

# Biometric and Computer Security Terminology

**ActiveX** – Is a set of technologies, developed by Microsoft, that are built on the Component Object Model (COM), and enable software components, regardless of the language in which they were created, to work together in a networked environment.

**ActiveX Control** – Are reusable, stand-alone software components that often expose a subset of the total functionality of a product or application. They were formerly referred to as OLE controls or OCX. ActiveX Controls cannot run stand-alone—they must be loaded into a control container, such as Microsoft Visual Basic or Microsoft Internet Explorer. An ActiveX Control can also be embedded in a Visual C++ resource. The DigitalPersona DCOM Software Development Kit includes ActiveX Controls.

**Algorithm** – A series of steps used to complete a task. (RSA)

**Application Programming Interface (API)** – A set of routines that an applications program uses to request and carry out lower-level services performed by a computer operating system.

**Arch** – One of the three most common fingerprint patterns. There are two types of arch patterns, the Plain Arch and the Tented Arch.

**Architecture** – A general term referring to the structure of all or part of a computer system. Also covers the design of system software, such as the operating system, as well as referring to the combination of hardware and basic software that links machines on a computer network.

**Asymmetric cipher** – *Please see Public Key Encryption.*

**Authentication** – The process of proving the identity of a user that is attempting to access a system.

**Authentication Token** – A portable device used for authentication of a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper based lists of one-time passwords.

**Authorization** – The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, that user may be authorized for different types of access or activity.

**Backup Domain Controller (BDC)** – In a Windows NT Server 4.0 or earlier domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). Backup domain controllers also authenticate user logons and can be promoted to function as PDCs as needed. Multiple backup domain controllers can exist on a domain.

**Biometrics** – Authentication techniques that use the analysis of a person's unique, measurable, anatomical traits of the human body as a credential.

**Basic Input Output System (BIOS)** – The lowest level of the Central Processing Unit's operating system. The BIOS contains information that allows the CPU to communicate with the computer's hardware. (Symantec)

**Certificate** – In cryptography, an electronic document binding some pieces of information together, such as a user's identity and public key. (RSA)

**Certificate Authority (CA)** – A person or organization that creates certificates.

**Challenge / Response** – An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.

**Cipher** – An encryption – decryption algorithm. (RSA)

**Cipher text** – Text that has been scrambled or encrypted so that it cannot be read without deciphering it. (Symantec)

**Cleartext** – Also plaintext, the input to an encryption function or the output of a decryption function.

**Component Object Model (COM)** – A specification for building software components that can be assembled into new programs or add functionality to existing programs. COM components can be written in a variety of computer languages and can be updated and reinstalled without requiring changes to other parts of the program.

**Cookie** – A string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart. (Symantec)

**Cracker** – Someone who breaks into computers. Often times Crackers actions are criminal in nature. The term Hacker is often used as a synonym to Cracker. Generally though, the term Hacker is not as closely associated to criminal activity as the term Cracker.

**Cracker Tools** – Programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war-dialers and worms.

**Credentials** – Is something that attests to your identity. Examples of credentials include: passports, driver's license, password, smart card, or fingerprint.

**Cryptoanalysis** – The act of analyzing (or breaking into) secure documents or systems that are protected with encryption. (Symantec)

**Cryptography** – The art and science of using mathematics to secure information by scrambling the information so that it is illegible.

**Decryption** – The translation of encrypted text or data (called the ciphertext) into original text or data (called cleartext). Also called deciphering.

**Data Encryption Standard (DES)** – A symmetric encryption algorithm developed by the US government and IBM in the 1970's. It allows the use of variable key lengths.

**Digital Signature** – Digital code that authenticates whomever signed the document or software. Software, messages, email, and other electronic documents can be signed electronically so that they cannot be altered by anyone else. If someone alters a signed document, the signature is no longer valid. Digital signatures are created when someone generates a hash from a message, then encrypts and sends both the hash and the message to the intended recipient. The recipient decrypts the hash and original message, makes a new hash on the message itself and compares the new hash with the old one. If the hashes are the same, the recipient knows that the message has not been changed. (Symantec)

**Digital Template** – In DigitalPersona's systems, this is a mathematical digitized representation of your fingerprint. The file is not the fingerprint image but is a data string created by feeding the captured fingerprint image through DigitalPersona's proprietary recognition algorithm. It is impossible to reverse the print analysis in an attempt to recreate the fingerprint image.

**Digital Timestamp** – A record mathematically linking a document to a time and date.

**Dynamic-Link Library (DLL)** – API routines that user-mode applications access through ordinary procedure calls. The code for the API routine is not included in the user's executable image. Instead, the operating system automatically points the executable image to the DLL procedures at run time.

**Domain** – In a Windows NT Server 4.0 or earlier domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). Backup domain controllers also authenticate user logons and can be promoted to function as PDCs as needed. Multiple backup domain controllers can exist on a domain.

**Dumpster Diving** – A common and legal method of obtaining sensitive information (i.e. passwords, logins, phone numbers, etc.) by rummaging through discarded trash.

**Electrostatic Discharge (ESD)** –The transference of static electricity from a human to an integrated circuit. This transference is generally catastrophic to integrated circuits.

**Encryption** – The conversion of plaintext or data into unintelligible form by means of a reversible translation that is based on a translation table or algorithm. Also called cipherring.

**Firewall** – A system or combination of systems that enforces a boundary between two or more networks.

**Global Features** – The ridge patterns on a finger. There are three main types of global features: Arch, Loop, Whorl.

**Hash Function** – A function that takes a variable sized input and has a fixed size output. (RSA)

**Identification** – A process through which one ascertains the identity of another person or entity within a large group of people.

**Insider attack** – An attack originating from inside a protected network.

**Kerberos** – A security system that authenticates users. Kerberos doesn't provide authorization to services or databases; it establishes identity at logon, which is used throughout the session. The Kerberos protocol is the primary authentication mechanism in the Windows 2000 operating system.

**Key** – A string of bits used widely in cryptography, allowing people to encrypt and decrypt data, a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. (RSA)

**Key Escrow** – The process of having a third party hold onto encryption keys. (RSA)

**Key Pair** – The full key information in a public-key cryptosystem, consisting of the public key and private key.

**Logic Bomb** – A virus that only activates itself when certain conditions are met. (Symantec)

**Loop** – The loop is the most common type of fingerprint pattern and accounts for about 65% of all prints.

**Microsoft Management Console (MMC)** – A feature of Internet Information Server, is a Windows-based multiple document interface (MDI) application that makes extensive use of Internet technologies. Both Microsoft and independent software vendors (ISVs) can extend the console by writing MMC snap-in components, which are responsible for performing management tasks.

**Minutia Point** – A point on your finger where the ridgeline ends or splits. Each minutia point has unique and measurable characteristics. There are five main types of minutia points.

- Island: A short ridge with distinct start and end points.
- Bifurcation: Also called a fork where one ridge splits into two.
- Enclosure: Where a ridge splits into two then rejoins into one.
- Terminator: Where a ridge line ends.
- Dot: A ridge line short enough it appears to be a point.

**National Institute of Standards and Technology (NIST)** – A United States agency that produces security and cryptography related standards (as well as others); these standards are published as FIPS documents. (RSA)

**OCX control** – *Please see ActiveX Control.*

**OLE control** – *Please see ActiveX Control.*

**Password Cracker** – A program that uses a dictionary of words, phrases, names etc. to guess a password. (Symantec)

**Password Encryption** – A system of encrypting electronic files using a text based credential or password. Anyone who knows the password can decrypt the file.

**Password Shadowing** – The storage of a user's username and password in a network administrator database. (Symantec)

**Primary Domain Controller (PDC)** – In a Windows NT Server 4.0 or earlier domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one primary domain controller. In Windows 2000, one of the domain controllers in each domain is identified as the PDC for compatibility with downlevel clients and servers.

**Private Key** – In public-key cryptography, this key is the secret key. It is primarily used for decryption, but is also used for encryption with digital signatures. (RSA)

**Public Key** – In public-key cryptography this key is made public to all, it is primarily used for encryption but can be used for verifying signatures. (RSA)

**Public Key Encryption** – System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption, and a corresponding private key used during decryption. (Symantec)

**Public Key Infrastructure (PKI)** – A public key infrastructure (PKI) makes it possible for you to identify and trust another Internet user, which can be another person, a computer, or some other electronic entity.

**Ridge** – The area, or line, of raised skin on your finger. Collectively, the pattern ridges on your finger are known as a fingerprint.

**RSA Algorithm** – A public-key cryptosystem based on exponentiation in modular arithmetic.. RSA stands for Rivest, Shamir, and Adleman, the developers of the RSA public-key cryptosystem and the founders of RSA Data Security, Inc.

**Session Key** – A key for symmetric-key cryptosystems which is used for the duration of one message or communication session. (RSA)

**Shoulder Surfing** – Looking over someone’s shoulder to see the numbers they dial on a phone or the information they enter into a computer. (Symantec)

**Secure HyperText Transfer Protocol (S-HTTP)** – A secure way of transferring information over the World Wide Web. (RSA)

**Solid State Fingerprint Sensor** – A type of fingerprint sensor that is an integrated silicon circuit the size of a fingertip. Solid state sensors measure fingerprint features through variations in temperature, or capacitance variance. Solid state sensors are adversely susceptible to electrostatic discharge.

**Secure Socket Layer (SSL)** – A protocol used for providing encrypted and authenticated service over the Internet. Using the Rivest, Shamir and Adleman (RSA) public key, specific TCP/IP ports can be encrypted. This general-purpose encryption standard is primarily used for secure Internet transactions.

**Smartcard** – A card, not much bigger than a credit card, that contains an imbedded computer chip that is used to store or process information. Smartcards work in conjunction with a Smartcard reader.

**Symmetric Cipher** – An encryption algorithm that uses the same key that is used for encryption as decryption. (RSA)

**Sniffer** – A networking tool that can capture data as it goes through a network. Sniffers are often programmed to search for and decode specific types of information. (Symantec)

**Social Engineering** – Telling a lie, or using deceptive tactics to gain access to private information. (Symantec)

**Spoofing** – Penetrating a computer by posing as an authorized user. (Symantec)

**Triple DES** – For some time it has been common practice to protect information with triple-DES instead of DES. This means that the input data is, in effect, encrypted three times. (RSA)

**Trojan Horse** – A program that is disguised to make a user want to run it. Trojans may display features of the expected program; they may show a game, or a network login. However, Trojans can cause many problems. They can steal passwords, delete data, format hard drives, or cause other problems.

**Tunneling** – Also called encapsulation. Tunneling enables a network to send or receive data through another network's connections. It does this by layering a special protocol on top of an existing one (usually done at the packet level). (Symantec)

**User Authentication Manager (UAM)** – A flexible and extensible DigitalPersona software architecture that enables the management of different authentication technologies (passwords, biometrics, smartcards, etc.).

**User Verification Manager (UVM)** – A DigitalPersona enabled, IBM client-based authentication and authorization policy software that is used to set-up user identity and determine access rights and privileges. The UVM ships as part of IBM PC 300PL systems.

**Verification** – The act of recognizing that a person or entity is who or what it claims to be. (RSA)

**Virus** – Computer code that attaches itself to other files on a computer system, Viruses spread through programs that are shared with other computers over the Internet. Some viruses are malicious and damage files and programs. Viruses spread without the user's knowledge and should be scanned for by an AntiVirus program on a regular basis. (Symantec)

**Virtual Private Network (VPN)** – These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes. (Symantec)

**Whorl** – A fingerprint defined by at least one ridge that makes a complete circle. Whorl patterns occur in about 30% of all fingerprints.

**Worm** – A program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.