Dictionary of the Computer Security and Incident Response terms

Толковый словарь терминов по компьютерной безопасности и реагированию на компьютерные инциденты безопасности

Compiled by Yuri Demchenko <demch@science.uva.nl>
AIRG, University of Amsterdam

$ access control – контроль доступа

Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.

$ access control list (ACL) – список контроля доступа

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

$ advisory (see security advisory) – рекомендации (рекомендации по безопасности)

Security advisories provide timely information about current security issues, vulnerabilities, and exploits. The term is branded from CERT/CC advisory service.

$ alert – тревога, оповещение

A message from an analyzer to a network (security) manager that an event of interest has been detected. An alert typically contains information about the unusual activity that was detected, as well as the specifics of the occurrence.

Alert can also be used as a synonym to the security advisory as a document providing timely information about current security issues, vulnerabilities, and exploits.

$ analyzer - анализатор

The Intrusion Detection System (IDS) component or process that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. In many existing IDS's, the sensor and the analyzer are parts of the same component.

$ attack - атака

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. Attack may consist of one or more steps taken by attacker to

achieve an unauthorised result. Successful attack may lead to intrusion and further escalated as an incident.

Active vs. passive: An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)

Insider vs. outsider: An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

$ attacker - атакующий

An attacker may be an insider, an outsider, or an entity acting via an attack mediator. For the purpose of Incident response/handling, an attacker is described by the computer/network ID, from which the attack was launched. The organization name and/or physical location of the computer/network may be used as additional information.

$ authority – центр, удостоверяющий центр

An entity, responsible for the issuance/provision of authoritative information in respect to Incident or other entity (e.g., organisation, personal, system).

Note. In PKI, a term “authority” for defining an entity responsible for the issuance of certificates.

$ availability - доступность

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.

$ back door – «черный ход»

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. (See: trap door.)

Note. For example, a way to access a computer other than through a normal login. Such access paths do not necessarily have malicious intent; e.g., operating systems sometimes are shipped by the manufacturer with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

$ brute force – грубая сила

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Note. For example, for ciphertext where the analyst already knows the decryption algorithm, a brute force technique to finding the original plaintext is to decrypt the message with every possible key.

$ Common Criteria – Общие критерии

"The Common Criteria" is a standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures. [CCIB]

Note. The standard addresses data confidentiality, data integrity, and availability and may apply to other aspects of security. It focuses on threats to information arising from human activities, malicious or otherwise, but may apply to non-human threats. It applies to security measures implemented in hardware, firmware, or software. It does not apply to (a) administrative security not related directly to technical security, (b) technical physical aspects of security such as electromagnetic emanation control, (c) evaluation methodology or administrative and legal framework under which the criteria may be applied, (d) procedures for use of evaluation results, or (e) assessment of inherent qualities of cryptographic algorithms.

$ Computer Emergency Response Team (CERT) – Центр реагирования на чрезвычайные ситуации в компьютерной безопасности

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks,
publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.
(See: CSIRT, security incident.)

Note. Currently, term “CERT” is registered as a trademark in US for the CERT Coordination Center at Carnegie-Mellon University (CERT/CC). Term CSIRT is encouraged to use worldwide for defining Computer Security Response Teams.

$ credential(s) – удостоверение, мандат

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

$ CSIRT (Computer Security Response Teams) – Центр Реагирования на Компьютерные Инциденты безопасности (ЦРКИБ)

CSIRT (Computer Security Incident Response Team) is a team that coordinates and supports the response to security incidents that involve sites within a defined constituency. The CSIRT generates, processes and maintains incident reports.

$ CVE (Common Vulnerability and Exposure) – общие уязвимости и слабости (аббревиатура для одноименной директории)

CVE list is a list of standardised names for Vulnerabilities and other Information Security Exposures aimed to easy sharing data across separate vulnerability databases and security tools. The content of CVE is a result of a collaborative effort of the CVE Editorial Board of many security-related organizations such as security tool vendors, academic institutions, and government as well as other security experts.

$ damage – повреждение, потери

An intended or unintended consequence of an attack which affects the normal operation of the targeted system or service. Description of damage may include free text description of actual result of attack, and, where possible, structured information about the particular damaged system, subsystem or service.

$ data compromise – раскрытие данных, несанкционированное раскрытие данных

A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information may have occurred.

$ data confidentiality – защита данных, конфиденциальность данных

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].

Note. The term SHOULD NOT be used as a synonym for "privacy", which is a different concept.

$ data integrity – целостность данных

The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Note. Deals with constancy of and confidence in data values, not
with the information that the values represent or the trustworthiness of the source of the values.

$ denial of service (DoS) – отказ в обслуживании

The prevention of authorized access to a system resource or the delaying of system operations and functions. DoS affects such security service as availability, and conducted via flooding, etc..

$ distributed denial of service (DDoS) – распределенный отказ в обслуживании

Denial of Service attack organised by flooding target system from multiple distributed sources.

$ dictionary attack – словарная атака

An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

For example, an attack on an authentication service by trying all possible passwords; or an attack on encryption by encrypting some known plaintext phrase with all possible keys so that the key for any given encrypted message containing that phrase may be obtained by lookup.

$ eavesdropping – секретное «подслушивание»

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

$ eCSIRT (The European CSIRT Network) – Европейская сеть CSIRT

The European CSIRT Network (http://www.ecsirt.net/) is originated from the European project resulted in the deployment of new techniques and practices of cooperation between incident response teams (CERTs or CSIRTs) in the exchange of incident related data and collection of shared data for statistical and knowledge-base purposes. Part of the project was devoted to set up a network of IDS sensors across Europe and collect the data about attacks for further analysis.

The co-operation of the volunteering teams providing the infrastructure support as well as the teams supporting the network by running IDS sensors in their area of interest is still based on the same policy and procedural framework, protecting the interest of all participating teams.

$ event (security event) – событие (событие безопасности)

An occurrence in a system or network, which maybe of interest and/or warrants attention. An event may indicate an attack. An event may also indicate an error or a fault or the result of a deliberate act that is not an attack. For example, the occurrence of three failed logins in 10 seconds is an event. It might indicate a brute- force login attack. A program failure, network fault, system shutdown are other examples of event.

$ evidence - улика

Evidence is information relating to an event that proves or supports a conclusion about the event. With respect to security incidents (the events), it may include but is not limited to: data dump created by Intrusion Detection System (IDS), data from syslog file, kernel statistics, cache, memory, temporary file system, or other data that caused the alert or were collected after the incident happened.

Special rules and care must be taken when storing and archiving evidence, particularly to preserve its integrity. When necessary evidence should be stored encrypted. The chain of evidence custody needs to be clearly documented. It is essential that evidence should be collected, archived and preserved according to local legislation.

$ exploit – эксплоид, потенциальная уязвимость (при определенных условиях)

An exploit is a common term in the computer security . There are multiple variants of exploits, a common term is 'remote exploit', which refers to an exploit that can take advantage of a security vulnerability remotely, over a network. A “local exploit” on the other hand can only increase privileges on a system where some kind of local access is already permitted.

Normally a single exploit can only take advantage of a specific software vulnerability. Often, as such an exploit is published, the vulnerability is fixed and the exploit becomes obsolete for newer versions of the software.

$ Federal Information Processing Standards (FIPS) – стандарты Национального Бюро стандартов США

The Federal Information Processing Standards Publication (FIPS PUB) series issued by the U.S. National Institute of Standards and Technology as technical guidelines for U.S. Government procurements of information processing system equipment and services.

$ firewall – сетевой экран, брандмауэр

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). gateway.)

Note. A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies security policy rules to control traffic that flows in and out of the protected network.

Note. A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep intruders out, but usually also needs to let authorized users in and out.

$ firmware – базовое программное обеспечение, поставляемое вместе с апаратным обеспечением

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

$ flooding – атака, направленная на создание потока запросов, превышающего проихводительность целевой системы, «забивание» системы

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.

$ Forum of Incident Response and Security Teams (FIRST) – Форум CSIRT

An international consortium of CSIRTs that work together to handle computer security incidents and promote preventive activities. (See: CSIRT, security incident.)

Note. FIRST was founded in 1990 and, as of June 2004, had nearly 200 members spanning the globe. Its mission includes:

- Provide members with technical information, tools, methods, assistance, and guidance.
- Coordinate proactive liaison activities and analytical support.
- Encourage development of quality products and services.
- Improve national and international information security for government, private industry, academia, and the individual.
- Enhance the image and status of the CSIRT community.

$ gateway - шлюз

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.

(C) In theory, gateways are conceivable at any OSI layer. In practice, they operate at OSI layer 3 (e.g., bridge, router) or layer 7 (e.g., proxy server). When the two networks differ in the protocol by which they offer service to hosts, the gateway may translate one protocol into another or otherwise facilitate interoperation of hosts (see: Internet Protocol).

$ honey pot – «сладкая» приманка, «липучка»

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. (Honey pot can be used as a synonym to “entrapment”.)

$ host - хост

General computer network usage: A computer that is attached to a communication subnetwork or internetwork and can use services provided by the network to exchange data with other attached systems.

Specific Internet Protocol Suite usage: A networked computer that does not forward Internet Protocol packets that are not addressed to the computer itself.

$ https (S-HTTP)

When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL. (see S-HTTP)

$ ICMP flood – атака, связанная с «забиванием» потоком управляющих сигналов ICMP

A denial of service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle.

$ IDMEF (Intrusion Description and Message Format) – формат для описания вторжений и сообщений о вторжениях

Intrusion Description and Message Format (IDMEF) is a format for information exchange between IDS and Network operation Center or CSIRT. IDMEF is a product of IETF ID WG. Currently IDMEF is widely used for integration of IDS and available as a plugin to popular IDS Snort.

$ impact – влияние, последствия

Impact describes result of attack expressed in terms of user community, for example the cost in terms of financial or other disruption

$ incident (see security incident) – инцидент, инцидент безопасности

An Incident is a security event that involves a security violation. An incident can be defined as a single attack or a group of attacks that can be distinguished from other attacks by the method of attack, identity of attackers, victims, sites, objectives or timing, etc.

$ incident coordination – координация инцидентов

Incident Coordination normally includes:

- Information categorization - Categorization of the incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- Coordination - Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

$ incident report – описание инцидента, отчет об инциденте

In CSIRT practice, an Incident Report refers to the information pertaining to an incident. An Incident Report may have some internal proprietary format that is adapted to the local Incident Handling System (IHS) and Incident handling procedures. Incident information exchange may use some proprietary format or developed by IETF Incident Object Description and Exchange Format (IODEF).

$ incident response – реагирование на инцидент безопасности

Incident response usually includes assessing incoming reports about incidents ("Incident Triage") and following up on these with other CSIRTs, ISPs and sites ("Incident Coordination"). A third range of services, helping a local site to recover from an incident ("Incident Resolution"), is comprised of typically optional services, which not all CSIRTs will offer.

$ incident resolution – разрешение/расследование инцидента

Usually additional or optional, incident resolution service include:

- Technical Assistance - This may include analysis of compromised systems.
- Eradication - Elimination of the cause of a security incident (the vulnerability exploited), and its effects (for example, continuing access to the system by an intruder).
- Recovery - Aid in restoring affected systems and services to their status before the security incident.

$ incident triage – (первичная) сортировка инцидентов

Building off of the information available and the assessments in the prior steps, identify and evaluate options to meet the established goals, define priority steps. This function is often performed by CSIRT member on duty, or defined by another collective procedure to assess Incident at the initial stage.

Incident triage usually includes:

- Report assessment - Interpretation of incoming incident reports, prioritizing them, and relating them to ongoing incidents and trends.
- Verification - Help in determining whether an incident has really occurred, and its scope.

$ Internet Control Message Protocol (ICMP) – протокол обмена управляющими сообщениями в Интернет

An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

$ Internet Draft – название начальной версии (наброски) документа, предлагаемого как RFC

A working document of the IETF, its areas, and its working groups. (Other groups may also distribute working documents as Internet Drafts.) An Internet Draft is not an archival document like an RFC is. Instead, an Internet Draft is a preliminary or working document that is valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. It is inappropriate to use an Internet Draft as reference material or to cite it other than as "work in progress."

$ Internet Engineering Task Force (IETF) – название форума (инженерной группа), занимающейся разработкой стандартов Интернет

A self-organized group of people who make contributions to the development of Internet technology. The principal body engaged in developing Internet Standards, although not itself a part of the ISOC. Composed of Working Groups, which are arranged into Areas (such as the Security Area), each coordinated by one or more Area Directors. Nominations to the IAB and the IESG are made by a committee selected at random from regular IETF meeting attendees who have volunteered.

$ Internet Protocol security (IPsec) – название группы технологий обеспечивающих безпасность передачи информации на сетевом/Интернет уровне

A name for the security architecture and protocols to provide security services for Internet Protocol traffic defined by a group of Internet standards and RFC.

The IPsec architecture specifies (a) security protocols (AH and ESP), (b) security associations (what they are, how they work, how they are managed, and associated processing), (c) key management (IKE), and (d) algorithms for authentication and encryption. The set of security services include access control service, connectionless data integrity service, data origin authentication service, protection against replays (detection of the arrival of duplicate datagrams, within a constrained window), data confidentiality service, and limited traffic flow confidentiality.

$ intruder -

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

$ intrusion detection – обнаружение вторжений

A security service that monitors and analyzes 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. Practically, intrusion detection infrastructure consists of IDS and sensors that guard virtually security perimeter of an organisation.

$ intrusion detection system – система, предназначенная для обнаружения вторжений

An "Intrusion Detection System (IDS)" is a system for detecting intrusions into computer system or controlled security perimeter. Network intrusion detection systems (NIDS) monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack). A typical example is a system that watches for large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. A NIDS may run either on the target machine who watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine promiscuously watching all network traffic (hub, router, probe).

$ IODEF (Incident Object Description and Exchange Format) – название формата для описания инцидентов

IODEF (Incident Object Description and Exchange Format) is a format developed by IETF INCH-WG for Incident information exchange between cooperating CSIRT's. IODEF currently is adopted by many CSIRT and association including CERT/CC.

$ IRT Object (RIPE NCC Database) – обьект в базе данных RIPE NCC, содержащий информацию о контакте безопасности для определенной группы IP-адресов

The **irt** object in RIPE NCC Database is used to provide information about a Computer Security Incident Response Team (CSIRT).

When a computer/network security incident happens, such as DOS (Denial of Service) or spam attack, or other abuse of services, it is important to know whom to contact. The RIPE Database provides the facility to get administrative and technical contacts for a network where the attack came from by a simple IP lookup. In many cases such incidents are handled by CSIRTs whose contacts are different from those listed in "admin-c:" and "tech-c:" attributes. Unfortunately there is no easy way to identify which CSIRT is serving any given IP address. Additional information, such as public certificates of a CSIRT, and query functionality that allows to search for the responsible team would facilitate prompt incident handling.

$ ISO17799 ISO/IEC 17799:2000 Information technology - Code of practice for information security management – стандарт, описывающие рекомендации по управлению безпасностью в организациях и системах

ISO/IEC 17799:2000 gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

Information security is characterized here as the preservation of:
a) confidentiality: ensuring that information is accessible only to those authorized to have access;
b) integrity: safeguarding the accuracy and completeness of information and processing methods;
c) availability: ensuring that authorized users have access to information and associated assets when required.

ISO17799 security standard is a detailed security standard. It is organised into ten major sections, each covering a different topic or area:
1. Business Continuity Planning
2. System Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organisation
8. Computer & Operations Management

9. Asset Classification and Control
10. Security Policy

$ ITU-T – сектор стандартизации в области телекомуникаций при ITU

International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations". (See: X.400, X.500.)

$ malware – злонамеренное программное обеспечение

A contraction of "malicious software".

$ man-in-the-middle – «человек-посредине» - тип атаки, связанный с возможным перехватом конфиденциальной информации, используемой потом для развития атаки или в преступных целях

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. (may originate hijack attack, piggyback attack.)

For example, suppose Alice and Bob try to establish a session key by using the Diffie-Hellman algorithm without data origin authentication service. A "man in the middle" could (a) block direct communication between Alice and Bob and then (b) masquerade as Alice sending data to Bob, (c) masquerade as Bob sending data to Alice, (d) establish separate session keys with each of them, and (e) function as a clandestine proxy server between them in order to capture or modify sensitive information that Alice and Bob think they are sending only to each other.

$ National Institute of Standards and Technology (NIST) – название национального института стандартизации США

A U.S. Department of Commerce agency that promotes U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. Has primary Government responsibility for INFOSEC standards for unclassified but sensitive information.

$ non-repudiation service – «неотпирательство», услуга, предотвращающая возможность отказа в совершенных действиях

A security service that provide protection against false denial of involvement in a communication.

Non-repudiation service does not and cannot prevent an entity from repudiating a communication. Instead, the service provides evidence that can be stored and later presented to a third party to resolve disputes that arise if and when a communication is repudiated by one of the entities involved. There are two basic kinds of non-repudiation service:

- "Non-repudiation with proof of origin" provides the recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny sending the data. This service can be viewed as a stronger version of an data origin authentication service, in that it proves authenticity to a third party.
- "Non-repudiation with proof of receipt" provides the originator of data with evidence that proves the data was received as addressed, and thus protects the originator against an attempt by the recipient to falsely deny receiving the data.

$ notarisation – нотаризация, нотариальная услуга

Registration of data under the authority or in the care of a trusted third party, thus making it possible to provide subsequent assurance of the accuracy of characteristics claimed for the data, such as content, origin, time, and delivery.

$ Open Systems Interconnection (OSI) Reference Model (OSIRM) – базовая модель взаимодействия открытых систем (ВОС)

A joint ISO/ITU-T standard [I7498 Part 1] for a seven-layer, architectural communication framework for interconnection of computers in networks.

The OSIRM layers, from highest to lowest, are (7) Application, (6) Presentation, (5) Session, (4) Transport, (3) Network, (2) Data Link, and (1) Physical. OSIRM provides a good methodological basis for analysing and designing network services and architectures but are not compatible with TCP/IP model used in the Internet. In contrary OSI Security Architecture is adopted by Internet community, in particular in PKI (Public Key Infrastructure).

$ OSI Security Architecture – архитектура безопасности на основе модели ВОС

$ password - пароль

A secret data value, usually a character string, that is used as authentication information.

A password is usually matched with a user identifier that is explicitly presented in the authentication process, but in some cases the identity may be implicit.

Using a password as authentication information assumes that the password is known only by the system entity whose identity is being authenticated. Therefore, in a network environment where wiretapping is possible, simple authentication that relies on transmission of static (i.e., repetitively used) passwords as clear text is inadequate. (See: one-time password, strong authentication.)

$ penetration test – тест на проникновение

A system test, often part of system certification, in which evaluators attempt to circumvent the security features of the system.

Penetration testing may be performed under various constraints and conditions. However, for a TCSEC evaluation, testers are assumed to have all system design and implementation documentation, including source code, manuals, and circuit diagrams, and to work under no greater constraints than those applied to ordinary users.

$ piggyback attack – атака «между строк»

A form of active wiretapping in which the attacker gains access to a system via intervals of inactivity in another user's legitimate communication connection. Sometimes called a "between-the-lines" attack. (See: hijack attack, man-in-the-middle attack.)

$ ping of death – пинг «смерти», тип атаки, использующий очень большой эхо-запрос с целью перегрузить целевую систему

An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

$ ping sweep – тип атаки, использующий сканирование группы IP-адресов с целью найти уязвимый хост

An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

$ port scan – тип атаки, использующий сканирование портов с целью найти активный порт и использовать известную уязвимость

An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

$ privacy - приватность

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.

Note. Term privacy should not be used as a synonym for "data confidentiality" or "data confidentiality service", which are different concepts. Privacy is a reason for security rather than a kind of security. For example, a system that stores personal data needs to protect the data to prevent harm, embarrassment, inconvenience, or unfairness to any person about whom data is maintained, and to protect the person's privacy. For that reason, the system may need to provide data confidentiality service.

$ proxy server – прокси-сервер, используемый как часть сетевого экрана и выступающий как промежуточный в коммуникациях между внутренней и внешней сетями

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.

In a firewall, a proxy server usually runs on a bastion host, which may support proxies for several protocols (e.g., FTP, HTTP, and TELNET). Instead of a client in the protected enclave connecting directly to an external server, the internal client connects to the proxy server which in turn connects to the external server. The proxy server waits for a request from inside the firewall, forwards the request to the remote server outside the firewall, gets the response, then sends the response back to the client. The proxy may be transparent to the clients, or they may need to connect first to the proxy server, and then use that association to also initiate a connection to the real server.

A proxy can provide security service beyond that which is normally part of the relayed protocol, such as access control based on peer entity authentication of clients, or peer entity authentication of servers when clients do not have that capability. A proxy at OSI layer 7 can also provide finer-grained security service than can a filtering router at OSI layer 3.

$ Rainbow Series – название группы стандартов безопасности, выпущенных NCSC

A set of more than 30 technical and policy documents with colored covers, issued by the NCSC, that discuss in detail the TCSEC and provide guidance for meeting and applying the criteria.

$ replay attack – тип атаки, использующий повтор предварительно записанной правильной последовательности сообщений с целью получить несанкционированный или неучтенный доступ к системе

An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack.

$ Request for Comment (RFC) – название стандартов Интернет, разрабатываемых IETF

One of the documents in the archival series that is the official channel for ISDs and other publications of the Internet Engineering Steering Group, the Internet Architecture Board, and the Internet community in general.

$ risk analysis – анализ риска

A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

$ Secure Sockets Layer (SSL) – название протокола безопасности транспортного уровня

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.

SSL is layered below HTTP and above a reliable transport protocol (TCP). SSL is independent of the application it encapsulates, and any higher level protocol can layer on top of SSL transparently. However, many Internet applications might be better served by IPsec.

SSL has two layers: (a) SSL's lower layer, the SSL Record Protocol, is layered on top of the transport protocol and encapsulates higher level protocols. One such encapsulated protocol is SSL Handshake Protocol. (b) SSL's upper layer provides asymmetric cryptography for server authentication (verifying the server's identity to the client) and optional client authentication (verifying the client's identity to the server), and also enables them to negotiate a symmetric encryption algorithm and secret session key (to use for data confidentiality) before the application protocol transmits or receives data. A keyed hash provides data integrity service for encapsulated data.

$ security (computer security) – безопасность, компьютерная безопасность

Computer security refers to efforts to create a secure computing platform, designed so that agents (users or programs) should not be able to perform actions that they are not allowed to perform, but can perform the actions that they are allowed to. This involves specifying and implementing a security policy. The actions in question can be reduced to operations of access, modification and deletion. Different aspects of security include:

(1.) Measures taken to protect a system. (2.) The condition of a system that results from the establishment and maintenance of measures to protect the system. (3.) The condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

$ security architecture – архитектура безопасности

A plan and set of principles that describe (a) the security services that a system is required to provide to meet the needs of its users, (b) the system elements required to implement the services, and (c) the performance levels required in the elements to deal with the threat environment.

A security architecture is the result of applying the system engineering process. A complete system security architecture includes administrative security, communication security, computer security, emanations security, personnel security, and physical security. A complete security architecture needs to deal with both intentional, intelligent threats and accidental kinds of threats.

$ security audit – аудит безопасности

An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises.

$ security compromise – нарушение безопасности

A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access.

$ security event – событие безопасности

A occurrence in a system that is relevant to the security of the system. (See: security incident.)

The term includes both events that are security incidents and those that are not. In a CA workstation, for example, a list of security events might include the following:

- Performing a cryptographic operation, e.g., signing a digital certificate or CRL.
- Performing a cryptographic card operation: creation, insertion, removal, or backup.
- Performing a digital certificate lifecycle operation: rekey, renewal, revocation, or update.
- Posting information to an X.500 Directory.
- Receiving a key compromise notification.
- Receiving an improper certification request.
- Detecting an alarm condition reported by a cryptographic module.
- Logging the operator in or out.
- Failing a built-in hardware self-test or a software system integrity check.

$ security incident – инцидент безопасности

An Incident is a security event that involves a security violation. An incident can be defined as a single attack or a group of attacks that can be distinguished from other attacks by the method of attack, identity of attackers, victims, sites, objectives or timing, etc.

However we should distinguish between the generic definition of 'Incident' which is an event that might lead to damage or damage which is not too serious, and 'Security Incident' and 'IT Security Incident' which are defined below:

a) Security incident is an event that involves a security violation. This may be an event that violates a security policy, UAP, laws and jurisdictions, etc. A security incident may also be an incident that has been escalated to a security incident. A security incident is worse than an incident as it affects the security of or in the organisation. A security incident may be logical, physical or organisational, for example a computer intrusion, loss of secrecy, information theft, fire or an alarm that doesn't

work properly. A security incident may be caused on purpose or by accident. The latter may be if somebody forgets to lock a door or forgets to activate an access list in a router.

b) An IT security incident is defined according to [9] as any real or suspected adverse event in relation to the security of a computer or computer network. Typical security incidents within the IT area are: a computer intrusion, a denial-of-service attack, information theft or data manipulation, etc.

$ security intrusion – вторжение, связанное с нарушением безопасности

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

$ security mechanism – механизмы безопасности

A process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system.

Some examples of security mechanisms are authentication exchange, checksum, digital signature, encryption, and traffic padding.

$ security policy – политика безопасности

The predefined, formally documented statement which defines what activities are allowed to take place on an organization's network or on particular hosts to support the organization's requirements. This includes, but is not limited to, which hosts are to be denied external network access.

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. Security policy can be treated as one of layers of the security engineering process

$ security service – услуга безопасности

A processing or communication service that is provided by a system to give a specific kind of protection to system resources. For example, according to OSI Security model, security services include: access control service, audit service, availability service, data confidentiality service, data integrity service, data origin authentication service, non-repudiation service, peer entity authentication service, system integrity service. Security services implement security policies, and are implemented by security mechanisms.

$ S-HTTP (Secure-HTTP, Secure Hypertext Transfer Protocol) – безопасная версия протокола HTTP, использующего механизмы безопасности транспортного уровня, название безопасного протокола доступа к веб-ресурсам

A Internet protocol for providing client-server security services for HTTP communications. S-HTTP supports choice of security policies, key management mechanisms, and cryptographic algorithms through option negotiation between parties for each transaction. S-HTTP supports both asymmetric and symmetric key operation modes. S-HTTP attempts to avoid presuming a particular trust model, but it attempts to facilitate multiply- rooted hierarchical trust and anticipates that principals may have many public key certificates.

$ Secure/MIME (S/MIME) – название механизма обеспечения безопасности обмена почтовыми сообщениями, позволяющего использовать шифрование и цифровую подпись сообщений с использованием сертификатов открытых ключей (СОК) по стандарту X.509

Secure/Multipurpose Internet Mail Extensions, an Internet protocol [R2633] to provide encryption and digital signatures for Internet mail messages.

$ sniffing – «вынюхивание», тип пассивной атаки, связанный с «подслушиванием» в сети

A synonym for "passive wiretapping".

$ Snort (tm) – название свободно распространяемой системы для обнаружения вторжений

The Open Source Network Intrusion Detection System (http://www.snort.org/)

$ source – источник, используется для определения источника атаки

The source of an attack. This can be a logical entity (e.g. a user account, a computer process or data, a logical network or internetwork) or a physical entity (e.g. a computer interface, a router etc.).

$ spam – спам, несанкционированная рассылка большого количества почтовых сообщений

(1.) Verb: To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. (2.) Noun: electronic "junk mail".

Note. In sufficient volume, spam can cause denial of service.

$ spoofing attack – тип атаки, использующий подмену IP-адресов

A synonym for "masquerade attack".

$ SYN flood – тип атаки, посылающий большое количество пакетов TCP SYN с целью перегрузить целевую систему

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.

$ target – цель, используется для обозначения цели атаки

A computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).

$ tamper – нарушать безопасность посредством несанкционированных изменений в системе

Make an unauthorized modification in a system that alters the system's functioning in a way that degrades the security services that the system was intended to provide.

$ TF-CSIRT (TERENA Task Force for CSIRT coordination for Europe) – специализированная рабочая группа при TERENA, служащая для координации активности CSIRT в Европе

$ threat - угроза

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an `earthquake, a fire, or a tornado).`

$ threat consequence – потенциальные последствия от угрозы

A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation.

The following subentries describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

1. "(Unauthorized) Disclosure" (a threat consequence): A circumstance or event whereby an entity gains access to data for which the entity is not authorized. (See: data confidentiality.) The following threat actions can cause unauthorized disclosure:

A. "Exposure": A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:

a. "Deliberate Exposure": Intentional release of sensitive data to an unauthorized entity.
b. "Scavenging": Searching through data residue in a system to gain unauthorized knowledge of sensitive data.
c* "Human error": Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data.
d* "Hardware/software error". System failure that results in an entity gaining unauthorized knowledge of sensitive data.

B. "Interception": A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations. This includes:

a. "Theft": Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
b. "Wiretapping (passive)": Monitoring and recording data that is flowing between two points in a communication system.
c. "Emanations analysis": Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

C. "Inference": A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by products of communications. This includes:

a. Traffic analysis: Gaining knowledge of data by observing the characteristics of communications that carry the data.
b. "Signals analysis": Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

D. "Intrusion": A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. This includes:

a. "Trespass": Gaining unauthorized physical access to sensitive data by circumventing a system's protections.
b. "Penetration": Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
c. "Reverse engineering": Acquiring sensitive data by disassembling and analyzing the design of a system component.
d. Cryptanalysis: Transforming encrypted data into plaintext without having prior knowledge of encryption parameters or processes.

2. "Deception" (a threat consequence): A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. The following threat actions can cause deception:

A. "Masquerade": A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.

a. "Spoof": Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
b. "Malicious logic": In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

B. "Falsification": A threat action whereby false data deceives an authorized entity.

a. "Substitution": Altering or replacing valid data with false data that serves to deceive an authorized entity.
b. "Insertion": Introducing false data that serves to deceive an authorized entity.

C. "Repudiation": A threat action whereby an entity deceives another by falsely denying responsibility for an act.

a. "False denial of origin": Action whereby the originator of data denies responsibility for its generation.
b. "False denial of receipt": Action whereby the recipient of data denies receiving and possessing the data.

3. "Disruption" (a threat consequence): A circumstance or event that interrupts or prevents the correct operation of system services and functions. The following threat actions can cause disruption:

A. "Incapacitation": A threat action that prevents or interrupts system operation by disabling a system component.

a. "Malicious logic": In context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources.
b. "Physical destruction": Deliberate destruction of a system component to interrupt or prevent system operation.
c* "Human error": Action or inaction that unintentionally disables a system component.
d* "Hardware or software error": Error that causes failure of a system component and leads to disruption of system operation.
e* "Natural disaster": Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

B. "Corruption": A threat action that undesirably alters system operation by adversely modifying system functions or data.

a. "Tamper": In context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.
b. "Malicious logic": In context of corruption, any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data.
c* "Human error": Human action or inaction that unintentionally results in the alteration of system functions or data.
d* "Hardware or software error": Error that results in the alteration of system functions or data.

e* "Natural disaster": Any "act of God" (e.g., power surge caused by lightning) that alters system functions or data.

C. "Obstruction": A threat action that interrupts delivery of system services by hindering system operations.

a. "Interference": Disruption of system operations by blocking communications or user data or control information.
b. "Overload": Hindrance of system operation by placing excess burden on the performance capabilities of a system component. (See: flooding.)

4. "Usurpation" (a threat consequence): A circumstance or event that results in control of system services or functions by an unauthorized entity. The following threat actions can cause usurpation:

A. "Misappropriation": A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.

a. "Theft of service": Unauthorized use of service by an entity.
b. "Theft of functionality": Unauthorized acquisition of actual hardware, software, or firmware of a system component.
c. "Theft of data": Unauthorized acquisition and use of data.

B. "Misuse": A threat action that causes a system component to perform a function or service that is detrimental to system security.

a. "Tamper": In context of misuse, deliberate alteration of a system's logic, data, or control information to cause the system to perform unauthorized functions or services.
b. "Malicious logic": In context of misuse, any hardware, software, or firmware intentionally introduced into a system to perform or control execution of an unauthorized function or service.
c. "Violation of permissions": Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.

$ traffic analysis – анализ трафика

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.

$ traffic flow confidentiality – конфиденциальность/секретность трафика

A data confidentiality service to protect against traffic analysis.

$ traffic padding – заполнение трафика

The generation of spurious instances of communication, spurious data units, and/or spurious data within data units to prevent statistical traffic wiretapping.

$ Transport Layer Security (TLS) and Transport Layer Security Protocol (TLSP – механизм и протокол безопасности транспортного уровня

TLS Version 1.0 is an Internet protocol based-on and very similar to SSL Version 3.0. The TLS protocol operation require upper layer services, i.e., session (OSI layer 4) and application layer.

An end-to-end encryption protocol(ISO Standard 10736) that provides security services at the bottom of OSI layer 4, i.e., directly above layer 3.

$ triage (see incident triage)

$ trojan horse – «троянский конь», закладка, компьютерная программа, которая имеет злонамеренные функции, тмеющие своей целью использовать известные уязвимости системы

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.

$ Trusted Introducer (TI) – «доверительный рекомендатель», название услуги, осуществляющей сертификацию CSIRT с целью введения их в «сеть доверия»

The Trusted Introducer (TI) is an initiative of the European CSIRTs. To cooperate efficiently and swiftly when security incidents occur, a certain level of mutual trust is needed between CSIRTs. An important pre-requisite for mutual trust is shared *and accurate* operational knowledge about each other. TI provides European CSIRTs with a public repository that lists all known European CSIRTs.

The TI accreditation service is defined for CSIRTs to be included into web-of trust. Once "accredited" CSIRTs gain access to the restricted TI repository: there they find the details about their fellow accredited CSIRTs, and several value-added services like readily downloadable contact lists and PGP-keyrings, secure discussion fora, automatic RIPE Database IRT-object registration and so on.

$ victim – жертва, используется для обозначения пострадавшей стороны с инциденте безопасности

Victim is individual or organisation which suffered the attack which is reported as an incident report. Typically, victim is described by its network ID, organisation and location information.

$ virtual private network (VPN) – вирутальная приватная сеть, сторящаяся на основе IPSec

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 tunneling links of the virtual network across the real network.

For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

$ virus – вирус, злонамеренная компьютерная программа, имеющая свойство само-воспроизведения и само-распространения

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting.i.e., inserting a copy of itself into and becoming part of another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

$ vulnerability - уязвимость

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

$ web of trust – «сеть доверия»

CSIRT community usage: A network of established relations between CSIRT based on individual contacts or trusted introducer service (for European CSIRTs provided by Trusted Introducer service). CSIRT web-of-trust is supported also by PGP key web of trust.

PKI/PGP usage: A trust-file PKI technique used in PGP for building a file of validated public keys by making personal judgments about being able to trust certain people to be holding properly certified keys of other people.

$ wiretapping – «посдлушивание» в сети

An attack that intercepts and accesses data and other information contained in a flow in a communication system.

"Active wiretapping" attempts to alter the data or otherwise affect the flow; "passive wiretapping" only attempts to observe the flow and gain knowledge of information it contains.

Note. Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as gateway or subnetwork switch.

$ worm – сетевой червь, представляющий собой вариант вируса, распространяющегося по сети

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.