QVLx Labs

Terminology of Embedded Systems Security

Purpose

In order to dive deeply into the vast and exciting field of cybersecurity, it's necessary to establish a baseline set of terminology so that semantics aren't a barrier to understanding concepts. This document defines terms commonly used in the field.

Access Control List (ACL)

A datastructure that holds a set of permissions used to access a resource.

Access Control Mechanism

Specific functionality that allows authorized access and denies unauthorized access.

Adaptive Content Inspection (ACI)

Data loss prevention mechanism that requires information processed on a system to conform to a set of policies.

Advanced Encryption Standard (AES)

Symmetric key encryption method. Better than DES and 3DES.

Advanced Persistent Threat (APT)

Targeted attack by a stealthy threat actor with patience and resources. Typically nation or state sponsored. Attacker learns about the target system and carry out specific misdeeds or acquire specific data undetected over a long period of time.

Asymmetric cryptography

Also known as public-key cryptography, this is a cryptosystem that uses a public-private key pair where the public key can be used to encrypt by any party but only the party that has access to the private key can decrypt.

Attack surface

Aggregate of the potential ways that an attacker can gain entry into a system of interest.

Authentication

Verifying whether the identity, priveleges, or other properties of an entity hold true.

Autokey cipher

A cipher that incorporates plaintext into a keystream.

Availability

Ensuring that data is readily available when it is needed by intended parties.

Black hat

A cracker and criminal, using skills for nefarious purposes.

Black–box testing

Penetration testing where the tester does not know details on the composition of the tested system.

Blacklist

Better term is blocklist. Access control mechanism where entities on the list are denied access to whatever is being controlled.

Block cipher

Symmetric key cipher that uses a plaintext string of fixed-length bits to generate a string of ciphertext output.

Block cipher mode of operating

Algorithm that uses block cipher to secure data in larger chunks than a block.

Blockchain

A highly secure and fault-tolerant database built on cryptographically linked blocks. Each block contains the hash of the previous block, a timestamp, and a Merkle tree of the transaction ledger. All nodes verify transactions in their ledger copy in a peer-to-peer, decentralized fashion.

Blue team

White hats that collaborate to defend a target system during a simulated cyberattack.

Bomb

Malicious script that activates upon detection that a specific event or point in system time has occured.

Bootloader

Software that performs hardware checks, initializes processor and peripherals, partitions or configures registers, loads an OS or next-stage bootloader into RAM and passes control to it, and updates firmware.

Botnet

A collection of computers that have been hacked and are remotely controlled by the hacker. If done skillfully, the user is completely unaware that their machine is compromised.

Brute force

An attack conducted by trying a large number of possible solutions until the correct solution is found.

Buffer overflow

If the boundaries of a fixed-length region of memory used to store data are not checked or tightly enforced when data is entered, the data can exceed the region and this allows an attacker to potentially access unauthorized memory and facilitate various attacks.

Buffer overflow prevention systems (BOPS)

Protective software that can detect when a buffer overflow event happens and subsequent exploitation.

Certificate authority

An official entity that acts as a trusted third party that issues digital certificates.

Chain of Trust

Verification method for checking the validity of software by verifying each hardware or software component between the software entity and its root of trust.

Chief information security officer (CISO)

Executive that oversees security strategy and implementation in an organization.

CIA triad

Security policy model centered on the confidentiality, integrity, and availability of information.

Cipher

Encryption algorithm.

Cipher block chaining mode (CBC)

Nondeterministic block cipher mode where plaintext blocks are XOR'd with their previous blocks and "chained". The very first block is a random initialization vector.

Cipher feedback mode (CFB)

Block cipher mode where you take the most recent ciphertext block, pass it through the block cipher, and then exclusive-or that with the plaintext block to generate the next ciphertext block

Ciphertext

Encryption text.

Common Vulnerabilities and Exposures (CVE)

MITRE-maintained public database of known security vulnerabilities.

Common vulnerability scoring system (CVSS)

Standardized system for measuring severity of software vulnerabilities.

Common weakness enumeration (CWE)

Community developed database for identifying or classifying software weaknesses, vulnerabilities, mitigations, and preventions.

Communications security (COMSEC)

Broad security field around protecting transmitted data.

Computer Network Attack (CNA)

Subset of CNO involving disruption, degradation, denial, or destruction of enemy systems using computer network means.

Computer Network Defense (CND)

Subset of CNO involving protection, monitoring, analysis, detection, and response of friendly systems from enemy attempts using network means.

Computer Network Exploitation (CNE)

Subset of CNO involving the gathering and leveraging of enemy data using network means.

Computer Network Operations (CNO)

One of five core capabilities under IO. The computer network can be leveraged to make the life of friendly parties better while weaponized against your enemies.

Confidentiality

Ensuring that private data stays private.

Control-flow Integrity (CFI)

Protection that monitors a program at runtime and compares its state to a set of precomputed valid states to ensure that control-flow is restricted to valid execution traces.

Cookie

A file stored on an OS but managed by the browser that stores web session data. Originally intended to improve web experiences but can be used maliciously with relative ease.

Counter mode (CTR)

Block cipher mode that uses an arbitrary number called the counter that changes with each block of text encrypted. The counter is encrypted with the cipher and the result XOR'd into ciphertext.

Cracker

Someone who breaks into unauthorized systems.

Cross-site scripting (XSS)

A method of hacking web applications by injecting malicious scripts into client-side code.

Cryptanalysis

The process of understanding cryptographic defenses in order to defeat them.

Cryptographic Message Syntax (CMS)

IETF standard for cryptographically protected messages.

Cryptography

Field centered around encrypting and decrypting information.

Cryptosystem

A suite of cryptographic algorithms needed to provide a specific security functionality. Often times used for key generation, encryption, and decryption.

Cyclic redundancy check (CRC)

A commonly used error-detecting technique.

Dark web

Websites and other services provided by servers that are intentionally hidden from digital means of discovery.

Data Encryption Standard (DES)

Symmetric key encryption method that uses a 56-bit key size and is hence obsolete.

Data loss prevention (DLP)

Strategy and technical measures centered around ensuring that information does not leak outside of an organization. Sometimes called information loss prevention (ILP).

Decryption

Using specific mathematical algorithms to convert secret text back into understandable text. Also referred to as deciphering.

Demilitarized zone (DMZ)

An isolated network sitting between a public network or the Internet and a private network that improves security of the private network. Also known as a perimeter network.

Denial-of-service (DoS)

A cyber attack where the target service is hindered or made unavailable. DDOS is the distributed form of this attack involving multiple attacking sources.

Diffie-Hellman key exchange (DH)

Method by which cryptographic keys can be exchanged over a public channel.

Digest

The resultant compressed string output of a hashing algorithm.

Digital footprint

Data left behind both actively and passively every time someone uses the internet that can potentially be used to trace the user's activities.

Digital forensics

Investigating data, logs, and other host artifacts regarding a cybercrime or attempted cybercrime.

Digital Signature Algorithm (DSA)

FIPS standard for creating and using signatures.

Digital watermarking

Security technique of embedding proof of ownership in a set of electronic information to allow for countermeasures to theft or tampering.

Discretionary Access Control (DAC)

TCSEC defined access control method that allows users to have full control of the objects they create or have been explicitly granted access to by authority. They may share these objects freely with other users.

DNS hijack

When target computers are hindered or redirected to fake or compromised sites via hacked host settings pointing to fraudulent DNS servers and leading to malicious sites.

Dropper

Program written to dodge anti-virus detection, typically by using encryption, and then becoming a vector to transport and install viruses.

Electronic code book mode (ECB)

Simple deterministic block cipher mode where each block of plaintext is encrypted to make a block of ciphertext without use of IV or chaining. Identical plaintexts with identical keys get encrypted to identical ciphertexts and there may be detectible patterns in the ciphertext.

Electronic Warfare (EW)

One of five core capabilities under IO where electromagnetic radiation is tactically denied from enemy use while being used to attack or counterattack the enemy.

Embedsec

Embedded systems security.

Encryption

Mathematical method of converting information into secret code to prevent understanding by unwanted parties. Also called encoding or rarely enciphering.

Encryption key

An input piece to a cipher that makes output of the algorithm unique. Keys can be private or public.

Entropy

A measure of the randomness and uncertainty of the result from a data-generating function.

Error correction codes (ECC)

Mathematical method for maintaining data integrity to a degree by reverting changed bits to their original values.

Error detecting techniques

Mathematical method for maintaining data integrity to a degree by determining when bits deviate from their original configuration.

Executable and Linkable Format (ELF)

A very common standard binary format for operating systems such as Linux.

Exploit

A hack leveraging a specific vulnerability in a system.

Firewall

Protective software that aims to prevent unauthorized access to a system.

Forward Secrecy (FS)

System security design so that if a host entity's private key is compromised, past transactions and communications are still secure.

Fuzzing

An automated software security testing technique that involves providing invalid, unexpected, or random data as inputs to the program being tested.

Gadgets

Slang for machine instruction sequences in memory that a cracker uses to bypass security in an attack. Gadgets typically end in a return and reside in a program or shared library subroutine.

Glitching

Attack on a system performed by first intentionally causing a hardware fault that then enables the bypassing of security features.

Grey hat

A person that walks the line between black hat and white hat.

Guard pages

Unmapped pages placed between all allocations of memory the size of one page or larger. These pages protect exploitation of heap buffer overflows by causing a segmentation fault upon access.

Hacker

A term that become synonymous with cracker, but was originally coined to define an advanced computer technology enthusiast and adherent of programming subculture.

Hardware security module (HSM)

An external removable device that functions like a TPM.

Hash-based message authentication code (HMAC)

Type of MAC that uses a secret shared key in conjunction to the hash function.

Hashing

Mathematically converting strings of varying size into compressed strings of fixed size. While the input and output strings are mapped, by design the original input can't be practically derived by knowing the output string.

HMAC-based One-time Password (HOTP)

Authentication method using a symmetric, one-time generated password.

Honeypot

A vulnerable target intentionally set by cybersecurity in order to trap or study hacker and attacks.

Host intrusion prevention systems (HIPS)

Protective software that can monitor host code execution to flag suspicious behavior and prevent attacks.

Hypertext Transfer Protocol Secure (HTTPS)

A more secure extension of HTTP that uses TLS to encrypt data in transit and authenticate server-client interactions.

Indicators of compromise (IOC)

Forensic data that suggests malicious activity has occurred on a system. Typically log entries or file integrity checks.

Information Operations (IO)

DoD term for the implementation of IW, where IW is the strategy behind the implementation.

Information warfare (IW)

Engagement of protecting friendly battlefield information sources while attacking enemy battlefield information sources.

Inherent risk

Risk before security controls have been applied to the system.

Initialization vector (IV)

String of fixed size that is an input into a cryptographic algorithm. Typically pseudorandom.

Initiative for Open Authentication (OATH)

Open standard centered around strong authentication methods.

Integrity

Ensuring that data is not altered by unintended parties.

Inter-Integrated Circuit (I2C)

A synchronous serial protocol to connect low-speed devices in a master-slave configuration using two wires.

Intrusion prevention system (IPS)

Monitor system and networks for threat actor activity to prevent a breach.

IP Security Protocol (IPSec)

Standard network protocol suite for cryptographically-based security measures provided to the IP datagram layer.

Joint Test Action Group (JTAG)

A common hardware interface that provides direct communication with chips on a board that were originally intended to be tested by the manufacturer.

Keylogger

Software deployed on a target host system to secretly record keystrokes in order to secretly learn information.

Keysteam

Cryptography term for a randomly generated string that is combined with plaintext to produce the ciphertext.

Malware

Malicious software intended on infiltrating/damaging/hindering a system, or accessing unauthorized data.

Mandatory Access Control (MAC)

TCSEC defined access control method that enforces policies where data is strictly inaccessible to users that don't possess the necessary permissions or clearance.

Man-In-The-Middle (MITM)

Attack initiated by hacker intercepting communication or transaction between parties.

Masquerade

A faux program used in spoofing that mimics a legitimate program and then captures the unknowing victim's input.

Master boot record (MBR)

A boot sector at the beginning of a mass storage partition that provides information necessary to boot an operating system.

Merkle tree

Also known as a hash tree, this datastructure has leaves that are hashes of data blocks and non-leaf nodes that are hashes of child nodes. This allows for recursive verification of elements that is also secure.

Military Deception (MILDEC)

One of five core capabilities under Integrated Information Operations (IO) involving intentionally misleading the enemy into making decisions that are strategically detrimental to the enemy.

Multi-factor Authentication (MFA)

Way of securing access to a resource by requiring more than one unique piece of identity verification from a user. If only two ways is known as two-factor authentication (2FA).

Multipartite

Type of virus that comprises of both boot sector and file infections.

National Security Agency (NSA)

United States agency focused on national network and information system security.

Network Access Control (NAC)

Protective set of software that authenticates users, ensures that user host systems meet security criteria, and enforces roles, data access, other policies.

Nonce

An arbitrary number intended to be used only once in a cryptographic operation.

Non-repudiation

Using cryptography to ensure that an unintended party cannot deny that a data transaction occurred and that it was facilitated by the intended parties.

Operations Security (OPSEC)

One of five core capabilities under IO where friendly parties determine if and how the enemy can obtain and leverage critical friendly information especially when multiple pieces of information are aggregated.

Output feedback mode (OFB)

Block cipher mode where you generate keystream blocks, which are XORed with plaintext blocks to get the ciphertext.

Packet sniffer

Also known as a network analyzer. A piece of hardware or software used to monitor network traffic.

Patch

Code that mends or replaces functionality of a deployed codebase. Can be used to eliminate vulnerabilities once they are discovered.

Payload

Code that is intended for execution by virtue of an exploit.

Penetration test

An evaluation of the security of a system conducted by system protectors traversing pathways into the system as a hacker would to gain access. Commonly called a pen test.

Phishing

When an attacker deceives a target into unknowingly giving data or access via forms of communication. Spearphishing is a more targeted form of this attack.

Plaintext

Unencrypted text.

Platform security architecture (PSA)

A security standard developed by Arm to protect embedded devices. It includes hardware, software, design principles, and strategy to secure devices.

Pointer Authentication Code (PAC)

Guard against unexpected changes to pointers in memory that uses the upper bits of a pointer as a cryptographic signature.

Polymorphic

Type of virus that alters itself upon replication in order to stay ahead of anti-virus detection and hence survive the unauthorized replication event.

Position Independent Executables (PIE)

Countermeasure that loads executable binaries at random memory addresses so the kernel can disallow text relocation and thwart return oriented programming attacks.

Potentially unwanted application (PUA)

Software that's not necessarily malicious but is not approved for use on a network and hence their use and distribution on said network need to be controlled. Sometimes referred to as a potentially unwanted program (PUP).

Pretty Good Privacy (PGP)

Software system used for cryptographic privacy and authentication of communicated data.

Principle of least privilege

Security principle that users and software entities should have only the absolutely necessary privileges needed to complete their tasks.

Privacy-Enhanced Mail (PEM)

IETF standardized file format for storing and sending cryptographic keys, certificates, and other data.

Protection rings

Hierarchical domains of varying privilege within a CPU that provide protection and isolation. These rings are hardware or microcode enforced.

Proxy server

Server that sits between a client and server. Can protect server from attackers by masking details or can allow users to hide web activity such as browsing or other requests.

Psychological Operations (PSYOP)

One of five core capabilities under IO that involves attacking enemy values, beliefs, emotions, motives, reasoning, or behavior through psychological means.

Purple team

This is more of a strategy rather than a team that lays out how to get Red and Blue teams to stay closely integrated for maximum response time and security implementation.

Quarantine

Isolating malware or infected files into a safe section of disk so that they can be subsequently removed with reduced risk of accidental execution.

Ransomware

Malicious software that holds the data on a system hostage until released when terms are met.

Recovery point objective (RPO)

Maximum amount of time that can elapse while operational data is being lost before causing detrimental harm to an organization.

Recovery time objective (RTO)

The amount of time an organization has to restore operational data in order to avoid intolerable harm.

Red team

White hats that attack a target system during a simulated cyberattack.

Relocation Read-Only (RELRO)

Security measure that makes some binary sections read-only.

Remediation

The act of detecting, limiting, and or solving an attack or vulnerability.

Remote attestation

Method with which a host authenticates itself to another host over a remote connection.

Residual risk

Risk after security controls have been applied to the system.

Return-oriented programming (ROP)

Exploitation technique that circumvents executable space protection and code signing by using control of the call stack to hijack program flow and execute strategic instructions in memory.

Reverse engineering

Act of looking at software or hardware starting with the finished product and working backward toward its composition, in order to learn about functionality or vulnerabilities.

Risk

Potential for damage or loss of an asset as a result of an attack. Formally defined as the sum of asset, threat, and vulnerability.

Rivest-Shamir-Adleman (RSA)

An old and widely used cryptosystem that generates a public-private key pair with algorithms that use two secret prime numbers and an auxiliary integer value.

Root of Trust (RoT)

The fundamental trusted component in a cryptographic system that gets leveraged to secure subsequent components.

Rootkit

Malware that allows for hidden unauthorized programs or processes to run on a target system that serve to command and control the system.

Salami

Perpetration technique done with multiple small changes that are hard to detect that eventually lead to a potent cumulative effect on the target.

Salt

Unique string that's combined with the input string to a hashing function to insure that two identical input strings will still hash to unique values. Generation and combination of the salt is called salting the hash. A salt that is kept secret is called a pepper.

Scavenging

Information gathering technique employed by attackers where user data that has been marked for deletion but not actually been removed from memory is read.

Script kiddies

Attacker with minimal technical skills that relies on already available scripts to attack a target. Also known as skiddies.

Secure boot

Chain-like sequential verification mechanism for ensuring that code running on a computing device is trusted. Depends on a hardware root of trust, which provides the first link in a chain of trusted components.

Secure file transfer protocol (SFTP)

Technical means of sending files securely over a network.

Secure Sockets Layer (SSL)

Security protocol for Internel point-to-point connections. Client and server authenticate each other when connecting and once authenticated exchange data over a secure channel. TLS has mostly replaced SSL.

Secure/Multipurpose Internal Mail Extensions (S/MIME)

Standard for public key encryption and signing of MIME data.

Security as a Service (SECaaS or SaaS)

Cloud-based method of providing third party cybersecurity services to a customer.

Security posture

Measurement of an organization's cybersecurity power by considering resources, reaction time, staff, and other relevant attributes.

Semantically secure cryptosystem

When only non-sensitive data or metadata can be extracted from ciphertext with any reasonable amount of effort.

Serial Peripheral Interface (SPI)

A synchronous serial communication protocol that provides full–duplex communication using a four-wire bus.

Shadow stack

A second, redundant call stack that protects a procedure's stored return address from exploitation.

Side-channel attack

System attack that leverages deep domain-specific details instead of vulnerabilities.

Signature

A cryptographically computed value derived using a private key that is appended to data allowing the data to be authenticated as being from a specific sender using the sender's public key.

Social engineering

Form of exploitation involving the mental manipulation of people into making targeted actions or revealing targeted information.

Spam

An unsolicited electronic message of any kind. Can be used to perform attacks.

Spoofing

When an attacker deceives a target into unknowingly giving data or access via mimicry of legitimate services.

Spyware

Software that runs on a system and tracks activity and reports it to the threat actor.

SQL injection

Exploit using insufficiently checked form input to execute unauthorized queries against a target database.

Stack canaries

Also known as stack cookies. A mitigation strategy against stack overflow attacks by pushing a randomly generated secret value onto the stack and monitoring changes in its value and position after returning from a function.

Static analysis

Parsing code to make determinations about it without compiling or executing the code. Commonly used to discover nonsecure coding practices and enforce coding standards.

Steganography

Practice of embedding hidden information inside a file. Can be used by malicious parties to communicate secretly.

Stream cipher

Symmetric key cipher that uses plaintext characters one at a time in conjunction with corresponding digit of a keystream to generate a character of ciphertext output at a time.

Symmetric cryptography

Sometimes referred to as private key cryptography. A cryptosystem used a shared key to encrypt and decrypt data. More algorithmically efficient than asymmetric crypto but is requires that the shared key is kept secret and hence is not feasible in situations where that secrecy is hard to establish.

System hardening

A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system.

Threat actor

Cybersecurity term for an individual or group that performs ill-intended action upon a target.

Threat agent

A party that performs malicious activity upon an asset of interest.

Time-based One-time Password Algorithm (TOTP)

Authentication method using a one-time generated string token that is created using the current time and hence can only be cracked in real time.

Token

A physical or digital entity used in two-factor authentication that grants access when possessed.

Transmission security (TRANSEC)

Segment of COMSEC dealing with the security of the transmission mechanism rather than the security of the data itself.

Transport Layer Security (TLS)

Cryptographic protocol for network communication. Encrypts and authenticates the connection. Look at it as a more secure replacement for SSL.

Triple Data Encryption Standard (3DES)

Symmetric key encryption method. Better than DES because it applies DES in triplicate but is still soon to be obsolete.

Trojan

Malware that hides its objective to its environment and users, pretending to be legitimate.

Trust anchor

A public key that is used to verify the authenticity of a signature.

Trusted Computer System Evaluation Criteria (TCSEC)

U.S. DoD standard for evaluating system security.

Trusted Platform Module (TPM)

A special standardized chip on a board that contains a cryptographic processor providing security services and secure memory for storing keys and protected configuration registers.

TrustZone

Arm design approach that aims to increase the security of the system using hardware and software isolation and device root of trust.

Tunnel mode

Sending information over the Internet where both data and the original IP address are encrypted.

Unified threat management (UTM)

Approach where one security solution offers multiple safeguarding functions.

Universal Asynchronous Receiver-Transmitter (UART)

Circuitry for full-duplex serial communication in which the data format and transmission speeds are configurable..

Virtual private network (VPN)

An encrypted internet connection that allows a host device to remotely access a private network as if it was connected internally to the network.

Virus

Malware that can spread from one host to another.

Vishing

Voice phishing. Form of social engineering using a phone to bait a target into doing the attacker's bidding.

Vulnerability

A flaw in software that can potentially be exploited by threat actors. Also known as a bug.

White hat

A person that uses their offensive skills for constructive or protective purposes. Also known as an ethical hacker.

White-box testing

Penetration testing where the tester understands the internal makeup of the system.

Whitelist

Better term is allowlist. Access control mechanism where entities on the list are granted access to whatever is being controlled.

Wi-Fi Protected Access (WPA)

WPA, WPA2, and WPA3 are security certifications for wireless networks.

Wired Equivalent Privacy (WEP)

Wireless network security standard that was replaced by WPA.

Worm

Malware that replicates itself to spread to other computers and perform malicious activity.

Zero–day

Exploit when attackers know about the vulnerability before system protectors do and before mitigations are applied.

Zombie

A single host system in the collective systems that is a botnet.