-to-Intermediate System
ISM industrial, scientific, and medical
ISM information security marking
ISMS information security management system
ISO International Organization for Standardization
ISP Internet service provider
ISSEA International Systems Security Engineering Association
ISSO information systems security officer
ISSPM information systems security program manager
IT information technology
ITAA Information Technology Association of America
ITF Interrogator Talks First
ITL Information Technology Laboratory

ITU	International Telecommunications Union
ITU-T	International Telecommunications Union-Telecommunication Standardization Sector
IUT	implementation under test
IV	initialization vector

J

Java EE	Java Platform, Enterprise Edition
JAXR	Java API for XML Registries
JFFS2	Journaling Flash File System, version 2
JIT	just-in-time
JPEG	Joint Photographic Experts Group
JRE	Java Runtime Environment
JSM	Java Security Manager
JSP	Java Server Pages
JSSE	Java Secure Socket Extension
JTAG	Joint Test Action Group
JTC1	Joint Technical Committee 1 (International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC])
JVM	Java Virtual Machine

K

KB	kilobyte
Kbps	kilobit per second
KDC	key distribution center
KEK	key encryption key
KG	key generator
KGD	key generation and distribution
kHz	kilohertz
KINK	Kerberized Internet Negotiation of Keys
KSG	key stream generator
KSK	key signing key

L

L2CAP	Logical Link Control and Adaptation Protocol
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LACNIC	Latin American and Caribbean IP Addresses Registry
LAN	local area network
LCD	liquid crystal display
LDA	local delivery agent
LDAP	Lightweight Directory Access Protocol
LED	light emitting diode

LF low frequency
LFSR linear feedback shift register
LIR local Internet registry
LM LAN Manager
LMP Link Manager Protocol
LOC location (DNS record)
LOS line-of-sight
LRA Local Registration Authority
LUA limited user account

M

m meter
MAC mandatory access control
MAC media access control (layer)
MAC Medium Access Control
MAC message authentication code
MAF multi-mode authentication framework
MAN metropolitan area network
MAPS Mail Abuse Prevention System
MB megabyte
Mbps megabits per second
MBR master boot record
MBSA Microsoft Baseline Security Analyzer
MD message digest
ME mobile equipment
MED multi-exit discriminator
MEP message exchange pattern
MES manufacturing execution system
MHz megahertz
MIB management information base
MIC mandatory integrity control
MIC message integrity check
MIC message integrity code
MIKEY Multimedia Internet KEYing
MIME Multipurpose Internet Mail Extensions
MIMO multiple-input, multiple-output
MIN mobile identification number
Mini SD mini secure digital
MIP Mobile Internet Protocol
MitM man-in-the-middle (attack)
MLD Multicast Listener Discovery
MMC Microsoft Management Console
MMC MultiMediaCard
MMCmobile MultiMediaCard Mobile
MMS Multimedia Messaging Service
MN mobile node
MO magneto-optical
MOA memorandum of agreement
MOBIKE IKEv2 Mobility and Multihoming Protocol

MODP modular exponential
MOSS MIME Object Security Services
MOU memorandum of understanding
MOVS Modes of Operation Validation System
MPA Mobile Prefix Advertisement
MPLS multiprotocol label switching
MPS Mobile Prefix Solicitation
MQV Menezes-Qu-Vanstone
MRI magnetic resonance imaging
MS Microsoft
MS mobile subscriber
MSC mobile switching center
MS-CHAP Microsoft Challenge Handshake Authentication Protocol
MS-DOS Microsoft Disk Operating System
MSDP Multicast Source Discovery Protocol
MSEC multicast security
MSEL Master Scenario Events List
MSIL Microsoft Intermediate Language
MSISDN Mobile Subscriber Integrated Services Digital Network
MSK master session key
MSKB Microsoft Knowledge Base
MSSP managed security services provider
MSWG Metadata Standards Working Group
MTA mail transfer agent
MTM Mobile Trusted Module
MTU master telemetry unit
MTU master terminal unit
MTU maximum transmission unit
MUA mail user agent
mW milliwatt
MX mail exchanger

N

NA Neighbor Advertisement
NAC network access control
NACI National Agency Check and Inquiries
NAP Network Access Protection
NARA National Archives and Records Administration
NAS network access server
NAT network address translation
NAT-PT network address translation—protocol translation
NAT-T network address translation traversal
NBA network behavior analysis
NBAD network behavior anomaly detection
NCES NetCentric Enterprise Services
NCP National Checklist Program
NCSD National Cyber Security Division
NCSI NIST National Center for Standards and Certification Information
ND Neighbor Discovery

NDAC	nondiscretionary access control
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NetBT	NetBIOS over TCP/IP
NFAT	network forensic analysis tool
NFC	near field communication
NFS	network file system
NFS	Network File Sharing
NH	next header
NIAC	National Infrastructure Advisory Council
NIAP	National Information Assurance Partnership
NIC	network interface card
NICC	National Infrastructure Coordinating Center
NIJ	National Institute of Justice
NIPC	National Infrastructure Protection Center
NIS	Network Information System
NISAC	National Infrastructure Simulation and Analysis Center
NISCC	National Infrastructure Security Co-ordination Centre
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NLOS	non-line-of-sight
NPIVP	NIST Personal Identity Verification Program
NPPI	nonpublic personal information
NS	name server
NS	Neighbor Solicitation
NSA	National Security Agency
NSAPI	Netscape Server Application Programming Interface
NSEC	Next Secure
NSI	national security information
NSRL	National Software Reference Library
NSS	Network Security Services
NSTB	National SCADA Test Bed
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTFS	New Technology File System
NTLM	NT LAN Manager
NTP	Network Time Protocol
NTTAA	National Technology Transfer and Advancement Act of 1995
NUD	Neighbor Unreachability Detection
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
NW3C	National White Collar Crime Center
NX	no execute

O

OASIS™	Organization for the Advancement of Structured Information Standards
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OCSP	Online Certificate Status Protocol
ODBC	Open Database Connectivity
OECD	Organisation for Economic Co-operation and Development
OEM	original equipment manufacturer
OFB	output feedback (mode)
OFDM	orthogonal frequency-division multiplexing
OGSA™	Open Grid Services Architecture
OHA	Open Handset Alliance
OIG	Office of Inspector General
OLE	object linking and embedding
OMB	Office of Management and Budget
ONS	Object Naming Service
OOB	out-of-band
OPC	OLE for Process Control
OpenPGP	An Open Specification for Pretty Good Privacy
OPM	U.S. Office of Personnel Management
ORB	open relay blacklist
OS	operating system
OSHA	Occupational Safety and Health Administration
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	open source software
OSSTMM	Open Source Security Testing Methodology Manual
OSVDB	Open Source Vulnerability Database
OTP	one-time password
OU	organizational unit
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
OWL-S	Web Ontology Language for Services

P

P2P	peer-to-peer
PAC	Privilege Attribute Certificate
PAC	Protected Access Credential
PAD	peer authorization database
PAM	pluggable authentication module
PAN	personal area network
PAOS	Reverse HTTP Binding for SOAP
PAP	Password Authentication Protocol
PAP	policy access point
PAS	publicly available specification
PBA	pre-boot authentication
PBAC	policy-based access control
PBCC	Packet Binary Convolutional Code

PBE	pre-boot environment
PBX	private branch exchange
PC	personal computer
PCI	Payment Card Industry
PCI	personal identity verification card issuer
PCI DSS	Payment Card Industry Data Security Standard
PCMCIA	Personal Computer Memory Card International Association
PCN	process control network
PCP	IP Payload Compression Protocol
PCS	process control system
PCSF	Process Control System Forum
PCSRF	Process Control Security Requirements Forum
PDA	personal digital assistant
PDD	Presidential Decision Directive
PDF	Portable Document Format
PDP	policy decision point
PDS	protective distribution systems
PEAP	Protected Extensible Authentication Protocol
PED	portable electronic devices
PEM	Privacy Enhanced Mail
PEP	policy enforcement point
PFS	perfect forward secrecy
PGP	Pretty Good Privacy
PHI	protected health information
PHP	PHP: Hypertext Preprocessor
PHY	Physical (layer)
PIA	privacy impact assessment
PICS™	Platform for Internet Content Selection
PII	personally identifiable information
PIM	personal information management
PIM-SM	Protocol Independent Multicast—Sparse Mode
PIN	personal identification number
PIP	policy information point
PIR	Public Interest Registry
PIV	personal identity verification
PKCS	Public Key Cryptography Standard
PKI	public key infrastructure
PKM	privacy key management
PKMv1	Privacy Key Management Protocol version 1
PKMv2	Privacy Key Management Protocol version 2
PL	public law
PLC	programmable logic controller
PMA	Policy Management Authority
PMK	pairwise master key
PMKSA	Pairwise Master Key Security Association
PMP	point-to-multipoint
PMTU	path maximum transmission unit
PN	packet number
PNG	Portable Network Graphics
POA&M	plan of action and milestones
POC	point of contact

POC	proof of concept
PoE	Power over Ethernet
POP	Post Office Protocol
POP3	Post Office Protocol version 3
PP	protection profile
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PPVPN	provisioner-provided virtual private network
PRA	Paperwork Reduction Act
Pre-PAK	pre-primary authorization key
PRF	pseudorandom function
PRNG	pseudorandom number generator
PSK	pre-shared key
PSTN	public switched telephone network
PTA	privacy threshold assessment (or analysis)
PTK	pairwise transient key
PTV	perceived target value
PUB	publication
PUK	PIN unblocking key
PVG	patch and vulnerability group

Q

QoP	quality of protection
QoS	quality of service

R

R&D	research and development
R/W	read/write
RA	receiver address
RA	Registration Authority
RA	remote assistance
RA	Router Advertisement
RAdAC	risk adaptive access control
RADIUS	Remote Authentication Dial In User Service
RAID	redundant array of independent disks
RAM	random access memory
RAT	remote administration tool
RBAC	role-based access control
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RCE	route cache entry
RCFL	Regional Computer Forensics Laboratory
RCP	Remote Copy Protocol
RDBMS	relational database management system
RDP	Remote Desktop Protocol
REL	rights expression language
REP	Robots Exclusion Protocol

REST Representational State Transfer
RF radio frequency
RFC request for comments
RFD route flap damping
RFID radio frequency identification
RFP request for proposal
RIB routing information base
RIP Routing Information Protocol
RIPE NCC Réseaux IP Européens Network Coordination Centre
RIPng Routing Information Protocol next generation
RIR regional internet registries
RIS Remote Installation Services
RMA reliability, maintainability, and availability
RMON Remote Monitoring
RNG random number generator
ROE rules of engagement
ROM read-only memory
RP responsible person (record)
RPC remote procedure call
RPF Reverse Path Forwarding
RPO recovery point objective
RR resource record
RRSIG resource record signature
RS relay station
RS Router Solicitation
RSA Rivest-Shamir-Adelman
RSBAC rule set-based access control
RSN Robust Security Network
RSNA Robust Security Network Association
RSNIE Robust Security Network Information Element
RSO reduced sign-on
RSS Really Simple Syndication
RSSI received signal strength indication
RSVP Resource ReSerVation Protocol
RTF Rich Text Format
RTLS real-time location system
RTO recovery time objective
RTP Real-Time Transport Protocol
RTU remote terminal unit or remote telemetry unit
RuBAC rule-based access control
R-UIM Removable User Identity Module

S

S/MIME Secure/Multipurpose Internet Mail Extensions
SA security association
SA source address
SACL system access control list
SAD security association database
SAFER Secure And Fast Encryption Routine

SAID	security association identifier
SAISO	senior agency information security officer
SAM	Security Account Manager
SAM	software asset management
SAMATE	Software Assurance Metrics and Tool Evaluation
SAML™	Security Assertion Markup Language™
SAN	storage area network
S-BGP	Secure Border Gateway Protocol
SC	subcommittee
SCADA	supervisory control and data acquisition
SCAP	Security Content Automation Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SD	Secure Digital
SDIO	Secure Digital Input Output
SDK	software development kit
SDLC	System Development Life Cycle
SDO	standards development organization
SDP	Session Description Protocol
SDP	Service Discovery Protocol
SEI	Software Engineering Institute
SEM	security event management
SEND	Secure Neighbor Discovery
SEP	secure entry point
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHA-1	Secure Hash Algorithm 1
shim6	Site Multihoming by IPv6 Intermediation
SHS	Secure Hash Standard
SIA	Security Industry Association
SID	security identifier
SIEM	security information and event management
SIG	special interest group
SIIT	Stateless IP/ICMP Translation Algorithm
SIM	security information management
SIM	subscriber identity module
SIP	Session Initiation Protocol
SIS	safety instrumented system
SKEME	Secure Key Exchange Mechanism
SLA	service level agreement
SMB	Server Message Block
SME	subject matter expert
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMS	Systems Management Server
SMT	scar, mark and tattoo
SMTP	Simple Mail Transfer Protocol
SNL	Sandia National Laboratories
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol

SOA	service-oriented architecture
SOA	start of authority (resource record)
soBGP	Secure Origin Border Gateway Protocol
SoD	separation of duties
SOHO	small office/home office
SOP	standard operating procedure
SOR	system of records
SORN	system of records notice
SOX	Sarbanes-Oxley Act of 2002
SP	service pack
SP	special publication
SPD	security policy database
SPI	security parameters index
SPL	Structured Product Labeling
SPML™	Service Provisioning Markup Language™
SPP-ICS	System Protection Profile for Industrial Control Systems
SQL	Structured Query Language
SR	service release
SRES	signed response
SRTP	Secure Real-Time Transport Protocol
SS	subscriber station
SSDP	Simple Service Discovery Protocol
SSE-CMM	Systems Security Engineering-Capability Maturity Model
SSH	Secure Shell
SSI	Server Side Includes
SSID	service set identifier
SSL	Secure Sockets Layer
SSLF	Specialized Security-Limited Functionality
SSN	social security number
SSO	single sign-on
SSoD	static separation of duty
SSP	secure simple pairing
SSPI	Security Support Provider Interface
ST	security target
STA	station
STIG	security technical implementation guide
STS	security token service
SUID	Set-User-ID
SWSA	Semantic Web Services Initiative Architecture
SZ	security zone

T

TA	test assertion
TA	transmitter address
TACACS	Terminal Access Controller Access Control System
TAG	technical advisory group
TB	terabyte
TC	technical committee

TC68	ISO/IEC Technical Committee 68
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TDM	time division multiplexing
TDMA	time division multiple access
TEK	traffic encryption key
TERENA	Trans-European Research and Education Networking Association
TFT	thin film transistor
TFTP	Trivial File Transfer Protocol
TGS	ticket-granting service
TIA®	Telecommunications Industry Association
TID	tag identifier
TK	temporal key
TKIP	Temporal Key Integrity Protocol
TLD	top-level domain
TLS	Transport Layer Security
TMOVS	Modes of Operation Validation System for the Triple DES Algorithm
TOE	target of evaluation
TOS	trusted operating system
ToS	Type of Service
TPC	transmission power control
TPM	trusted platform module
TR	technical report
TRT	transport relay translator
TS	technical specification
TSA	time stamping authority
TSC	TKIP sequence counter
TSIG	Secret Key Transaction Authentication for DNS
TSIG	Transaction Signature
TSN	transitional security network
TSP	Time-Stamp Protocol
TT&E	test, training, and exercise
TTF	tag talks first
TTL	time to live
TTLS	Tunneled Transport Layer Security
TTP	trusted third party
TXT	text (record)

U

U.S.	United States
U.S.C.	United States Code
UAC	User Account Control
UART	universal asynchronous receiver/transmitter
UBR	Universal Description, Discovery and Integration (UDDI) Business Registry
UCC	Uniform Code Council, Inc.
UCE	unsolicited commercial email
UDDI™	Uniform Description, Discovery, and Integration™
UDF	Universal Disk Format

UDP	User Datagram Protocol
UFS	UNIX File System
UHF	ultra high frequency
UI	user interface
UK	United Kingdom
UL	Underwriters' Laboratories®
ULA	unique local address
ULP	upper layer protocol
UML®	Unified Modeling Language™
UMPC	ultra-mobile personal computer
UMTS	Universal Mobile Telecommunications System
UNII	Unlicensed National Information Infrastructure
UPC	Universal Product Code
UPnP	Universal Plug and Play
UPS	uninterruptible power supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USIM	UMTS Subscriber Identity Module *or* Universal Subscriber Identity Module
UTM	unified threat management
UUID	Universally Unique Identifier
UWB	ultrawideband

V

VB	Visual Basic
VB.NET	Visual Basic .NET
VBA	Visual Basic for Applications
VBScript	Visual Basic Script
VFD	variable frequency drive
VHD	virtual hard drive
VHF	very high frequency
VLAN	virtual local area network
VM	virtual machine
VMS	vulnerability management system
VoIP	Voice over Internet Protocol
VOIPSA	Voice over IP Security Alliance
VPN	virtual private network
VPNC	Virtual Private Network Consortium
VRRP	Virtual Router Redundancy Protocol

W

W3C®	World Wide Web Consortium
WAN	wide area network
WAP	wireless access point
WAP	Wireless Application Protocol
WaSP	Web Standards Project

WAVE	Wireless Access for Vehicular Environment
WAYF	Where Are You From
WCCP	Web Cache Coordination Protocol
W-CDMA	Wideband Code Division Multiple Access
WDS	wireless distribution system
WebDAV	Web Distributed Authoring and Versioning
WEP	Wired Equivalent Privacy
WfMC	Workflow Management Coalition
WfMS	workflow management system
WG	working group
WIDPS	wireless intrusion detection and prevention system
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless local area network
WMAN	wireless metropolitan area network
WMM®	Wi-Fi Multimedia™
WORM	write once, read many
WPA	Wi-Fi Protected Access
WPA2®	Wi-Fi Protected Access® 2
WPAN	wireless personal area network
WS	Web services
WSDL	Web Services Description Language
WSH	Windows Script Host
WS-I	Web services interoperability
WS-I	Web Services Interoperability Organization
WSS4J	Web Services Security for Java
WS-Security	Web Services Security
WSUS	Windows Server Update Services
WVE	Wireless Vulnerabilities and Exploits
WWAN	wireless wide area network
WWW	World Wide Web

XYZ

XACL	XML Access Control Language
XACML™	eXtensible Access Control Markup Language™
XCBC	XOR Cipher Block Chaining
XCCDF	eXtensible Configuration Checklist Description Format
XHTML	Extensible Hypertext Markup Language
XKMS	XML Key Management Specification
XML	Extensible Markup Language
XOR	exclusive OR
XrML	eXtensible Rights Markup Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformation
XSS	cross-site scripting
ZSK	zone signing key

Appendix A—References

Sources used in the development of the list of system and network security acronyms and abbreviations in this document include the following:

National Institute of Standards and Technology Publications, NIST Computer Security Division Resource Center Web site, http://csrc.nist.gov/

Internet Engineering Task Force (IETF), http://www.ietf.org/

Microsoft Hardware Developer Central, Glossary of Acronyms for PC and Server Technologies, http://www.microsoft.com/whdc/resources/support/glossary.mspx

Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/home/index.php

Appendix B—Former Acronyms

Over time, as organizations, technologies, or other entities change, some acronyms associated with them may lose their definitions and thus no longer be considered acronyms. This appendix presents selected former acronyms related to system and network security. As additional acronyms in this publication lose their definitions, readers are encouraged to send notification of these, along with references to authoritative sources of information, to securityacronyms@nist.gov for possible inclusion in future releases of this report.

IEEE	Originally defined as "Institute of Electrical and Electronics Engineers, Inc." Definition dropped by the organization (http://www.ieee.org/web/aboutus/home/index.html).
SOAP	Originally defined as "Simple Object Access Protocol." Definition dropped as of April 2007 (http://www.w3.org/TR/soap12-part1/#intro).