Definition of Terms used by the Auto-ID Labs in the Anti-Counterfeiting White Paper Series

Alfio Grasso and Peter H. Cole
School of Electrical and Electronics Engineering,
The University of Adelaide, SA 5005, Australia
alf@eleceng.adelaide.edu.au and cole@eleceng.adelaide.edu.au

ABSTRACT
The objective of this paper is to provide a reference source for terms used by the Auto-ID Labs, Adelaide in the Anti-Counterfeiting White Paper Series. Such terms are commonly used in the security industry, and are now starting to fund their way into RFID applications. While the terms are well defined in the security industry, RFID Engineers need to have a common understanding. Papers in the white series have been reviewed, and when a term is used that is not contained either within ISO 19762 - Harmonized vocabulary, for RFID related terms, or EPCglobal's Tag/Reader Security Glossary (26th April 2006), a definition is provided in this document.

Appendix A lists useful Security & Authentication Glossaries, available online, some of which have been used to compile this Glossary.

Most of the definitions in this document come from Wikipedia (http://en.wikipedia.org/).

AES:
Advanced Encryption Standard (AES) was announced in September 1997as the successor to DES. AES is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf), that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. AES supports key sizes of 128 bits, 192 bits, and 256 bits, in contrast to the 56-bit keys offered by DES. The reference for this description is http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html

Abelian Group:
In mathematics, an abelian group, also called a commutative group, is a group (G,*), such that a*b=b*a for all a and b in G. In other words, the order of elements under the conjunction * doesn't matter.

Asymmetric public key system:
An asymmetric public key system is a cryptographic system in which a different key is used to decrypt a message from the key originally used to encrypt the message. RSA is an example of an asymmetric public key system. Each user has a public key, which is different for each user, which is exchanged via secure methods such as digital signatures, trusted systems or otherwise. Each user also has a private key, again which is different for each user. The public and private keys are mathematically related, but to deduce (calculate) the private key from the public is believed to be impossible (it has not yet been mathematically proven). See also Cryptography / Cryptographic Algorithm, Public Key Cryptography Systems, Public/Private Keys, RSA and Symmetric Key System definitions below.

Buffer Overflow Vulnerability:
In computer security and programming, a buffer overflow, or buffer overrun, is an anomalous condition where a process attempts to store data beyond the boundaries of a buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data. Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows. See Heap Smashing Attack and Stack Smashing Attack below.

Challenge-and-Response Protocol:
The Challenge-Response protocol is an exchange of information used to establish the authenticity of a party in a communication session. The mechanism, is that the sender choses a challenge x, which is a random number and transmits it to the receiver. The receiver computes y = eK (x) and transmits the value y to the reader (here e is the encryption rule that is publicly known and K is a secret key known only to the sender and receiver). The receiver then computes y' = eK (x) and then verifies that y' = y.

Characteristic polynomial[1]:
The characteristic polynomial of a linear feedback shift register is defined as the polynomial $P_n(x) = 1+ c_1x + c_2x^2 + \ldots + c_nx^n$, with $c_n \neq 0$, and where the feedback coefficients c_i of the register are either 0 or 1. The characteristic polynomial is primitive if (a) it has no proper factors and (b) $P_n(x)$ does not divide x^d+1 for any $d<2^n-1$.

Ciphertext:
Ciphertext is the message after the original message (or plaintext) has been encrypted. Ciphertext = Encryption(plaintext). See keystream and plaintext below.

Code Injection Vulnerability:
Code injection is a technique to introduce (or "inject") code into a computer program or system by taking advantage of the un-enforced and unchecked assumptions the system makes about its inputs. Most of these problems are related to erroneous or no assumptions of what input data is possible, or the effects of special data. The purpose of the injected code is typically to bypass or modify the originally intended functionality of the program. Classic examples of dangerous assumptions a software developer might make about the input to a program include:

- assuming that metacharacters for an API never occurs in an input; e.g. assuming punctuation like quotation marks or semi-colons would never appear;
- assuming only numeric characters will be entered as input;
- assuming the input will never exceed a certain size;
- assuming that numeric values are equal or less than upper bound;
- assuming that numeric values are equal or greater than lower bound;

[1] Welsh, Dominic, "Codes and Cryptography", Oxford University Press, Oxford. 1990, ISBN 0-19-853287-3.

- assuming that client supplied values set by server (such as hidden form fields or cookies), cannot be modified by client. This assumption ignores known attacks such as Cookie poisoning, in which values are set arbitrarily by malicious clients;
- assuming that it is okay to pick pointers or array indexes from input;
- assuming an input would never provide false information about itself or related values, such as the size of a file.

Computationally intractable:
Computationally intractable problems are mathematical problems that are solvable in theory, but cannot be solved in practice. What can be solved "in practice" is open to debate, but in general only problems that have polynomial-time solutions are solvable for more than the smallest inputs.
To see why exponential-time solutions are not usable in practice, consider a problem that requires 2^n operations to solve (n is the size of the input). For a relatively small input size of n=100, and assuming a computer that can perform 10^{10} (10 giga) operations per second, a solution would take about $4*10^{12}$ years, much longer than the current age of the universe.

Cookie:
A cookie is a string of data exchanged between a web server and a web browser that may contain user preferences and personal information. Cookies are assigned to a web browser during the protocol negotiation. When the same web browser accesses that particular domain again, it constructs its request header such that it contains the cookie information, provided that cookies have been enabled in the web browser and that the cookie has not expired.

Cryptography / Cryptographic Algorithm:
A Cryptographic Algorithm is firmware or some combination of hardware, software and firmware that implements cryptographic logic or processes, on a data input stream and transforms the data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form.
Cryptography systems can be broadly classified into:
- Symmetric-key systems that use a single key that both the encryptor and decryptor have, and
- Asymmetric-key (Public-key) systems that use two keys, a public key known to everyone and a private key that only the decryptor or the signer of the message uses. The public key is generally used for encryption and/or Digital Signature verification.

Data Keys (KD):
Data keys are used for bulk encryption, and are used in a three level key management system (ANSI X9.17), used in financial institutions. The highest level is Master Key, which is the most secure and manually delivered, some Master Keys are one-time codes. The next level is a Key Encryption Keys (KEK), which are encrypted from the Master Key, and used by major nodes in the financial network to establish a local secure connection, and are changed periodically. Data keys are the lowest level and used to encrypt message.

Decryption/ Encryption:
A cryptographic transformation of encrypted data that restores encrypted data to its original state.

Denial of Service (DoS) attack:
A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

DES:
Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS) 46-3, which describes the data encryption algorithm (DEA). The DEA is also defined in the ANSI standard X3.92. The DEA has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key). The DEA is a symmetric cryptosystem, specifically a 16-round Feistel cipher and was originally designed for implementation in hardware.

When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code (MAC) (see Message Authentication Code below).

Diffie-Hellman problem:
The Diffie-Hellman problem (DHP) is the task in cryptography of computing g^{xy} given g, g^x, and g^y, where g is an element of some group, typically the multiplicative group of a finite field, or an elliptic curve group. In other words, the problem is to perform the private key operation given only their public keys in a Diffie-Hellman key exchange. A fast means of solving the DHP would yield a method to break Diffie-Hellman key exchange and many of its variants. To specify the problem with complete precision, one must specify the group exactly and how x and y are generated. The problem was first posed by Whitfield Diffie and Martin Hellman. In cryptography, for certain groups, it is assumed that the DHP is hard, and this is often called the Diffie-Hellman assumption.

Digital Signature:
A value (called “digital signature” or simply “signature”) computed with a cryptographic algorithm for a data object in such a way that any one can use the signature to verify the data's originator and integrity.

Elliptic Curve Cryptography:
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The elliptic curve function is the perimeter of an ellipse $y^2 = x^3 + ax + b$, where all variables, x, y, and parameters, a, b must be integers. The set of points on such a curve (i.e., all solutions of the equation together with a point at infinity) can be shown to form an abelian group (with the point at infinity as identity element). If the coordinates x and y are chosen from a large finite field, the solutions form a finite abelian group. The discrete logarithm problem on such elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field. Thus keys in elliptic curve cryptography can be chosen to be

much shorter for a comparable level of security. In ECC use, the solution $y^2 = x^3 + ax + b$ is usually done over a modulo field, e.g. $[y^2 = x^3 + ax + b] \mathrm{mod}(n)$ where n is a prime number.

Encryption:
See Decryption and Cryptographic Algorithm above.

Feistel cipher:
In cryptography, a Feistel cipher is a block cipher with a particular structure, named after IBM cryptographer Horst Feistel. A large proportion of block ciphers use this scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel ciphers and similar constructions combine multiple rounds of repeated operations, such as:

* Bit-shuffling (often called permutation boxes or P-boxes);
* Simple non-linear functions (often called substitution boxes or S-boxes);
* Linear mixing (in the sense of modular algebra) using XOR

to produce a function with large amounts of "confusion and diffusion". Bit shuffling creates the diffusion effect, while substitution is used for confusion.

Fractal tail distribution:
A long-tailed or heavy-tailed probability distribution is one that assigns relatively high probabilities to regions far from the mean or median. In the context of Internet Traffic a number of quantities of interest have been shown to have a long-tailed distribution. For example, considering the sizes of files transferred from a web-server, then, to a good degree of accuracy, the distribution is heavy-tailed, that is, there are a large number of small files transferred but, crucially, the number of very large files transferred remains significant.

Firewall:
In computing, a firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy. A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle (see Least Privilege Principle below).

Genus:
In general genus is a term from algebraic geometry. It indicates how many twists or torsions are there in the curve. For example for any conic section, such as the circle, the (actual, geometrical) ellipse, parabola, hyperbola, there are no twists, hence genus is 0. Similarly for other planar figures such as a triangle, the genus is 0. Elliptic curves have genus of 1, while hyperelliptic curves have a genus of 2 or more. In general, The Fermat curve, derived from $x^n + y^n = z^n$, has genus $g= (n-1)(n-2)/2$.

Hash:

A hash function H is a function that transforms a message m into a fixed size string denoted as the hash value h. h = H(m) Hashing is a quite common technique used in database applications and cryptography. In cryptography, however, hash functions need to exhibit the following requirements:

- One way: Easy to derive h = H(m) but computationally infeasible to calculate the message m given the hash value h.
- Variable input length: It should be possible to derive h = H(m) independent on the size of m.
- Fixed output length: The hash value should always be of the same length independent of the message m.
- Collision free: Given a message x it should be computationally infeasible to find a message y so that H(x) = H(y).

Hash functions are used as message digests (reduction of large message to a much smaller number of bits) to ensure data integrity and to provide a digital signature.

Heap Smashing Attacks:
A buffer overflow occurring in the heap data area is referred to as a heap overflow (or Heap Smashing Attack) and is exploitable in a different manner to that of stack-based overflows (See Stack Smashing Attack below). Memory on the heap is dynamically allocated by the application at run-time and typically contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.

Hyper-Elliptic Curve Cryptography:
Hyperelliptic curve cryptography is similar to elliptic curve cryptography (ECC) insomuch as the algebraic geometry construct of a hyperelliptic curve with an appropriate group law provides an Abelian group on which to do arithmetic.

Although introduced only 3 years after ECC, not many cryptosystems implement hyperelliptic curves because the implementation of the arithmetic isn't as efficient as with cryptosystems based on elliptic curves or factoring (RSA). Because the arithmetic on hyperelliptic curves is more complicated than that on elliptic curves, a properly implemented cryptosystem based on hyperelliptic curves can be more secure than elliptic curve based cryptosystems that have the same key size.

The hyperelliptic curves used are typically of the sort $y^2 = f(x)$, where the degree of $f(x) = 2g+1$, where g=genus.

Interlock Protocol:
The Interlock Protocol is a method that exposes a middle-man attack (see Man in the Middle attack below) who might try to compromise two parties that use anonymous key agreement to secure their conversation. The Interlock protocol works roughly as follows: the sender sends half the encrypted message to the receiver. The receiver uses the senders key and replies with half of response encrypted message. The sender then sends the other half of encrypted message to the receiver, who then sends the remainder of the response encrypted message. The strength of the protocol lies in the fact that half of an encrypted message cannot be decrypted. Thus, if the man-in-the-middle intercepts the first half encrypted message he will be unable to decrypt that first half encrypted message (encrypted using his key) and re-encrypt it using the

receivers. He must wait until both halves of the message have been received to read it, and can only succeed in duping one of the parties if he composes a completely new message.

Internet Key Exchange (IKE) protocol:
Internet key exchange (IKE) is the protocol used to set up a Security Association in the IPsec protocol suite. IKE is defined in RFC 2409 (http://rfc.net/rfc2409.html) and uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a Pre-shared key, is used to mutually authenticate the communicating parties.

Internet Protocol Security (IPsec):
IPsec (IP security) is a standard for securing Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. IPsec provides security at the network layer. IPsec is a set of cryptographic protocols for (1) securing packet flows and (2) key exchange. There are two secure packet flows (1) Encapsulating Security Payload (ESP) provides authentication, data confidentiality and message integrity; (2) Authentication Header (AH) provides authentication and message integrity, but does not offer confidentiality. Currently only one key exchange protocol is defined, the IKE (Internet Key Exchange) protocol. IPsec protocols operate at the network layer, layer 3 of the OSI model. Other Internet security protocols in widespread use, such as SSL and TLS, operate from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting both TCP and UDP-based protocols, but increases its complexity and processing overhead, as it cannot rely on TCP (layer 4 OSI model) to manage reliability and fragmentation.

Key Encrypting Keys (KEK):
See Data Keys above.

Keystream:
A set of bits randomly obtained, in which plaintext can be converted to ciphertext. The most common form of conversion is a process of XORing each bit of the plaintext message with the corresponding bit in the key or keystream.

Least Privilege Principle:
In computer science the principle of minimal privilege, also known as principle of least privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module (which can be for example, a process, a user or a program) must be able to see only such information and resources that are immediately necessary. The idea of the principle is to grant just the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults (fault tolerance) and malicious behaviour (computer security).

Lightweight Cryptography:
Lightweight cryptography employs symmetric encryption algorithms and modes of encryption, along with key-management schemes, so that implementations can be simplified, to the point that they may be implemented on passive RFID tags, where energy consumption cannot be devoted to intense computational tasks.

Message Authentication Code (MAC):
A cryptographic message authentication code (MAC) is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks. This implies that an attacker be unable to find any two messages M and M' which both produce the same MAC under some unknown secret key, even when the attacker has access to an "oracle" which possesses the secret key and generates MACs for messages of the attacker's choosing. Note that this differs from the property of collision resistance required by a cryptographic hash function: a MAC may be considered secure even if the key-holder can efficiently find collisions.

MACs differ from digital signatures, as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on keys before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures: any user who can verify a MAC is also capable of generating MACs for other messages.

Man in the Middle Attack (MITM):
In cryptography, a man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. The MITM attack is particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication. With the exception of the Interlock Protocol, all cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over some kind of secure channel. Many key agreement methods with different security requirements for the secure channel have been developed. The MITM attack may include one or more of:

- eavesdropping, including traffic analysis and possibly a known plaintext attack;
- chosen ciphertext attack, depending on what the receiver does with a message that it decrypts;
- substitution attack;
- replay attacks;
- denial of service attack.

Master Keys:
See Data Keys above.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP):
The Challenge-Handshake Authentication Protocol (CHAP) authenticates a user to an Internet access provider. RFC 1994: (http://www.ietf.org/rfc/rfc1994.txt) PPP

Challenge Handshake Authentication Protocol (CHAP) defines the protocol. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link, and may happen again at any time afterward. The verification is based on a shared secret (such as the client user's password).

1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function, such as MD5 (see below).
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 to 3.

CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and of a variable challenge-value.

Message-Digest algorithm 5 (MD5):
MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321) (http://www.faqs.org/rfcs/rfc1321.html), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. In 1996, a flaw was found with the design of MD5; while it was not a clearly fatal weakness, cryptographers began to recommend using other algorithms, such as SHA-1 (recent claims suggest that SHA-1 has been broken, however) (see SHA-1 below). In 2004, more serious flaws were discovered making further use of the algorithm for security purposes questionable.

NIST Test for random numbers:
National Institute of Standards and Technology, USA Publication (SP) 800-22 is a Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. The publication and the associated tests are intended for individuals who are responsible for the testing and evaluation of random and pseudorandom number generators. NIST SP 800-22 is available at http://csrc.nist.gov/rng/

The NIST Statistical Test Suite is a package of 16 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by random or pseudorandom number generators. The tests focus on a variety of different types of non-randomness that could exist in a sequence.

One Time Codes (One Time Pad):
A one-time pad, sometimes called the Vernam cipher, uses a string of bits that is generated completely at random. The keystream is the same length as the plaintext message and the random string is combined using bitwise XOR with the plaintext to produce the ciphertext. Since the entire keystream is random, even an opponent with infinite computational resources can only guess the plaintext if he or she sees the ciphertext.

One Way (Hash) Function:
A hash function, H, is defined, by h = H(m), where m is the message, and h, is the hash value. The requirements for cryptographic hash functions are:

(a) The input may be of any length;
(b) The output must have a fixed size;
(c) Hash function z = H(k) is comparatively easy to calculate, for any given k;
(d) H(m) is one-way, i.e. is hard to invert, infeasible, computationally, to obtain, $k = z^{-1}$, or $H^{-1}(k)$, where z = H(k);
(e) H(m) is collision free.

Physical Attack:
In RFID systems the labels themselves are exposed to physical attacks due to the absence of tamper proofing as dictated by cost limitations of low cost tags. Physical attacks are possible irrespective of whether measures are in place to protect labels. The majority of physical attacks possible on devices in general can be bundled into two broad categories based on the means used for accessing the device.
Non-invasive attacks: These attacks are as a result of timing analysis, power analysis, analysis of certain glitches [radio finger printing], and exploitation of data remanence.
Invasive attacks: An adversary may simply reverse engineer labels to create fraudulent labels for cloning or DOS attacks or use probing techniques to obtain information stored in memory (micro-probing and Focus Ion Beam editing) or alter information stored in memory (using a laser cutting microscope). Attacks, such as optical probing and fault injection attacks where the chip is removed from its packaging with the passivation layer still unbroken are also invasive attacks but these attacks are may be further qualified as semi-invasive attacks.

Plaintext:
Plaintext is the original message, prior to encryption, or the message obtained after decryption, both of which should be the same, if the correct encryption/decryption process was used.

Public Key Cryptography Systems:
Public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key. This is done by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically. In public key cryptography, the private key is kept secret, while the public key may be widely distributed. In a sense, one key "locks" a lock; while the other is required to unlock it. It should not be possible to deduce the private key of a pair given the public key, and in high quality algorithms no such technique is known. There are many forms of public key cryptography, including:

- public key encryption — keeping a message secret from anyone that does not possess a specific private key;
- public key digital signature — allowing anyone to verify that a message was created with a specific private key;
- key agreement — generally, allowing two parties that may not initially share a secret key to agree on one.

Public/Private Keys:

A key is a constant number which is used in the encryption/decryption process. The public key is used to encrypt messages and can be insecure, but the private key must be confidentially exchanged between the originator (source) and receiver (destination).

PUF (Physically Unclonable Functions):
In RFID PUF circuits may be exploited to provide a source of truly random bit sequences, to be used in a challenge-response protocol exchange in security and authentication applications. The technique employs a PUF (Physically Unclonable Function) circuit which has an exponential number of delay path configurations determined by a challenge input. The observation of PUF results reveals that a string of challenge bit sequences can be used to generate a response string unique to each IC. The PUF circuit is able to uniquely characterise each IC due to manufacturing variations. These individual characteristics then become similar to the secret keys used in a symmetrical encryption scheme. Thus, it is possible to identify and authenticate each IC reliably by observing the PUF response.

Quality of Service (QoS):
In the fields of packet-switched networks and computer networking, the traffic engineering term Quality of Service (QoS) refers to the probability of the telecommunication network meeting a given traffic contract, or in many cases is used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

Replay Attack:
A replay attack is one in which an attacker monitors transactions (messages) between two communicating parties, record the transactions and use parts of the messages to illicitly obtain information. Retransmission of such recorded information may be used to attack the communication system.

RSA:
In cryptography, RSA is an algorithm for public-key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames. RSA involves two keys: a public key and a private key. The public key is known to everyone and is used to encrypt messages. These messages can only be decrypted by use of the private key. In other words, anybody can encrypt a message, but only the holder of a private key can actually decrypt the message and read it. Refer to http://en.wikipedia.org/wiki/RSA for a detailed explanation of the RSA algorithm.

Secure Shell (SSH):
Secure Shell or SSH is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and (optionally) to allow the remote computer to authenticate the user. SSH provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes. SSH is typically used to login to a remote machine and execute commands, but it also supports tunnelling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. An SSH server, by default, listens on the standard TCP port 22.

Secure Hash Algorithm SHA-1
The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard. The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512 — sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

Secure Socket Layer (SSL):
See Transport Layer Security (TLS) below.

SQL Injection Vulnerability:
See Code Injection Vulnerability above.

Stack Smashing Attack:
Stack smashing attacks refers to various techniques used by attackers to compromise the security of a computer system, by causing a buffer overflow, on stack-allocated variables. See Heap Smashing Attack above for another kind of buffer overflow attack.

Symmetric key system:
A symmetric key system is a cryptographic system in which both the sender and the receiver use the same keys.

TCP/IP:
The internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It is sometimes called the TCP/IP protocol suite, after the two most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two defined. TCP/IP is composed of layers:

- IP - is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number).
- TCP - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

Transport Layer Security (TLS)
Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols which provide secure communications on the Internet. There

are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same.

The first definition of TLS appeared in RFC 2246: "The TLS Protocol Version 1.0". The current approved version is 1.1, which is specified in RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

Other RFCs subsequently extended TLS, including:

- RFC 2712: "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)". The 40-bit cipher suites defined in this memo appear only for the purpose of documenting the fact that those cipher suite codes have already been assigned.
- RFC 2817: "Upgrading to TLS Within HTTP/1.1", explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection. This allows unsecured and secured HTTP traffic to share the same well known port (in this case, http: at 80 rather than https: at 443).
- RFC 2818: "HTTP Over TLS", distinguishes secured traffic from insecure traffic by the use of a different 'server port'.
- RFC 3268: "AES Cipher suites for TLS". Adds Advanced Encryption Standard (AES) cipher suites to the previously existing symmetric ciphers.
- RFC 3546: "Transport Layer Security (TLS) Extensions", adds a mechanism for negotiating protocol extensions during session initialisation and defines some extensions.
- RFC 4279: "Pre-Shared Key Cipher suites for Transport Layer Security (TLS)", adds three sets of new cipher suites for the TLS protocol to support authentication based on pre-shared keys.
- RFC 4347: "Datagram Transport Layer Security" specifies a TLS variant that works over datagram protocols (such as UDP).
- RFC 4366: "Transport Layer Security (TLS) Extensions" describes both a set of specific extensions, and a generic extension mechanism.

The SSL protocol exchanges records; each record can be optionally compressed, encrypted and packed with a message authentication code (MAC). Each record has a content_type field that specifies which upper level protocol is being used.

When the connection starts, the record level encapsulates another protocol, the handshake protocol, which has content_type 22.

The client sends and receives several handshake structures:

1. It sends a ClientHello message specifying the list of cipher suites, compression methods and the highest protocol version it supports. It also sends random bytes which will be used later.
2. Then it receives a ServerHello, in which the server chooses the connection parameters from the choices offered by the client earlier.
3. When the connection parameters are known, client and server exchange certificates (depending on the selected public key cipher). These certificates are currently X.509, but there's also a draft specifying the use of OpenPGP based certificates.

4. The server can request a certificate from the client, so that the connection can be mutually authenticated.
5. Client and server negotiate a common secret called "master secret", possibly using the result of a Diffie-Hellman exchange, or simply encrypting a secret with a public key that is decrypted with the peer's private key. All other key data is derived from this "master secret" (and the client- and server-generated random values), which is passed through a carefully designed "Pseudo Random Function".

TLS/SSL protocols have a variety of security measures:

1. Numbering all the records and using the sequence number in the MACs.
2. Using a message digest enhanced with a key (so only with the key can you check the MAC). This is specified in RFC 2104).
3. Protection against several known attacks (including man in the middle attacks), like those involving a downgrade of the protocol to previous (less secure) versions, or weaker cipher suites.
4. The message that ends the handshake ("Finished") sends a hash of all the exchanged data seen by both parties.
5. The pseudo random function splits the input data in 2 halves and processes them with different hashing algorithms (MD5 and SHA), then XORs them together. This way it protects itself in the event that one of these algorithms is found vulnerable.

Trap Door One Way Function:

A trapdoor function is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are widely used in cryptography. In mathematical terms, if f is a trapdoor function there exists some secret information y, such that given f(x) and y it is easy to compute x. For example if $[y=x^n]$mod(p), mod(p) is the secret information, and p is usually a prime number. Without the mod(p) it may be easy for an eavesdropper to map the values transmitted and guess that the sequence fits an exponential curve and hence calculate x.

Trojan Attack or Trojan Horse:

A Trojan horse is a malicious program that is disguised as or embedded within legitimate software. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. There are two common types of Trojan horses. One, is otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer to peer file sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives. Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. Trojan horse programs depend on actions by the intended victims. As such, if trojans replicate and even distribute themselves, each new victim must run the program/trojan.

User Datagram Protocol (UDP):

The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP can also stand for "Unreliable". It doesn't mean you will lose all your data, but it does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also its stateless nature is useful for servers that answer small queries from huge numbers of clients. Compared to TCP, UDP is required for broadcast (send to all on local network) and multicast (send to all subscribers). Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, Trivial File Transfer Protocol (TFTP), and online games.

Virtual Private Network (VPN):
A virtual private network (VPN) is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well-defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

VPN involves two parts:
(1) The protected or "inside" network that provides physical security and administrative security sufficing to protect transmission, and
(2) A less trustworthy or "outside" network or segment (the internet).

Generally, a firewall sits between a remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter. Many VPN client programs can be configured to require that all IP traffic must pass through the tunnel while the VPN is active, for better security. From the user's perspective, this means that while the VPN client is active, all access outside their employer's secure network must pass through the same firewall as would be the case while physically connected to the office ethernet.

Appendix A
Other online sources of terms and glossaries

http://www.opengroup.org/onlinepubs/008329799/glossary.htm#tagcjh_12

http://www.discretix.com/glossary.shtml

http://www.orionsec.com/Security_Glossary.html

http://www.17799central.com/glossary.htm

http://www.watchguard.com/glossary/?nav=ic

http://www.primode.com/glossary.html

http://www-306.ibm.com/software/webservers/httpservers/doc/v1326/manual/ibm/9agloss.htm

http://www.clusit.it/whitepapers/glossary.htm

http://www.aamc.org/members/gir/gasp/definitions.pdf

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_GlossaryofTerms.pdf

http://www.infosec.gov.hk/english/general/glossary.htm