unbound security

cryptography reimagined

The Cybersecurity Acronym Book

acronym noun

ac·ro·nym | \ a-krə-nim

unbound security

Find Your Acronym

Acronyms
A-B

AES

Advanced Encryption Standard

A symmetrical block cipher algorithm using keys of lengt 128, 192, and 256 bits. It was established by the U.S. National Institute of Standards and Technology (NIST) in 2001 and is considered to be highly secure. AES is used with different modes of operation, the best - AES-GCM and AES-CCM - achieving both privacy and integrity.

AES-NI AES

New Instructions

A set of instructions designed by Intel, but now widely popular, for computing AES in hardware. Hardware with AES-NI can encrypt and decrypt at amazing speed.

AML

Anti-Money Laundering

A set of laws, regulations and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income

API

Application Programming Interface

An application programming interface is a computing interface that defines interactions between multiple software applications or mixed hardware-software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, and so on.

APT

Advanced Persistent Threat

A cyber-attack typically by a very sophisticated attacker (possibly even nation state) that works over a long period of time using advanced techniques to conduct cyber espionage or crime

APWG

Anti-Phishing Working Group

An international consortium that brings together businesses affected by phishing attacks with security companies, law enforcement, government, trade associations, and others.

ASV

Approved Scanning Vendor for PCI

An organization certified by the PCI SSC with a set of security services and tools to conduct external vulnerability scanning services.

ATT&CK

Adversarial Tactics, Techniques and Common Knowledge

A comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.

AV

Antivirus

A computer program used to prevent, detect, and remove malware.

AVIEN

Anti-Virus Information Exchange Network

A group of Antivirus and security specialists who share information regarding AV companies, products, malware and other threats.

BaaS

Blockchain as a Service

Cloud-based solutions that allows company to build, host, and operate their own blockchain apps and related functions on the blockchain, while the service provider maintains the infrastructure and operations.

BAS

Breach and Attack Simulation Tools

A tool that can automatically spot vulnerabilities in an organization's cyber defenses through continuous, automated penetration testing.

BYOD

Bring Your Own Device

An IT policy where employees are allowed to use personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data, hence exposed to risk.

BYOK

Bring your own key

A system that allows customers to choose and import their own encryption key to a cloud application.

Acronyms

C-D

CA

Certificate Authority

An entity that issues digital certificates to certify the ownership of a public key.

CAPI

Crypto API

CAPI is an API included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. CAPI has been replaced by CNG.

CAPTCHA

Completely Automated Public Turing Test to Tell Computers and Humans Apart

A response test used in computing, especially on websites, to confirm that a user is human instead of a bot.

CARO

Computer Antivirus Research Organization

An organization established in 1990 to study malware.

CASB

Cloud Access Security Broker

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies.

CAVP

Cryptographic Algorithm Validation Program

This program provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and individual components. Cryptographic algorithm validation is a necessary precursor to cryptographic module validation.

CBC

Cipher Block Chaining

A popular mode of operation for block cipher encryption using a random initialization vector and a chaining mechanism.

CBC-MAC

Cipher Block Chaining Message Authentication Code

A method for constructing a message authentication code (see MAC) from a block cipher, using the same chaining method as CBC encryption but with different padding methods and without any IV.

CCA

Chosen-Ciphertext Attack

A type of attack on encryption where the attacker is assumed to be able to obtain decryptions of ciphertexts of its choosing. Consider theoretical only for many years, it turned out to be very practical in its incarnation as a "padding oracle attack". By default, encryption schemes deployed should provide security against these attacks.

CCM

Counter with CBC-MAC (mode)

A mode of operation for encryption using a block cipher that provides both privacy and integrity. CCM combines CTR encryption with CBC-MAC and is simple to implement.

CERIAS

Center for Education and Research in Information Assurance and Security

A part of Purdue University dedicated to research and education in information security.

CERT

Computer Emergency Response Team

In this case– an expert group that handles computer security incidents and alerts organizations about them.

CHAP

Challenge-Handshake Authentication Protocol

A protocol for authentication that provides protection against replay attacks through the use of a changing identifier and a variable challenge-value.

CIRT

Computer Incident Response Team

A group that handles events involving computer security and data breaches.

CIS

Center for Internet Security

A 501 nonprofit organization with a mission to “Identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace.”

CISA

Certified Information Systems Auditor

Professionals who monitor, audit, control, and assess information systems.

CISM

Certified Information Systems Security Manager

A certification offered by ISACA which “Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives.”

CISO

Chief Information Security Officer

The CISO is the executive responsible for an organization's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. CISOs are also increasingly in a "coaching role" helping the business manage cyber risk. This is according to Ponemon Institute research.

CISSP

Certified Information Systems Security Professional

The CISSP is a security certification for security analysts, offered by ISC(2). It was designed to indicate a person has learned certain standardized knowledge in cybersecurity.

CKMS

Cryptographic key management system

See Key Management System (KMS).

CLOUD Act

Clarifying Lawful Overseas Use of Data Act

A United States federal law enacted in 2018 that provide trans-border access to communications data of U.S.-based technology companies via warrant or subpoena regardless of whether the data is stored in the U.S. or on foreign soil.

CMAC

Cipher-based Message Authentication Code

A type of CBC-MAC with specific padding and formatting that prevents attacks on naively implemented CBC-MAC. The recommended version of CBC-MAC to be used.

CNAP

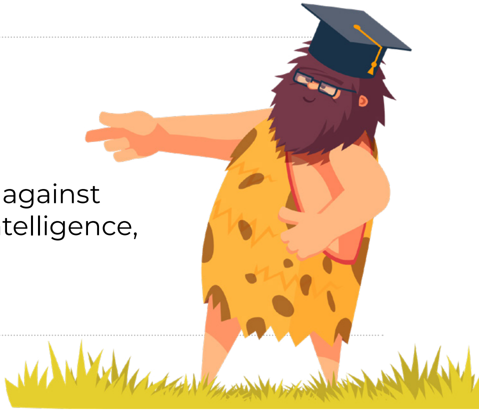
Cybersecurity National Action Plan

A U.S. plan to enhance cybersecurity awareness and protections, protect privacy, maintain public safety, and economic and national security.

CNCI

Comprehensive National Cybersecurity Initiative

A U.S. government initiative designed to establish a front line of defense against network intrusion, defend the U.S. against the threats through counterintelligence, and strengthen the cybersecurity environment.



CND

Computer Network Defense

CND is defined by the U.S. military as defined by the US Department of Defense (DoD) as, “Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.” This style of defense applies to the private sector as well.

CNG

Cryptographic API Next Generation

The next generation of Microsoft's CAPI, with more cryptographic algorithms and functions.

COBIT

Control Objectives for Information and Related Technologies

An IT management including practices, tools and models for risk management and compliance.

CPA

Chosen-Plaintext Attack (not certified public accountant)

A type of attack on encryption where the attacker is assumed to be able to obtain encryptions of plaintexts of its choosing. This is the default for asymmetric encryption, and can be achieved in many real-world settings also for symmetric encryption.

CSA

Cloud Security Alliance

The Cloud Security Alliance is the world's leading organization for defining best practices in cloud cybersecurity. It also provides a cloud security provider certification program, among other things.

CSEC

Cyber Security Education Consortium

The CSEC, also known as the CEC, partners with educators and the broader cybersecurity community to ensure students are prepared to lead and be changemakers in the cybersecurity workforce.

CSO

Chief Security Officer

In some cases, the Chief Security Officer is in charge of an organization's entire security posture or strategy. This includes both physical security and cybersecurity. In other cases, this title belongs to the senior most role in charge of cybersecurity.

CSP

Cloud Service Provider

A third-party company that offers a cloud-based platform for infrastructure, application, storage or other services.

CSSIA

Center for Systems Security and Information Assurance

The CSSIA is a U.S. leader in training cybersecurity educators. It provides these teachers and professors with real-world learning experiences in information assurance and network security.

CTI

Cyber Threat Intelligence

Information about threats and threat actors that helps mitigate harmful events in cyberspace. Sources can include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web.

CTR

Counter (mode)

A popular mode of operation for encrypting with a block cipher using a unique or random initial counter. Counter mode generates a stream for masking the plaintext, where the next keystream block is generated by applying the block cipher to successive values of a “counter”.

CVE

Common Vulnerabilities and Exposures

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

CVSS

Common Vulnerability Scoring System

An industry standard for rating the severity of security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

CYOK

Control Your Own Key (Unbound)

A solution developed by Unbound that allows SaaS and IaaS customers to keep full control of their cryptographic keys, while maintaining full functionality of their applications and services in the cloud.

DAST

Dynamic Application Security Testing

A type of black-box security testing in which tests are performed by attacking an application from the outside. It is a type of application security testing (AST) and is a part of software development.

DDoS

Distributed Denial of Service

A distributed denial-of-service (DDoS) attack attempts to disrupt normal traffic of a targeted server, service or network to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).

DES and 3DES

Data Encryption Standard

DES was the symmetric algorithm of choice standardized by NIST in the 1970s. The key in the original DES was too short and so 3DES was devised that works by applying DES three times. 3DES has been replaced by AES and is used today only for legacy applications.

DH

Diffie-Hellman

A widely used method of key exchange. Devised by Whitfield Diffie and Martin Hellman in 1976, it is still the choice of key exchange today.

DID

Digital Identity Database

A database storing information representing external agents, such as people, organizations, applications, or devices.

DLP

Data Loss Prevention

An information security strategy to protect corporate data. DLP is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users, either inside or outside of an organization.

DNS attack

Domain Name Server

DNS uses the name of a website to redirect traffic to its owned IP address. Amazon.com should take you to Amazon’s website, for example. During this type of attack,which is complex and appears in several ways, cybercriminals can redirect you to another site for their own purposes. This attack takes advantage of the communication back and forth between clients and servers.

DSA

Digital Signing Algorithm

A digital signature scheme developed and standardized by NIST in the 1990s. DSA has been effectively replaced with ECDSA.

DUKPT

Derived Unique Key Per Transaction

DUKPT is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key.

Acronyms

E-F

ECB

Electronic Codebook (mode)

This is the simplest mode of encryption where messages are divided into blocks and encrypted separately. ECB is not secure and should not be used.

ECC

Elliptic Curve Cryptography

Refers to cryptographic schemes that are based on hard problems in elliptic curves.

ECDH

Elliptic Curve Diffie-Hellman

A version of the Diffie-Hellman (DH) key exchange protocol that uses elliptic curves.

ECDSA

Elliptic Curve Digital Signature Algorithm

A variant of the Digital Signature Algorithm (DSA) using elliptic curve cryptography, which is more efficient than the original DSA based on large numbers in finite fields.

EdDSA

Edwards-curve Digital Signature Algorithm

A digital signature scheme based on Schnorr signatures using a special type of Elliptic curve, called a twisted Edwards curve. EdDSA is faster and more robust than ECDSA.

ECIES

Elliptic Curve Integrated Encryption Scheme

A public-key encryption scheme using elliptic curves that provides security against advanced attackers carry out advanced active (chosen-ciphertext) attacks.

EDR

Endpoint Detection & Response

Endpoint Detection & Response solutions are designed to detect and respond to endpoint anomalies. EDR solutions are not designed to replace IDPS solutions or firewalls but extend their functionality by providing in-depth endpoint visibility and analysis. EDR uses different datasets, which facilitates advanced correlations and detection.

EKMS

Enterprise key management system

See Key Management System (KMS).

EV

Extended Validation (used for code signing certificates)

A code signing certificate issued by a public CA, following a rigorous validation of the requesting organization, as well as required proof of security measures to protect the certificate from compromise. EV certificates are required for stronger code signing validation.

FIPS

Federal Information Processing Standards

A set of public standards developed byNIST for use in computer systems by non-military American government agencies and government contractors. FIPS 140-2 (and now 140-3) are standards regulating the use of cryptography modules. Although not required outside of government, FIPS 140-2 (and now 140-3) are considered an important validation of cryptographic libraries and modules for commercial use.

FISMA

Federal Information Security Modernization Act (2014)

Laws that assigns responsibilities within the U.S. federal government for setting and complying with policies to secure agencies' information systems. For example, Department of Homeland Security administers cybersecurity policies and the Office of Management and Budget provides oversight.

FISSEA

Federal Information Systems Security Educators' Association

An organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, and education responsibilities.

FPE

Format Preserving Encryption

An encryption method that maintains the original format of the plaintext - credit card numbers are encrypted to valid random credit card numbers, and so on. Also known as tokenization, and can be used when encrypted data needs to be of a certain format (like in existing databases).

Acronyms

G-H

GCM

Galois Counter Mode

A mode of operation for encryption using a block cipher that provides both privacy and integrity. GCM is extremely efficient and widely used.

GDPR

General Data Protection Regulation

A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). Its impact extended beyond the European borders and became a global baseline for regulations worldwide, such as the California Consumer Privacy Act in California.

GRC

Governance, Risk Management, and Compliance

Three parts of a strategy for managing an organization’s overall governance, enterprise risk management and compliance with regulations. Cybersecurity people, practices and tools play a key part in GRC for many organizations.

HD Wallet

Hierarchical Deterministic Wallet

A digital wallet for cryptocurrencies that automatically generates a hierarchical tree-like structure of private/public addresses (or keys) from a single seed key, providing users increased privacy & security.

HIPAA

Health Insurance Portability and Accountability Act

A United States federal statute to address the flow of healthcare information. Specifically, Title II, known as the Administrative Simplification (AS) provisions, regulates the use and disclosure of protected health information (PHI), and outlined related security standards required to protect the data.

HMAC

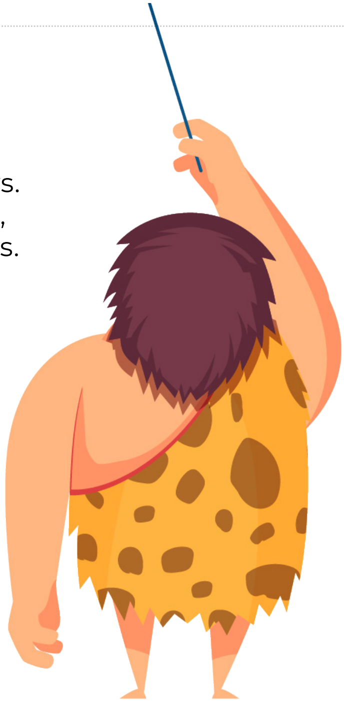
Hash Message Authentication Code

An algorithm for generating message authentication code (MAC) that uses cryptographic hash functions (like SHA-2), to provide authenticity and integrity.

HSM

Hardware Security Module

A specialized physical device built to protect cryptographic keys. HSMs perform cryptographic operations such as key exchange, encryption and decryption internally, and do not reveal the keys.



HTTPS

Secure Hypertext Transfer Protocol

An extension of the Hypertext Transfer Protocol (HTTP) that includes the use of TLS. It is used for secure communication over a computer network by encrypting the information you send from your computer to another website, for example. It is a means of ensuring privacy, security and also a way of authenticating that the site you're on is the one you intended to visit.

HYOK

Hold Your Own Key

A configuration that allows customers to retain full control over access to their data regardless of where it is stored or processed. The customer encrypts before data is sent to the cloud and keeps the key, preventing the cloud provider from decrypting.

Acronyms

I-J

IA

Information Assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

IAM

Identity and access management

A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. This helps organizations maintain "least privileged" or "zero trust" account access, where employees only have access to the minimum amount of data needed for their roles.

IBE

Identity-Based Encryption

A type of public-key encryption in which the public key of a user is some unique information about the identity of the user, like a user's email address, for example.

IDaaS

Identity as a Service

A software as a service offering surrounding identity and access management (IAM) that helps organizations provide secure access through SSO, authentication and access controls.

IDS/IDP

Intrusion Detection/Intrusion Detection and Prevention

Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyze packets as well, but can also stop the packet from being delivered based on what kind of attacks it detects, helping to stop the attack.

IIoT

Industrial Internet of Things

The use of internet of things (IoT) in industrial sectors and applications, such as interconnected sensors, instruments, and other devices, normally focused on data collection, exchange, and analysis of industrial operations.

IPsec

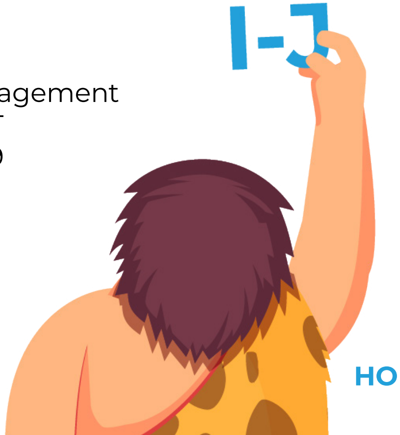
Internet Protocol Security

A secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

ISACA

Information Systems Audit and Control Association

ISACA provides certifications for IT security, audit and risk management professionals. ISACA also maintains the COBIT framework for IT management and governance. ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves professionals in 180 countries.



ISAKMP

Internet Security Association and Key Management Protocol

A protocol for establishing Security Associations and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.

ISAP

Information Security Automation Program

The ISAP is a U.S. government agency initiative to enable automation and standardization of technical security operations. Its standards based design may benefit those in the private sector as well.

(ISC)^2

International Information Systems Security Certification Consortium

A non-profit organization which specializes in training and certification for cybersecurity professionals. Certifications include the CISSP.

ISO

International Organization for Standardization

An organization that develops international standards of many types, including two major information security management standards, ISO 27001 and ISO 27002.

ISSA

Information Systems Security Association

ISSA is a not-for-profit, international organization of information security professionals and practitioners.

ISSO

Information Systems Security Officer

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

ISSPM

Information Systems Security Program Manager

The ISSPM, sometimes called an IT Security Manager, coordinates and executes security policies and controls, as well as assesses vulnerabilities within a company. They are often responsible for data and network security processing, security systems management, and security violation investigation.

IV

Initialization Vector

A random input used in symmetric encryption to ensure that the same value encrypted multiple times, even with the same secret key, will look completely different. For some modes of operation (e.g., CTR), it suffices for the IV to be unique; in others (e.g., CBC) it has to be random.

JCA

Java Cryptography Architecture

JCA is a framework for working with cryptography using the Java programming language. It forms part of the Java security API, and can be used for encryption, key generation and management, secure random-number generation, certificate validation, and so on.

JSM

Java Security Manager

To use Java security to protect a Java application from performing potentially unsafe actions, you can enable a security manager for the JVM in which the application runs. The security manager enforces a security policy, which is a set of permissions (system access privileges) that are assigned to code sources.

Acronyms
K-M

KM

Key Management

Refers to the management of an encryption key lifecycle, including its creation, storage and protection of both existing and expired keys, distribution, and replacement and destruction

KMS

Key Management System

A system for managing encryption keys throughout their entire lifecycle, including backend functionalities for key generation, distribution, and replacement, as well as client functionalities for injecting keys, storing and managing keys on devices.

KYC

Know Your Customer

A regulatory process to verify a customer’s identity before permitting a transaction to take place. KYC is normally a component of a broader AML (Anti-Money Laundering) policy

LMS

Learning Management System

A learning management system is a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, or learning and development programs.

MAC

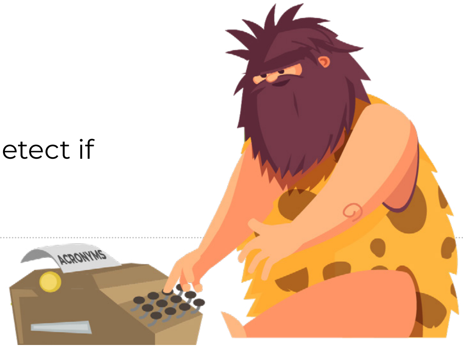
Message Authentication Code

A method of verifying the authenticity and integrity of a message sent using symmetric cryptography.

MDC

Modification Detection Code

MDC is an integrity check for OpenPGP messages which helps detect if messages have been tampered with.



MPC

Multiparty Computation

A cryptographic protocol that protects individual parties' privacy within a distributed computation function.

MS-ISAC

Multi-State Information Sharing and Analysis Center

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

MSSP

Managed Security Services Provider

Provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

Acronyms

N-O

NCS

National Cryptologic School

A school within the National Security Agency. The NCS provides the NSA workforce and its Intelligence Community and Department of Defense partners highly-specialized cryptologic training, as well as courses in leadership, professional development, and over 40 foreign languages.

NCSA

National Cyber Security Alliance

A non-profit working with the Department of Homeland Security, private sector sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education.

NCSAM

National Cyber Security Awareness Month

NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. It occurs each year in October. The security awareness month started with a joint effort by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance.

NCSD

National Cyber Security Division

A division of the Office of Cyber Security & Communications with the mission of collaborating with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructures.

NICCS

National Initiative for Cybersecurity Careers and Studies

An online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the United States.

NICE

National Initiative for Cybersecurity Education

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

NISPOM

National Industrial Security Program Operating Manual

The National Industrial Security Program Operating Manual establishes the standard procedures and requirements for all government contractors, with regards to classified information. It covers the entire field of government-industrial security related matters.

NIST

National Institute of Standards and Technology

In cybersecurity circles, NIST is extremely well known for the NIST Cybersecurity Framework, as well the NIST Risk Management Framework (RMF), NIST 800-53 control guidance, NIST Digital Identity Guidelines and others. The overall NIST mission is to “promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.” NIST is part of the U.S. Department of Commerce.

NYCRR

NYDFS Cybersecurity Regulation (NYDFS is New York State Department of Financial Services)

A regulation implemented by the New York State Department of Financial Services (DFS) to require financial services firms doing business in New York State to have a full security risk assessment and plan.

OPSEC

Operational Security

OPSEC is a term derived from the U.S. military and is an analytical process used to deny an adversary information that could compromise the secrecy and/or the operational security of a mission. Performing OPSEC related techniques can play a significant role in both offensive and defensive cybersecurity strategies.

OSINT

Open Source Intelligence

OSINT is information drawn from publicly available data that is collected, exploited, and reported to address a specific intelligence requirement. In the intelligence community, the term “open” refers to overt, publicly available sources (as opposed to covert or clandestine sources).

OTP

One-Time Password

A method of authentication where users obtain a one-time passwords (typically 6 digits) that can be used to authenticate once only. OTPs are generated using hardware tokens, mobile apps or sent by SMS, with different levels of security for each method.

Acronyms P-R

PCI-DSS

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

PII

Personal Identifying Information

Infromation that identifies specific people and so must be protected according to regulations.

PIN

Personal Identification Number

A secure alphanumeric or numeric code that validates your identity with various types of networks and systems, such as computer networks, credit/debit cards, and mobile phones.

PKCS

Public-Key Cryptography Standards

A group of public-key cryptography standards developed by RSA Laboratories to promote the use of cryptography techniques. PKCS11 is a widely used library (API) for carrying out cryptographic operations.

PKI

Public Key Infrastructure

An umbrella term for everything used to establish and manage public key encryption, including any roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and public key encryption - one of the most common forms of internet encryption.

PQC

Post-Quantum Cryptography

Refers to a family of cryptographic algorithms that remain secure even if the attacker has a fully functioning quantum computer.

RBAC

Role-based access control

A method of restricting network access where only necessary permissions are granted to individual users needing to perform certain operations based on their specific roles.

RoT

Root of Trust

The foundational source that establishes the trust within a cryptographic system for use in the rest of the system to ensure security.

RSA

Rivest–Shamir–Adleman

One of the oldest and most established asymmetric public-private key cryptographic algorithm used for encryption and digital signing.

RSA-OAEP

RSA Optimal Asymmetric Encryption Padding

A specific way of encrypting with RSA that specifies how plaintext messages are padded. RSA-OAEP provides strong protection against advanced active attacker (CCA attacks) and should be the default method used when encrypting with RSA.

RSA-PSS

RSA Probabilistic Signature Scheme

A signature scheme based on the RSA cryptography system that uses a type of random padding, used to verify the authenticity of digital messages or documents.

Acronyms

S-T

SaaS

Security as a Service, or Software as a Service

A third-party company that uses a Software as a Service model to handle and manage security services on a subscription basis.

SANS

System Administration, Networking, and Security Institute

A private company that specializes in information security training and security certification.

SDK

Software Development Kit

A collection of software development tools that allows developers to create programs in a certain programming language. The kit can include but not limited to libraries, relevant documentation, code samples, processes and guides.

SDLC

Software Development Life Cycle

A process used by the software industry to design, develop, test, and deploy software securely.

SGX

Intel Software Guard Extensions

A set of security-related instruction codes that increases the security of application code and data by running them inside firmware-protected enclaves. Applications run inside SGX can keep all data encrypted, even while in memory.

SHA

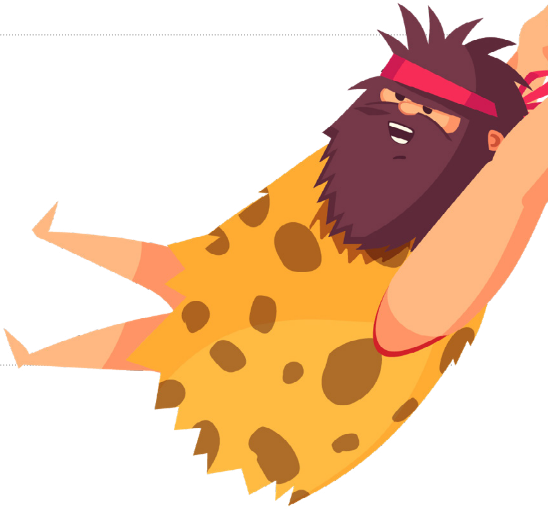
Secure Hash Algorithms

A series of families of cryptographic functions standardized by NIST, used in many cryptographic contexts like digital signatures, message authentication, password protection, and more. SHA-1 is no longer secure and may not be used. The SHA-2 and SHA-3 families are both considered to be secure.

SIEM

Security Information and Event Management

Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual sources.



SOAR

Security, Orchestration, Automation and Response

SOAR is a stack of compatible software programs that enables an organization to collect data about security threats and respond to security events without human assistance.

SOC

Security Operations Center

A central location or team within an organization that is responsible for monitoring, assessing and defending security issues.

SSH

Secure Shell

A cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution.

SSL

Secure Sockets Layer

The predecessor of TLS.

SSO

Single Sign-On

A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials.

TLS

Transport Layer Security

A set of cryptographic protocols designed to provide communications security between a client and a server over a computer network. It is the successor of Secure Sockets Layer (SSL).

TPM

Trusted Platform Module

A computer chip (microcontroller) designed to provide hardware-based, security-related functions by storing artifacts used to authenticate the platform such as passwords, certificates, or encryption keys.

TTP

Tactics, Techniques, and Procedures

The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Acronyms

U-X

UBA / UEBA

User Behavior Analytics

UBA tracks a system's users, looking for unusual patterns of behavior. In cybersecurity, the process helps detect insider threats, and other targeted attacks including financial fraud. User behavior analytics solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns. This guides efforts to correct unintentional behavior that puts business at risk and risky and intentional deceit.

vHSM

Virtual Hardware Security Module

A layer of abstraction providing a unified API for cryptography consumption, irrespective of where the actual cryptographic key resides. Keys can be used in physical HSMs, cloud KMSs, and Unbound's MPC key store, in a unified way.

VPN

Virtual Private Network

By connecting through a VPN, all the data you send and receive travels through an encrypted "tunnel" so that no one can see what you are transmitting or decipher it if they do get a hold of it. VPNs also allow you to hide your physical location and IP address, often displaying the IP address of the VPN service, instead.

WAF

Web Application Firewall

WAF is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service.

XSS

Cross-site Scripting

Cross-site scripting is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users.

unbound security

cryptography reimagined

In a world moving towards everything encrypted, signed, and authenticated — secure and operationally efficient cryptographic infrastructure is an absolute must for enterprises. Our vision at Unbound is to be the global cryptographic orchestration platform of choice for the enterprise. By leveraging the latest advancements in multi-party computations, our platform is the industry choice to secure the world's largest banks and Fortune 500 companies. With a headquarters in New York, and an EMEA office in Tel Aviv, Unbound provides the cryptographic orchestration platform that enables enterprises worldwide to easily secure and manage all their information and digital assets.

unboundsecurity.com | contact@unboundsecurity.com

HOME →