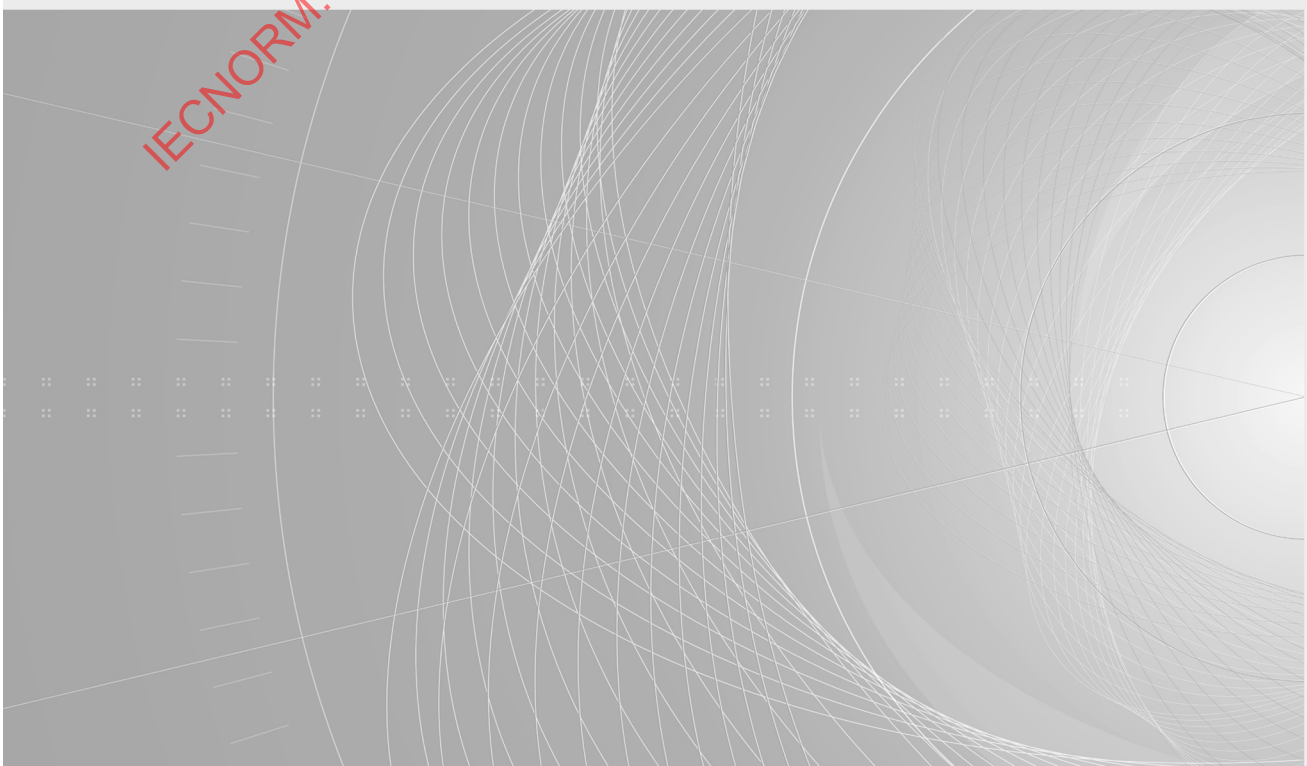
IEC/TS 62351-2

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

Power systems management and associated information exchange – Data and communications security –
Part 2: Glossary of terms



IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62351-2

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 2-8318-9956-7

CONTENTS

FOREWORD 9
1 Scope and object 11
2 Terms and definitions 11
2.1 Glossary references and permissions 11
2.2 Glossary of security and related communication terms 13
2.2.1 Abstract Communication Service Interface (ACSI) 13
2.2.2 Access 13
2.2.3 Access Authority 13
2.2.4 Access Control 13
2.2.5 Access Control List (ACL) 13
2.2.6 Accountability 13
2.2.7 Adequate Security 13
2.2.8 Advanced Encryption Standard (AES) 14
2.2.9 Alarm 14
2.2.10 Application Layer 14
2.2.11 Association 14
2.2.12 Assurance 14
2.2.13 Asymmetric Cipher 14
2.2.14 Asymmetric Cryptography 14
2.2.15 Asymmetric Key Pair 14
2.2.16 Attack 14
2.2.17 Audit 15
2.2.18 Audit Log 15
2.2.19 Audit Record Field 15
2.2.20 Audit Trail 15
2.2.21 Authentic Signature 15
2.2.22 Authentication 15
2.2.23 Authorization 15
2.2.24 Authorization Process 15
2.2.25 Authorized User 16
2.2.26 Availability 16
2.2.27 Back Door 16
2.2.28 Bandwidth 16
2.2.29 Biometric 16
2.2.30 Block Cipher 16
2.2.31 Boundary Protection 16
2.2.32 Buffer Overflow 16
2.2.33 Bump-in-the-Stack 17
2.2.34 Bump-in-the-Wire 17
2.2.35 Call Back 17
2.2.36 Certificate 17
2.2.37 Certificate Management 17
2.2.38 Certificate Revocation List (CRL) 17
2.2.39 Certification 17
2.2.40 Certification Authority (CA) 18

2.2.41 Chain of Custody 18
2.2.42 Challenge Handshake Authentication Protocol (CHAP) 18
2.2.43 Challenge-Response, Challenge-Response Protocol 18
2.2.44 Checksum 18
2.2.45 Cipher 18
2.2.46 Ciphertext 19
2.2.47 Cleartext 19
2.2.48 Client 19
2.2.49 Compromise 19
2.2.50 Computer Emergency Response Team (CERT) 19
2.2.51 Computer Virus 19
2.2.52 Confidentiality 19
2.2.53 Conformance Test 19
2.2.54 Control Network 20
2.2.55 Control System 20
2.2.56 Control System Operations 20
2.2.57 Cookie 20
2.2.58 Countermeasure 20
2.2.59 Cracker 20
2.2.60 Credential 21
2.2.61 Critical System Resource 21
2.2.62 Crypto-algorithm 21
2.2.63 Cryptographic Hash 21
2.2.64 Cryptographic Key 21
2.2.65 Cryptography 21
2.2.66 Cyber 21
2.2.67 Cyber Attack 21
2.2.68 Cyber Security 22
2.2.69 Cyclic Redundancy Check (CRC) 22
2.2.70 Data Authentication 22
2.2.71 Data Corruption 22
2.2.72 Data Encryption Standard (DES) 22
2.2.73 Data Integrity 22
2.2.74 Data Object (DO) 22
2.2.75 Data Security 22
2.2.76 Datagram 22
2.2.77 Decode 23
2.2.78 Decrypt 23
2.2.79 Decryption 23
2.2.80 De-Facto Standard 23
2.2.81 Defence in Depth 23
2.2.82 Denial of Service (DoS) 23
2.2.83 Designated Approving Authority (DAA) 24
2.2.84 Device 24
2.2.85 Diffie-Hellman Key Exchange 24
2.2.86 Digital Certificate 24
2.2.87 Digital Data 24
2.2.88 Digital Signature 24
2.2.89 Digital Signature Standard (DSS) 25

2.2.90 Distributed Control System (DCS) 25
2.2.91 Dongle 25
2.2.92 Eavesdropping 25
2.2.93 Electronic Deception 25
2.2.94 Elliptic Curve Cryptography 25
2.2.95 Encrypt 25
2.2.96 Encryption 25
2.2.97 Firewall 26
2.2.98 Flooding 26
2.2.99 Flow Control 26
2.2.100 Functions 26
2.2.101 Gateway 26
2.2.102 Generic Upper Layer Security (GULS) 26
2.2.103 Hacker 26
2.2.104 Hash Function 27
2.2.105 Honey Pot 27
2.2.106 Identification 27
2.2.107 IEEE 802.11i 27
2.2.108 Information Security 27
2.2.109 Instrumentation, Systems, and Automation Society (ISA) 27
2.2.110 Integrity 27
2.2.111 Intelligent Electronic Device (IED) 28
2.2.112 Intercept 28
2.2.113 Interchangeability 28
2.2.114 Interface 28
2.2.115 Internet Protocol security (IPsec) 28
2.2.116 Interoperability 28
2.2.117 Intruder 28
2.2.118 Intrusion Detection System (IDS) 29
2.2.119 Key 29
2.2.120 Key Distribution 29
2.2.121 Key Logger 29
2.2.122 Key Pair 29
2.2.123 Key Update 29
2.2.124 Latency 29
2.2.125 Local Area Network (LAN) 29
2.2.126 Malicious Code 29
2.2.127 Malware 30
2.2.128 Management Information Base (MIB) 30
2.2.129 Man-in-the-Middle Attack 30
2.2.130 Manufacturing Message Specification (MMS) 30
2.2.131 Masquerade 30
2.2.132 Mockingbird 31
2.2.133 Multicast 31
2.2.134 Network Layer Protocol 31
2.2.135 Network Management 31
2.2.136 Non-repudiation 31
2.2.137 Object Identifier (OID) 31
2.2.138 Open Protocol 31

2.2.139 Open System 31
2.2.140 Open Systems Architecture 32
2.2.141 Open Systems Interconnection – Reference Model (OSI-RM) 32
2.2.142 Password 32
2.2.143 Personal Identification Number (PIN) 32
2.2.144 Phishing 32
2.2.145 Physical Layer Protocol 32
2.2.146 Plaintext 32
2.2.147 Point-to-Point Protocol (PPP) 33
2.2.148 Port Scanning 33
2.2.149 Pretty Good Privacy (PGP) 33
2.2.150 Private Key 33
2.2.151 Protection Profile 33
2.2.152 Proxy, Proxy Server 33
2.2.153 Pseudorandom Number Generator (PRNG) 34
2.2.154 Public Key 34
2.2.155 Public Key Asymmetric Cryptographic Algorithm 34
2.2.156 Public Key Certificate 34
2.2.157 Public Key Cryptography 34
2.2.158 Public Key Infrastructure (PKI) 35
2.2.159 Replay Attack 35
2.2.160 Repudiation 35
2.2.161 Risk 35
2.2.162 Risk Assessment 35
2.2.163 Risk Management 35
2.2.164 Rivest, Shamir and Adleman (RSA) 36
2.2.165 Role Based Access Control (RBAC) 36
2.2.166 Secret Key 36
2.2.167 Secret Key Encryption 36
2.2.168 Secret Key Symmetric Cryptographic Algorithm 36
2.2.169 Secure Hash Algorithm (SHA) 36
2.2.170 Secure Shell (SSH) 36
2.2.171 Secure Sockets Layer (SSL) 36
2.2.172 Secure/ Multipurpose Internet Mail Extensions (S/MIME) 37
2.2.173 Security 37
2.2.174 Security Domain 37
2.2.175 Security Guidelines 37
2.2.176 Security Management 37
2.2.177 Security Performance 37
2.2.178 Security Perimeter 37
2.2.179 Security Policy 38
2.2.180 Security Risk Assessment 38
2.2.181 Security Services 38
2.2.182 Server 38
2.2.183 Session Key 38
2.2.184 Shoulder Surfing 38
2.2.185 Signature Certificate 38
2.2.186 Simple Network Management Protocol (SNMP) 38
2.2.187 Smart Card 39

2.2.188 Smurf 39
2.2.189 Sniffing 39
2.2.190 Social Engineering 39
2.2.191 Spoof 39
2.2.192 Spyware 39
2.2.193 Strong Authentication 39
2.2.194 Strong Secret 39
2.2.195 Supervisory Control and Data Acquisition (SCADA) 39
2.2.196 Symmetric Cryptography 40
2.2.197 Symmetric Key 40
2.2.198 Symmetric Key Algorithm 40
2.2.199 SYN Flood 40
2.2.200 Tamper Detection 40
2.2.201 Tampering 40
2.2.202 TASE.2 40
2.2.203 Threat 40
2.2.204 Throughput 40
2.2.205 Traffic Analysis 41
2.2.206 Transport Level Security (TLS) 41
2.2.207 Trap Door 41
2.2.208 Triple DES 41
2.2.209 Trojan Horse 41
2.2.210 Trust 41
2.2.211 Tunnel 42
2.2.212 Unforgeable 42
2.2.213 Update Key 42
2.2.214 Virtual Private Network (VPN) 42
2.2.215 Virus 43
2.2.216 Vulnerability 43
2.2.217 Vulnerability Assessment 43
2.2.218 Wide Area Network (WAN) 43
2.2.219 WiFi 43
2.2.220 Wired Equivalent Privacy (WEP) 43
2.2.221 Wireless Application Protocol (WAP) 44
2.2.222 Wireless LAN (WLAN) 44
2.2.223 Worm 44
2.2.224 X.509 44
3 Abbreviations 45
3.1.1 3DES 45
3.1.2 ACL 45
3.1.3 ACSI 45
3.1.4 AES 45
3.1.5 AGA 45
3.1.6 ANSI 45
3.1.7 BIS 45
3.1.8 BSI 45
3.1.9 BTW 45
3.1.10 CA 45
3.1.11 CERT 45

3.1.12 CHAP 45
3.1.13 CIP 45
3.1.14 CRC 45
3.1.15 CRL 45
3.1.16 DAA 45
3.1.17 DCS 45
3.1.18 DES 45
3.1.19 DO 45
3.1.20 DoS 45
3.1.21 DSS 45
3.1.22 ECC 45
3.1.23 EM/RF 45
3.1.24 EMS 45
3.1.25 FIPS 45
3.1.26 GULS 45
3.1.27 ICCP 45
3.1.28 IDS 46
3.1.29 IED 46
3.1.30 IEEE 46
3.1.31 IETF 46
3.1.32 IPS 46
3.1.33 IPsec 46
3.1.34 ISA 46
3.1.35 ISO 46
3.1.36 IT 46
3.1.37 LAN 46
3.1.38 MIB 46
3.1.39 MMS 46
3.1.40 NERC 46
3.1.41 NIST 46
3.1.42 OID 46
3.1.43 OSI-RM 46
3.1.44 PGP 46
3.1.45 PICS 46
3.1.46 PIN 46
3.1.47 PIXIT 46
3.1.48 PKI 46
3.1.49 PLC 46
3.1.50 PLC 47
3.1.51 PPP 47
3.1.52 PRNG 47
3.1.53 RA 47
3.1.54 RBAC 47
3.1.55 RSA 47
3.1.56 RTU 47
3.1.57 SCADA 47
3.1.58 SHA 47
3.1.59 SNMP 47
3.1.60 SSH 47

3.1.61 SSL 47
3.1.62 TASE.2 47
3.1.63 TDEA 47
3.1.64 TDES 47
3.1.65 TLS 47
3.1.66 VPN 47
3.1.67 WAN 47
3.1.68 WEP 47
3.1.69 WiFi 47
3.1.70 WLAN 47
3.1.71 WPA 47
BIBLIOGRAPHY 48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 2: Glossary of terms

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-2, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/853/DTS	57/922/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

A list of all parts of the IEC 62351 series, under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual edition of this document may be issued at a later date.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 2: Glossary of terms

1 Scope and object

This part of IEC 62351 covers the key terms used in the IEC 62351 series, and is not meant to be a definitive list. Most terms used for cyber security are formally defined by other standards organizations, and so are included here with references to where they were originally defined.

2 Terms and definitions

2.1 Glossary references and permissions

With permission granted by the appropriate organizations, the definitions in this glossary were copied from the following sources:

- **[API 1164] American Petroleum Institute.** This standard on SCADA security provides guidance to the operators of Oil and Gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines, but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system. This document embodies the "API Security Guidelines for the Petroleum Industry." This guideline is specifically designed to provide the operators with a description of industry practices in SCADA Security, and to provide the framework needed to develop sound security practices within the operator's individual companies.
- **[ATIS]** ATIS Telecom Glossary 2007 at http://www.atis.org/glossary/. This web site incorporates and supersedes T1.523-2001, the ATIS Telecom Glossary of 2000 which was an expansion of FS-1037C, the Federal Standard 1037, *Glossary of Telecommunication Terms* initially published in 1980[1].
- **[FIPS-140-2]** This is the US Federal Information Processing Standard Publication 140-2, titled "*Security Requirements for Cryptographic Modules*".
- **[ISA99]** This ISA Technical Report provides a framework for developing an electronic security program and provides a recommended organization and structure for the security plan. The information provides detailed information about the minimum elements to include. Site or entity specific information should be included at the appropriate places in the program.
- **[ISO/IEC 27002:2005]** "Information technology - Security techniques - Code of practice for information security management" is an internationally-accepted standard of good practice for information security. This standard was originally the British Standard, BS7799, and later was termed ISO/IEC 17799, and was recently renamed to ISO/IEC 27002:2005.

---

[1] The ATIS Document Center is the leading, online resource to published and pre-published telecommunication standards, technical reports and requirements, guidelines produced by the ATIS sponsored industry forums and committees. The web site is http://www.atis.org Copyright © Alliance for Telecommunications Industry Solutions, 2001 in connection with all copyrightable subject matter created by and in Committee T1 and contained herein or comprised hereof. All Rights Reserved. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628-6380. ATIS is online at <http://www.atis.org>.

- **[ISO/IEC]** Many ISO/IEC documents contain term definitions that have been accepted as international standards. These documents are individually cited.
- **[NIST SP 800-53: December 2007]** National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems.
- **[NIST SP 800-82: September 2007]** National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security
- **[NIST SP 800-xx]** Other National Institute of Standards and Technology (NIST) documents are cited.
- **[NIST IR 7298]** National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms. This document usually cites other sources, which are therefore cited directly in this document.
- **[RFC 2828]** IETF RFC 2828 standard glossary of terms used for the Internet[2]

Other sources are cited as necessary.

2 The Internet Society. Copyright I The Internet Society (2000). All Rights Reserved. This document (RFC 2828) and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

2.2 Glossary of security and related communication terms

2.2.1 Abstract Communication Service Interface (ACSI)

A virtual interface to an IED providing abstract communication services, e.g. connection, variable access, unsolicited data transfer, device control and file transfer services, independent of the actual communication stack and profiles used. [IEC 61850 series]

2.2.2 Access

The ability and means to communicate with or otherwise interact with a system in order to use system resources to either handle information or gain knowledge of the information the system contains. [RFC 2828]

2.2.3 Access Authority

An entity responsible for monitoring and granting access privileges for other authorized entities. [RFC 2828]

2.2.4 Access Control

1. Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO/IEC 18028-2:2006]
2. Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [RFC 2828]
3. Rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist. [ISO/IEC 27002:2005]

2.2.5 Access Control List (ACL)

A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources. [RFC 2828]

2.2.6 Accountability

1. The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC 7498-2]
2. The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions. [RFC 2828]

2.2.7 Adequate Security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls. [NIST SP 800-53]

2.2.8 Advanced Encryption Standard (AES)

1. A symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard (FIPS) 197. [ISO/IEC 18028-4:2005]
2. The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. [NIST SP 800-46]
3. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. [FIPS 1]

2.2.9 Alarm

A device or function that signals the existence of an abnormal condition by making an audible or visible discrete change, or both, so as to attract attention to that condition. [ANSI/ISA 5.1:1979]

2.2.10 Application Layer

See Open Systems Interconnection—Reference Model Layer 7

2.2.11 Association

A cooperative relationship between system entities, usually for the purpose of transferring information between them. [RFC 2828]

2.2.12 Assurance

In the context of security: Grounds for confidence that a deliverable meets its security objectives. [ISO/IEC 15408-1]

NOTE This definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfils specified requirements. [ISO/IEC Guide 2]

2.2.13 Asymmetric Cipher

Cipher based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption. [ISO/IEC 18033-1].

2.2.14 Asymmetric Cryptography

A modern branch of cryptography (popularly known as "public- key cryptography") in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm. [RFC 2828]

2.2.15 Asymmetric Key Pair

A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1:1997]

2.2.16 Attack

1. An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. [RFC 2828]
2. [An] intentional act of attempting to bypass one or more of the following security controls of an information system (IS): non-repudiation, authentication, integrity, availability, or confidentiality. [ATIS]

2.2.17 Audit

1. Formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity. [ISO/IEC 18028-3:2005]
2. To conduct an independent review and examination of system records and activities in order to test the adequacy and effectiveness of data security and data integrity procedures, to ensure compliance with established policy and operational procedures, and to recommend any necessary changes. [ATIS]

2.2.18 Audit Log

Computer files containing details of amendments to records, which may be also used in the event of system recovery being required. Enabling this feature usually incurs some system overhead, but it does permit subsequent review of all system activity. [ISO/IEC 27002:2005]

NOTE Audit trails are crucial to the technical and forensic analysis of possible security breaches.

2.2.19 Audit Record Field

A field containing information regarding all entities in a transaction, and indicators of the types of processing performed by those entities. [ATIS]

2.2.20 Audit Trail

A record or series of records, which allows the processing carried out by a computer or clerical system to be accurately identified. Often enables verification of the authenticity of amendments, including details of the users who created and authorised them. [ISO/IEC 27002:2005]

NOTE Audit trails are crucial to the technical and forensic analysis of possible security breaches.

2.2.21 Authentic Signature

A signature (particularly a digital signature) that can be trusted because it can be verified. [RFC 2828]

2.2.22 Authentication

1. [Any] Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [ATIS]
2. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [NIST SP 800-53]
3. Evidence by proper signature or seal that a document is genuine and official. [ATIS]
4. A process that establishes the origin of information, or determines an entity's identity. [RFC 2828]
5. The provision of assurance of the claimed identity of an entity [ISO/IEC 10181-2:1996]

2.2.23 Authorization

A right or a permission that is granted to a system entity to access a system resource. [RFC 2828]

2.2.24 Authorization Process

An "authorization process" is a procedure for granting [to a system entity the] rights [to access a system resource]. [RFC 2828]

2.2.25 Authorized User

In security, a user who may, according to an organization's security policy, perform an operation. [ATIS]

2.2.26 Availability

1. The property of being accessible and usable upon demand by an authorized entity [ISO/IEC 13335-1:2004]
2. The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. [RFC 2828]

2.2.27 Back Door

A hardware or software mechanism that (a) provides access to a system and its resources by other than the usual procedure, (b) was deliberately left in place by the system's designers or maintainers, and (c) usually is not publicly known. [RFC 2828]

NOTE Similar to Trap Door, but usually not implemented for malicious reasons.

2.2.28 Bandwidth

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. [RFC 2828]

2.2.29 Biometric

1. A physical or behavioural characteristic of a human being. [NIST SP 800-32]
2. A measurable physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics. [FIPS 201]

2.2.30 Block Cipher

Symmetric encryption algorithm with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1]

2.2.31 Boundary Protection

Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). [NIST SP 800-53]

2.2.32 Buffer Overflow

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. [NIST SP 800-28]

2.2.33 Bump-in-the-Stack

Insertion of security modules, which snoop data flowing between a TCP/IPv4 module and network card driver modules and translate IPv4 into IPv6 and vice versa, into the hosts, and makes them self-translators. [RFC 2767]

2.2.34 Bump-in-the-Wire

In security, the addition of encryption boxes at either end of a communications link, just after the connection of the devices/system. One encryption box takes the plain text messages from one device and encrypts them, while the other box receives the encrypted messages and decrypts them back into plain text, and vice versa. This approach provides external encryption and avoids the need to embed an encryption function within the device. [Common usage]

2.2.35 Call Back

An authentication technique for terminals that remotely access a computer via telephone lines. The host system disconnects the caller and then calls back on a telephone number that was previously authorized for that terminal. [RFC 2828]

2.2.36 Certificate

1. In cryptography, the public key and the identity of an entity, with other information, rendered unforgeable (*not able to be forged*) by digitally signing the entire information with the private key of the issuing certification authority. [ATIS]
2. A digital representation of information which at least:
   1) identifies the certification authority issuing it,
   2) names or identifies its subscriber,
   3) contains the subscriber's public key,
   4) identifies its operational period, and
   5) is digitally signed by the certification authority issuing it. [NIST SP 800-32]

2.2.37 Certificate Management

[The] process whereby certificates [...] are generated, stored, protected, transferred, loaded, used, and destroyed. [ATIS]

2.2.38 Certificate Revocation List (CRL)

1. A list of revoked public key certificates created and digitally signed by a Certification Authority. [NIST SP 800-63]
2. A list of revoked but un-expired certificates issued by a CA. [NIST SP 800-21 [2nd Edition]]

2.2.39 Certification

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST SP 800-37]

2.2.40 Certification Authority (CA)

1. An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys. [ISO/IEC 13888-1:2004]
2. A trusted third party 'clearing house' that issues digital signatures and digital certificates. [ISO/IEC 27002:2005]
3. An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. [RFC 2828]

2.2.41 Chain of Custody

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. [NIST SP 800-72]

2.2.42 Challenge Handshake Authentication Protocol (CHAP)

A peer entity authentication method for PPP, using a randomly generated challenge and requiring a matching response that depends on a cryptographic hash of the challenge and a secret key. [RFC 2828]

2.2.43 Challenge-Response, Challenge-Response Protocol

1. An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge value. [RFC 2828]
2. An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. [NIST SP 800-63]

2.2.44 Checksum

The sum of a group of data items, which sum is used for checking purposes to detect error or manipulation during transmission. See hash total. [ATIS]

2.2.45 Cipher

1. Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1]
2. A cipher is any cryptographic system in which arbitrary symbols, or groups of symbols, represent units of plain text of regular length, usually single letters, or in which units of plain text are rearranged, or both, in accordance with certain predetermined rules. [ATIS]

2.2.46 Ciphertext

Data which has been transformed to hide its information content [ISO/IEC 10116:2006]

2.2.47 Cleartext

Synonym: *Plaintext*. Unencrypted information. [ATIS]

2.2.48 Client

A device or application receiving or requesting services or information from a server application. [ATIS]

2.2.49 Compromise

1. Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NIST SP 800-32]
2. The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters). [FIPS 140-2]

2.2.50 Computer Emergency Response Team (CERT)

The CERT is generally recognised as the Internet's official emergency team. [ISO/IEC 27002:2005]

NOTE This term can also be used within companies or other groups to describe emergency teams.

2.2.51 Computer Virus

A computer virus is similar to a Trojan horse because it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference between a virus and a Trojan horse is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met. [NIST SP 800-46]

2.2.52 Confidentiality

1. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST SP 800-53]
2. Of classified or sensitive data, the degree to which the data have not been compromised; i.e., have not been made available or disclosed to unauthorized individuals, processes, or other entities. [ATIS]
3. Assurance that information is not disclosed to unauthorized persons, processes, or devices. [ATIS]
4. A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities, or processes. [ATIS]
5. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 7498-2]

2.2.53 Conformance Test

A test performed by an independent body to determine if a particular piece of equipment satisfies the criteria in a specified controlling document, such as a Federal standard, an American National Standard, a Military Standard, or a Military Specification. Contrast with acceptance test. [ATIS]

2.2.54 Control Network

Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site. [NIST SP 800-82]

2.2.55 Control System

1. A system constituted by a controlled system, its controlling system, the measuring element and the associated transducing elements. [IEV 351-28-06]
2. A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems. [NIST SP 800-82]

2.2.56 Control System Operations

Control system operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a manufacturing facility. Control system operations include:

- facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials into end-products
- functions that may be performed by physical equipment, human effort, and information systems
- managing information about the schedules, use, capability, definition, history, and status of all of resources (personnel, equipment, and material) within the facility. [ISA99]

2.2.57 Cookie

A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. [NIST SP 800-46]

2.2.58 Countermeasure

1. An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. [RFC 2828]
2. Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. [NIST SP 800-53]

2.2.59 Cracker

1. Hacker jargon to indicate "one who breaks security on a system." [ATIS]

Note: The term cracker was coined ca. 1985 by hackers in defense against journalistic misuse of the term hacker. [ATIS]

2. An individual who, with malicious intent, gains or tries to gain illegal access to computers or computer programs. [ATIS]

NOTE Synonym: password cracker. [ATIS]

2.2.60 Credential

Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. [RFC 2828]

2.2.61 Critical System Resource

A condition of a service or other system resource such that denial of access to (i.e., lack of availability of) that resource would jeopardize a system user's ability to perform a primary function or would result in other serious consequences. [RFC 2828]

Note: In addition to denial of access, other security threats such as lack of integrity of information can also make a resource categorized as a critical system.

2.2.62 Crypto-algorithm

[A] well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc. [ATIS]

2.2.63 Cryptographic Hash

1. Function that maps octet strings of any length to octet strings of fixed length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output. The precise security requirements depend on the application. [ISO/IEC 18033-2:2006]
2. A mathematical function that maps values from a large (or even very large) domain into a smaller range, and is (a) one-way in that it is computationally infeasible to find any input which maps to any pre-specified output; and (b) collision-free in that it is computationally infeasible to find any two distinct inputs which map to the same output. [ATIS]

2.2.64 Cryptographic Key

A mathematical value that is used (a) in an algorithm to generate cipher text from plain text or vice versa, and (b) to determine the operation of a cryptographic function (e.g., the synchronized generation of keying material), or a digital signature computation or validation. [ATIS]

2.2.65 Cryptography

1. [The] art or science concerning the principles, means, and methods for rendering plain information unintelligible, and for restoring encrypted information to intelligible form. [ATIS]
2. The branch of cryptology that treats of the principles, means, and methods of designing and using cryptosystems. [ATIS]
3. The discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO/IEC 18014-2:2002]

2.2.66 Cyber

Loosely, a prefix referring to anything related to computers or networking. [ATIS]

2.2.67 Cyber Attack

See Attack

2.2.68 Cyber Security

Synonym: Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [ATIS]

2.2.69 Cyclic Redundancy Check (CRC)

A method to ensure data has not been altered after being sent through a communication channel. [NIST SP 800-72]

2.2.70 Data Authentication

Verification of the authenticity of data. Authentication techniques usually form the basis for all forms of access control to systems or data. [ISO/IEC 27002:2005]

2.2.71 Data Corruption

An accidental or intentional violation of data integrity. [ATIS]

2.2.72 Data Encryption Standard (DES)

1. [A] cryptographic algorithm for the protection of unclassified computer data and published by the National Institute of Standards and Technology in Federal Information Processing Standard Publication 46-1. [ATIS]

NOTE DES is not approved for protection of national security classified information. [ATIS]

2. A well-known symmetric encryption mechanism using a 56 bit key. Due to its short key length DES was replaced by the AES, but is still used in multiple encryption mode, e.g., 3DES or Triple DES (FIPS 46-3). [ISO/IEC 18028-4:2005]

2.2.73 Data Integrity

1. The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [RFC 2828]
2. [The] condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [ATIS]
3. The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval. [FIPS 140-2]

2.2.74 Data Object (DO)

Part of a logical node object representing specific information, e.g., status or measurement. From an object-oriented point of view, a data object is an instance of a class data object. DOs are normally used as transaction objects; i.e., they are data structures. [IEC 61850 series]

2.2.75 Data Security

[The] protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. [ATIS]

2.2.76 Datagram

In packet switching, a self-contained packet, independent of other packets, that contains information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on prior exchanges between the equipment and the network.

NOTE Unlike virtual call service, when datagrams are sent, there are no call establishment or clearing procedures. Thus, the network may not be able to provide protection against loss, duplication, or mis-delivery. [ATIS]

2.2.77 Decode

1. To convert data by reversing the effect of previous encoding. [FIPS 140-2]
2. To interpret a code. [ATIS]
3. [To] convert encoded text into equivalent plain text by means of a code. [ATIS] [FIPS 140-2]

NOTE Decoding does not include deriving plain text by cryptanalysis. [ATIS]

2.2.78 Decrypt

1. [A] generic term encompassing decode and decipher. [ATIS]
2. To convert encrypted text into its equivalent plain text by means of a cryptosystem. (This does not include solution by cryptanalysis.) [ATIS]

NOTE The term "decrypt" covers the meanings of "decipher" and "decode." [ATIS]

2.2.79 Decryption

1. Reversal of a corresponding encryption. [ISO/IEC 18033-1]
2. The process of changing ciphertext into plaintext using a cryptographic algorithm and key. [RFC 2828]

2.2.80 De-Facto Standard

A standard that is widely accepted and used, but lacks formal approval by a recognized standards organization. [ATIS]

NOTE Some security technologies are proprietary to certain vendors even though widely used and often quite effective. However, these should be regarded as de-facto standards, until they are formally standardized.

2.2.81 Defence in Depth

A security architecture based on the idea that any one point of protection may, and probably will, be defeated. It implies layers of security and detection, even on single systems and provides the following features:

- Attackers are faced with breaking through or bypassing each layer without being detected.
- A flaw in one layer can be protected by capabilities in other layers.
- System security becomes a set of layers within the overall network security.
- Security is improved by requiring the attacker to be perfect while ignorant. [ISA99]

2.2.82 Denial of Service (DoS)

1. The prevention of authorized access to a system resource or the delaying of time-critical operations and functions. [RFC 2828]
2. The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) [NIST SP 800-27A]

2.2.83 Designated Approving Authority (DAA)

[The] official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. *Synonyms:* accrediting authority, delegated accrediting authority, designated accrediting authority. [ATIS]

2.2.84 Device

A mechanism or piece of equipment designed to serve a purpose or perform a function. [IEEE Std 100-1996, IEEE Dictionary of Electrical and Electronic Terms]

2.2.85 Diffie-Hellman Key Exchange

A cryptographic protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. [published as W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), 644-654]

2.2.86 Digital Certificate

A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. [RFC 2828]

2.2.87 Digital Data

1. Data represented by discrete values or conditions, as opposed to analogue data. [ATIS]
2. Discrete representations of quantized values of variables, *e.g.*, the representation of numbers by digits, perhaps with special characters and the “space” character. [ATIS]

2.2.88 Digital Signature

1. A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. [RFC 2828]
2. Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO/IEC 13888-1:2004]
3. A cryptographic modification of data that provides: (a) origin authentication, (b) data integrity, and (c) signer non-repudiation (when associated with a data unit and accompanied by the corresponding public-key certificate). A cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonym electronic signature. [ATIS]
4. The result of a cryptographic transformation of data which, when properly implemented, provides the services of:
   - origin authentication,
   - data integrity,
   - signer non-repudiation. [FIPS 140-2]

2.2.89 Digital Signature Standard (DSS)

A standard for digital signing, including the Digital Signing Algorithm, approved by the National Institute of Standards and Technology, defined in NIST FIPS PUB 186, "Digital Signature Standard," published May, 1994 by the U.S. Dept. of Commerce. [NIST SP 800-53]

2.2.90 Distributed Control System (DCS)

In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit. [ISA dictionary 2003]

2.2.91 Dongle

A portable, physical, electronic device that is required to be attached to a computer to enable a particular software program to run. [RFC 2828]

2.2.92 Eavesdropping

Passive wiretapping done secretly, i.e., without the knowledge of the originator or the intended recipients of the communication. [RFC 2828]

2.2.93 Electronic Deception

1. The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons.

NOTE Among the types of electronic deception are: (a) manipulative electronic deception–Actions to eliminate revealing or convey misleading, telltale indicators that may be used by hostile forces; (b) simulative electronic deception–Actions to represent friendly notional or actual capabilities to mislead hostile forces; (c) imitative electronic deception–The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. [ATIS]

2. Deliberate activity designed to mislead an enemy in the interpretation or use of information received by his electronic systems. [ATIS]

2.2.94 Elliptic Curve Cryptography

A type of asymmetric cryptography based on mathematics of groups that are defined by the points on a curve. [RFC 2828]

2.2.95 Encrypt

1. [A] generic term encompassing encipher and encode. [ATIS]

2. To convert plain text into unintelligible forms by means of a cryptosystem. *Note*: The term encrypt covers the meanings of encipher and encode. [ATIS]

2.2.96 Encryption

1. (Reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1]

2. Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption”, which is a transformation that restores encrypted data to its original state. [RFC 2828]

2.2.97 Firewall

An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). [RFC 2828]

NOTE Firewalls may not always be gateways, and may be considered as mechanisms to separate security domains or multiple networks

2.2.98 Flooding

An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly. [RFC 2828]

2.2.99 Flow Control

A procedure or technique to ensure that information transfers within a system are not made from one security level to another security level, and especially not from a higher level to a lower level. [RFC 2828]

2.2.100 Functions

Tasks which are performed through automation by computer systems with or without direct user interactions. Functions rely on one or more software applications that may exchange data with other applications. [Common Usage]

2.2.101 Gateway

A relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other; an intermediate system that is the interface between two computer networks. [RFC 2828]

2.2.102 Generic Upper Layer Security (GULS)

A five-part standard (ISO/IEC 11586) for the exchange of security information and security-transformation functions that protect confidentiality and integrity of application data. [RFC 2828]

2.2.103 Hacker

1. A person who breaks into, or attempts to break into, or use, a computer network or system without authorization, often at random, for personal amusement or gratification, and not necessarily with malicious intent [ATIS]
2. A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term. See also: cracker. [RFC 1392]
3. An individual whose objective is to penetrate the security defences of a third party computer system or network. [ISO/IEC 27002:2005]
4. A person who uses a computer resource in a manner for which it is not intended or which is in conflict with the terms of an acceptable-use policy, but (unlike the work of a cracker) is not necessarily malicious in intent. [ATIS]

2.2.104 Hash Function

1. An algorithm that computes a value based on a data object (such as a message or file; usually variable-length; possibly very large), thereby mapping the data object to a smaller data object (the "hash result") which is usually a fixed-size value. [RFC 2828]
2. A function which maps strings of bits to fixed-length strings of bits, satisfying two properties.

– it is computationally infeasible to find for a given output, an input which maps to this output;

– it is computationally infeasible to find for a given input, a second input which maps to the same output. [ISO/IEC 9796-3:2006]

2.2.105 Honey Pot

1. A system (e.g., a web server) or a system resource (e.g., a file on a server), that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. [RFC 2828]
2. Generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user. [ISO/IEC 18043:2006]

2.2.106 Identification

An act or process that presents an identifier to a system so that the system can recognize a system entity and distinguish it from other entities. [RFC 2828]

2.2.107 IEEE 802.11i

International Electrical and Electronic Engineers (IEEE) Standard for Information technology -Telecommunications and information exchange between system-Local and metropolitan area networks -Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 6: Medium Access Control (MAC) Security Enhancements (IEEE 802.11i)

2.2.108 Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NIST SP 800-53]

2.2.109 Instrumentation, Systems, and Automation Society (ISA)

ISA is a non-profit professional organization for instrument engineers that was originally known as the Instrument Society of America. The society is more commonly known by its acronym, ISA. [ISA]

2.2.110 Integrity

1. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [NIST SP 800-53]
2. The property that sensitive data have not been modified or deleted in an unauthorized and undetected manner. [FIPS 140-2]
3. Property that sensitive data has not been modified or deleted in an unauthorised and undetected manner. [ISO/IEC 19790:2006]

2.2.111 Intelligent Electronic Device (IED)

Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, or controllers) [AGA 12]

2.2.112 Intercept

1. To gain possession of communications intended for others without their consent, and, ordinarily, without delaying or preventing the transmission. [ATIS]

NOTE An intercept may be an authorized or unauthorized action.

2. The acquisition of a transmitted signal with the intent of delaying or eliminating receipt of that signal by the intended destination user. [ATIS]

2.2.113 Interchangeability

1. The ability to exchange hardware components having the same form, fit, and function, across platforms, without affecting the functionality of the system. [ATIS]
2. A condition which exists when two or more items possess such functional and physical characteristics as to be equivalent in performance and durability, and are capable of being exchanged one for the other without alteration of the items themselves, or of adjoining items, except for adjustment, and without selection for fit and performance. [ATIS]

2.2.114 Interface

1. Shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate. [IEV 351-21-35]
2. A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [FIPS 140-2]

2.2.115 Internet Protocol security (IPsec)

A collective name for that architecture and set of protocols. (Implementation of IPsec protocols is optional for IP version 4, but mandatory for IP version 6.) [RFC 2828]

2.2.116 Interoperability

1. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. [ATIS]
2. Allows applications executing on separate hardware platforms, or in multi-processing environments on the same platform, to share data and cooperate in processing it through communications mechanisms such as remote procedure calls, transparent file access, etc. [ATIS]
3. The capability to provide useful and cost-effective interchange of electronic data among, e.g., different signal formats, transmission media, applications, industries, or performance levels. [ATIS]

2.2.117 Intruder

An entity that gains or attempts to gain access to a system or system resource without having authorization to do so. [RFC 2828]

2.2.118 Intrusion Detection System (IDS)

1. A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. [RFC 2828]
2. Information system used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in Information Systems and networks. [ISO/IEC 18043:2006]

2.2.119 Key

A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. [NIST SP 800-63]

2.2.120 Key Distribution

The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. [RFC 2828]

2.2.121 Key Logger

A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures. [NIST SP 800-82]

2.2.122 Key Pair

1. Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key. [NIST SP 800-32]
2. A public key and its corresponding private key used with a public key algorithm. [RFC 2828]

2.2.123 Key Update

Derive a new key from an existing key. [RFC 2828]

2.2.124 Latency

For store and forward devices: The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port. For bit forwarding devices: The time interval starting when the end of the first bit of the input frame reaches the input port and ending when the start of the first bit of the output frame is seen on the output port. [RFC 1242]

2.2.125 Local Area Network (LAN)

A communications network designed to connect computers and other intelligent devices in a limited geographic area (typically under 10 km). [ATIS]

2.2.126 Malicious Code

A program or part of a program which is deliberately coded in order to cause an unexpected undesired event. [ISO/IEC 27002:2005]

2.2.127 Malware

1. Malicious software, such as a virus or a Trojan horse, designed specifically to damage or disrupt a system. [ISO/IEC 18028-1:2006]
2. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware). [NIST SP 800-53]

2.2.128 Management Information Base (MIB)

A MIB is a type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using Abstract Syntax Notation One (ASN.1), the software that performs the parsing is a MIB compiler. The database is hierarchical (tree structured) and entries are addressed through object identifiers. Internet documentation RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", and its two companions, RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol" (SNMP) [IETF RFCs]

2.2.129 Man-in-the-Middle Attack

1. An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data travelling between them. [NIST SP 800-63]
2. A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association. [RFC 2828]

2.2.130 Manufacturing Message Specification (MMS)

1. ISO 9506 is an Application Layer communication specification, in accord with the OSI communication model. It provides a set of services appropriate to communications between automated equipment and systems that interrogate or control them. Its description of interactions follows the client server model. It is suitable for use over any network that supports full-duplex, reliable communication, such as the Internet. ISO 9506-1:2003 provides a set of abstract models of information objects that may be found in such automated systems, and the specifications of a set of abstract services that operate on these models. ISO 9506-2 provides the protocol for the messages to be exchanged between client and server to realize support for the abstract services defined in Part 1. [ISO 9506-1:2003]
2. MMS is one of the communication protocols that IEC 61850 is mapped to. [IEC 61850 series]

2.2.131 Masquerade

The pretence by an entity to be a different entity in order to gain unauthorized access. [ATIS]

2.2.132 Mockingbird

A type of Trojan Horse virus program which intercepts communications between users and hosts and provides system-like responses, whilst usually storing the users responses for later (sometimes malicious) use. [ISO/IEC 27002:2005]

2.2.133 Multicast

1. In a network, a technique that allows data, including packet form, to be simultaneously transmitted to a selected set of destinations. [ATIS]

NOTE Some networks, such as Ethernet, support multicast by allowing a network interface to belong to one or more multicast groups.

2. To transmit identical data simultaneously to a selected set of destinations in a network, usually without obtaining acknowledgement of receipt of the transmission. [ATIS]

2.2.134 Network Layer Protocol

Protocols for routing of messages through a complex network. Layer 3 of the OSI reference model. [ATIS]

2.2.135 Network Management

Process of planning, designing, implementing, operating, monitoring and maintaining a network. [ISO/IEC 18028-1:2006]

2.2.136 Non-repudiation

1. The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later [ISO/IEC 13888-1: ISO 7498-2]

2. A security service that provides protection against false denial of involvement in a communication. [RFC 2828]

2.2.137 Object Identifier (OID)

An official, globally unique name for a thing, written as a sequence of integers (which are formed and assigned as defined in the ASN.1 standard) and used to reference the thing in abstract specifications and during negotiation of security services in a protocol. [RFC 2828]

2.2.138 Open Protocol

Protocol whose stack is either standardized or publicly available. [ATIS]

2.2.139 Open System

A system with characteristics that comply with specified, publicly maintained, readily available standards, and that therefore can be connected to other systems that comply with these same standards. [ATIS]

2.2.140 Open Systems Architecture

1. The layered hierarchical structure, configuration, or model of a communications or distributed data processing system that

   a) enables system description, design, development, installation, operation, improvement, and maintenance to be performed at a given layer or layers in the hierarchical structure,

   b) allows each layer to provide a set of accessible functions that can be controlled and used by the functions in the layer above it,

   c) enables each layer to be implemented without affecting the implementation of other layers, and

   d) allows the alteration of system performance by the modification of one or more layers without altering the existing equipment, procedures, and protocols at the remaining layers.

NOTE 1 Examples of independent alterations include
a) converting from wire to optical fibres at a physical layer without affecting the data-link layer or the network layer except to provide more traffic capacity, and
b) altering the operational protocols at the network level without altering the physical layer.

NOTE 2 Open systems architecture may be implemented using the Open Systems Interconnection-Reference Model (OSI-RM) as a guide while designing the system to meet performance requirements.

2. Non-proprietary systems architecture. [ATIS]

2.2.141 Open Systems Interconnection – Reference Model (OSI-RM)

Information technology - Open Systems Interconnection - Basic Reference Model - Conventions for the definition of OSI services, layers 1-7 [ISO/IEC 10731:1994]

2.2.142 Password

1. A secret data value, usually a character string that is used as authentication information. [RFC 2828]
2. Secret word, phrase, number or character sequence used for entity authentication, which is a memorized weak secret. [ISO/IEC 11770-4:2006]
3. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS 140-2]

2.2.143 Personal Identification Number (PIN)

An alphanumeric code or password used to authenticate an identity. [FIPS 140-2]

2.2.144 Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means (e.g., internet web sites). [NIST SP 800-82]

2.2.145 Physical Layer Protocol

Protocols for transmitting raw electrical signals over the communications channel. Deals with transmission physics such as cabling, modulation, and transmission rates. Layer 1 of the OSI reference model. [ATIS]

2.2.146 Plaintext

Unencrypted information. [ISO/IEC 10116:2006]

2.2.147 Point-to-Point Protocol (PPP)

The Internet standard protocol for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links. [RFC 1661]

2.2.148 Port Scanning

Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). [NIST SP 800-61]

2.2.149 Pretty Good Privacy (PGP)

A publicly available encryption software program based on public key cryptography. The message formats are specified in RFC 1991 and RFC 2440. [ISO/IEC 18028-4:2005]

2.2.150 Private Key

1. The secret component of a pair of cryptographic keys used for asymmetric cryptography. [RFC 2828].
2. That key of an entity's asymmetric key pair which should only be used by that entity. [ISO/IEC 11770-1:1996]
3. The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. [NIST SP 800-63]
4. A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used to:
   1) compute the corresponding public key,
   2) compute a digital signature that may be verified by the corresponding public key,
   3) decrypt data that was encrypted by the corresponding public key, or
   4) compute a piece of common shared data, together with other information. [NIST SP 800-57]

2.2.151 Protection Profile

An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. [ISO/IEC 15408 Common Criteria]

2.2.152 Proxy, Proxy Server

1. A proxy is an application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. [NIST SP 800-44]
2. A computer process - often used as, or as part of, a firewall - that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. [RFC 2828]

2.2.153 Pseudorandom Number Generator (PRNG)

An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG “appears” to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [RFC 2828]

2.2.154 Public Key

1. The publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography. [RFC 2828]
2. That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1:1997]
3. The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. [NIST SP 800-63]
4. A cryptographic key that is used with a public key cryptographic algorithm. The public key is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to:
   1) Verify a digital signature that is signed by the corresponding private key,
   2) Encrypt data that can be decrypted by the corresponding private key, or
   3) Compute a piece of shared data. [NIST SP 800-57]

2.2.155 Public Key Asymmetric Cryptographic Algorithm

A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [FIPS 140-2]

2.2.156 Public Key Certificate

A set of data that uniquely identifies an entity, contains the entity’s public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [FIPS 140-2]

2.2.157 Public Key Cryptography

1. The type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. Note: Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography. [ATIS]
2. [An] Encryption system using a linked pair of keys. What one pair of keys encrypts, the other pair decrypts. [ATIS]

2.2.158 Public Key Infrastructure (PKI)

A system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography. [RFC 2828]

NOTE Certificates may also be managed by other trusted groups such as the PGP web of trust.

2.2.159 Replay Attack

1. A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1:1997]

2.2.160 Repudiation

Denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship. [RFC 2828]

2.2.161 Risk

1. The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence. [ISO/IEC 13335-1:2004]
2. An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [RFC 2828]
3. The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [NIST SP 800-30]

2.2.162 Risk Assessment

1. A risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The target of the risk assessment process is the identification and evaluation of risks, which have negative impacts to identified assets and the definition of appropriate safeguards and actions, which minimize the effects of the identified risks. [ISO/IEC 15443-3:2007]
2. The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses. [NIST SP 800-53]

2.2.163 Risk Management

The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. [NIST SP 800-30]

2.2.164 Rivest, Shamir and Adleman (RSA)

A public-key cryptosystem based on the factoring problem. RSA stands for Rivest, Shamir and Adleman, the developers of the RSA public-key cryptosystem. [defined in work by Rivest, Shamir, and Adleman]

2.2.165 Role Based Access Control (RBAC)

A form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process. [RFC 2828]

2.2.166 Secret Key

1. A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO/IEC 13888-1:2004]
2. A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. [FIPS 140-2]

2.2.167 Secret Key Encryption

A synonym for "symmetric cryptography". [RFC 2828]

2.2.168 Secret Key Symmetric Cryptographic Algorithm

A cryptographic algorithm that uses a single secret key for both encryption and decryption. [FIPS 140-2]

2.2.169 Secure Hash Algorithm (SHA)

The Secure Hash Algorithm is defined in Federal Information Processing Standard FIPS 180-1. [NIST SP 800-22]

2.2.170 Secure Shell (SSH)

A protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security. [ISO/IEC 18028-4:2005]

2.2.171 Secure Sockets Layer (SSL)

1. An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (often a web browser) and a server, and that can optionally provide peer entity authentication between the client and the server. [RFC 2828]
2. Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:”. TLS is an Internet standard based on SSL version 3.0. There are only very minor differences between SSL and TLS. [NIST SP 800-46]

2.2.172 Secure/ Multipurpose Internet Mail Extensions (S/MIME)

Method to provide a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). [RFC 2633]

2.2.173 Security

1. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. [ATIS]
2. All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. [ISO/IEC 13335-1]

2.2.174 Security Domain

1. An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources. [RFC 2828]
2. A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (e.g., hierarchically) to form larger domains. [RFC 2828]

2.2.175 Security Guidelines

Security guidelines define the objectives and constraints for the security program. Guidelines are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, guidelines provide answers to the questions “what” and “why” without dealing with “how.” Guidelines are normally stated in terms that are technology-independent. [ISA99]

2.2.176 Security Management

In network management, the set of functions (a) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and (b) that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges. [ATIS]

2.2.177 Security Performance

Performance evaluated in terms of a program’s compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance. [ISA99]

2.2.178 Security Perimeter

The boundary of the domain in which a security policy or security architecture applies; i.e., the boundary of the space in which security services protect system resources. [RFC 2828]

2.2.179 Security Policy

1. A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources. [RFC 2828]
2. Set rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context. [ISO/IEC 15408]
3. The objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent. [ISA99]

2.2.180 Security Risk Assessment

The process of analyzing threats to and vulnerabilities of an information system (IS) and the potential impact the loss of information or capabilities of a system would have on national [or any system] security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. [ATIS]

2.2.181 Security Services

Mechanisms used to provide confidentiality, data integrity, authentication or non-repudiation of information. [RFC 2828]

2.2.182 Server

A device or application that provides information or services to client applications and devices. [ATIS]

2.2.183 Session Key

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. [RFC 2828]

2.2.184 Shoulder Surfing

Looking over someone's shoulder as they enter their password. [ISO/IEC 27002:2005]

2.2.185 Signature Certificate

A public-key certificate that contains a public key that is intended to be used for verifying digital signatures, rather than for encrypting data or performing other cryptographic functions. [RFC 2828]

2.2.186 Simple Network Management Protocol (SNMP)

1. A UDP-based, application-layer, Internet Standard protocol [RFC 2570, RFC 2574] for conveying management information between managers and agents. [RFC 2828]
2. A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or "hard-coded" in the MIB, while others are dynamic values calculated by agent software running on the device. [API 1164]

2.2.187 Smart Card

A credit-card sized device containing one or more integrated circuit chips, which perform the functions of a computer's central processor, memory, and input/output interface. [RFC 2828]

2.2.188 Smurf

1. Software that mounts a denial-of-service attack ("smurfing") by exploiting IP broadcast addressing and ICMP ping packets to cause flooding. [RFC 2828]
2. An attack that exploits features of the IP protocol within the TCP/IP protocol. [ISO/IEC 27002:2005]

2.2.189 Sniffing

A synonym for "passive wiretapping". [RFC 2828]

2.2.190 Social Engineering

1. A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems. [RFC 2828]
2. Extraction of information, usually verbally, by impersonating a legitimate third party or by using other social interactions. [ISO/IEC 27002:2005]

2.2.191 Spoof

Pretending to be an authorized user and performing an unauthorized action. [RFC 2828]

2.2.192 Spyware

Software that is secretly or surreptitiously installed onto an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [NIST SP 800-53]

2.2.193 Strong Authentication

1. Authentication by means of cryptographically-derived credentials. [ATIS]
2. An authentication process that uses cryptography - particularly public-key certificates - to verify the identity claimed for an entity. [RFC 2828]

NOTE Multi-factor authentication may be stronger than any single authentication method.

2.2.194 Strong Secret

Secret with a sufficient degree of entropy that conducting an exhaustive search for the secret is infeasible, even given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess.

NOTE This might, for example, be achieved by randomly choosing the secret from a sufficiently large set of possible values with an even probability distribution. [ISO/IEC 11770-4:2006]

2.2.195 Supervisory Control and Data Acquisition (SCADA)

1. SCADA (Supervisory Control and Data Acquisition): System that supervises and controls a geographically distributed process [IEC/TR 60870-1-3:1997]
2. The SCADA system is known also as “Telecontrol System”: System serving for monitoring and control of processes which are geographically widespread. This includes all equipment and functions for acquisition, processing, transmission, and display of the necessary process information [IEC/TR 60870-1-3:1997]

2.2.196 Symmetric Cryptography

1. A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). [RFC 2828]
2. Cryptographic technique that uses the same secret key for both the encryption and the decryption transformations. [ISO/IEC 19790:2006]

2.2.197 Symmetric Key

A cryptographic key that is used in a symmetric cryptographic algorithm. [RFC 2828]

2.2.198 Symmetric Key Algorithm

See Secret Key Cryptographic Algorithm. [RFC 2828]

2.2.199 SYN Flood

A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle. [RFC 2828]

2.2.200 Tamper Detection

Automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module. [ISO/IEC 19790:2006]

2.2.201 Tampering

1. Penetration or modification of internal operations, or the insertion of active or passive tapping mechanisms, to determine the nature of, or monitor or record, e.g., secret data. [ATIS]
2. Unauthorized modification of sensitive systems or sensitive information. [ATIS]

2.2.202 TASE.2

Telecontrol Application Service Element, number 2, formally IEC 60870-6 and informally ICCP. [IEC 60870-6]

2.2.203 Threat

1. A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. [RFC 2828]
2. Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others. [ISO/IEC 21827:2002]
3. Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST SP 800-53]

2.2.204 Throughput

The maximum continuous traffic rate that a device can handle without dropping a single packet. [ATIS]

2.2.205 Traffic Analysis

1. Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence. [RFC 2828]
2. In a communications system, the analysis of traffic rates, volumes, densities, capacities, and patterns specifically for system performance improvement. [ATIS]

2.2.206 Transport Level Security (TLS)

An Internet protocol [RFC 2246] based on and very similar to SSL Version 3.0. [RFC 2828]

2.2.207 Trap Door

1. A hidden computer flaw known to an intruder, or a hidden computer mechanism (usually software) installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms. [RFC 2828]

NOTE Similar to Back Door, but may have been implemented for malicious reasons.

2. A hidden software or hardware mechanism, usually created for testing and troubleshooting, that may be used to circumvent computer security. Synonym for Back Door. [ATIS]

2.2.208 Triple DES

A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits. [RFC 2828]

2.2.209 Trojan Horse

1. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. [RFC 2828]
2. [A] program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. [ATIS]

2.2.210 Trust

1. Information system usage: The extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions. [RFC 2828]
2. In cryptology and cryptosystems: That characteristic allowing one entity to assume that a second entity will behave exactly as the first entity expects.

NOTE Trust may apply only for some specific function. The critical role of trust in the authentication framework is to describe the relationship between an authenticating entity and a certification authority; an authenticating entity must be certain that it can trust the certification authority to create only valid and reliable certificates. [ATIS].

2.2.211 Tunnel

A communication channel created in a computer network by encapsulating (carrying, layering) a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. [RFC 2828]

NOTE VPN is an example of a tunnelling protocol

2.2.212 Unforgeable

The property of a cryptographic data structure (i.e., a data structure that is defined using one or more cryptographic functions) that makes it computationally infeasible to construct (i.e., compute) an unauthorized but correct value of the structure without having knowledge of one of more keys. [RFC 2828]

2.2.213 Update Key

Every key pair needs to be updated regularly (i.e., replaced with a new key pair), and a new certificate needs to be issued. [...] When a key pair is due to expire the relevant end entity MAY request a key update - that is, it MAY request that the CA issue a new certificate for a new key pair. The request is made using a key update request (kur) message. [RFC 2510]

NOTE Symmetric update keys may not involve a new certificate, but simply a new key.

2.2.214 Virtual Private Network (VPN)

1. A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network. [RFC 2828]
2. Restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunnelling links of the virtual network across the real network. [ISO/IEC 18028-1:2006]
3. A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network. [NIST SP 800-46]