Cyber security glossary

Biometrics

In the context of logging in to software, or authorising actions within software, biometrics are inputs based on "something you are". The most common example is fingerprints, and you may also use 3D facial recognition to unlock your smartphone. In the future we expect voice recognition to become an additional factor in helping prove your identity.

Botnet

A network of bots, i.e. a collection of computers being used, in this context, to attack other networks and software. A lot of attack methods by bad actors depends on quantity of computing power and range of different locations or network addresses. Criminals commonly hijack otherwise normal computing resources so they can use them as part of a botnet to attack systems or spread malware. Even if your systems are not the ultimate target, they could unwittingly become resources actively used by a criminal enterprise.

Brute force

If a bad actor wants to gain entry to systems they're not permitted to access, brute force applies to the practice of simply trying lots of password guesses if encrypted data has been stolen. With software and large amounts of cheap computing power to automate this, hundreds of thousands of combinations can be tried very rapidly. This is one of the reasons why password strength is so important, as well as avoiding password reuse.

Certificate

In software and networking a certificate is a document exchanged between software systems to ensure they are talking to the right places. Signing of certificates in a chain up to global certificate authorities provides a system of authority so that it's not just a matter of self-declaration.

Certificate pinning

A practice in software systems that connects a certificate (an assertion of digital identity between communicating parties) with particular hardware. This makes it much harder to **spoof** connections, and provides good confidence within an application that the data that flows back and forth across the public internet is securely limited to trusted parties.

Cloud

Cynics in the software and IT worlds offer an obligatory definition that "the cloud means someone else's computer"! When software runs or stores data "in the cloud" this means that the servers are within data centres and hosting providers following a particular shared service model, pioneered by Amazon Web Services, but now also available from other big names like Google, Microsoft, IBM, and Oracle. The most significant differences to older ways of operating is that users of software are less likely to install and run software on their local PCs, but commonly depend on applications accessed through a browser, and data created by and stored for the application resides in network-accessible data centres rather than either the local PC or servers physically located with the provider of the application (such as the bank).

CoP

Confirmation of payee. A new requirement within European payment systems to prevent people accidentally sending money to the wrong account. This is significant for anti-fraud because criminals often try to trick people in to sending them money by impersonating legitimate companies.

Cracking

The word "hacking" originally meant experimental and enthusiastic use of technology, without negative connotations. Therefore the term cracking is a more correct, but less common description, for breaking or compromising computer systems. This is often malicious, although legitimate purposes exist such as security testing of software – with the permission of the owners of course. Another common use of the term is in gaining access to secure systems by guessing passwords or decrypting data.

DDoS

Stands for **Distributed Denial of Service.** A denial of service (DoS) attack aims to overwhelm a computer system with meaningless or malicious requests so that it stops working properly. This can be used purely to cause stoppages and therefore a method of attacking an organisation, or can be used as a cover or facilitator for other attacks. A distributed DoS means that the attack is staged from many computers and locations, e.g. with a botnet. This can be extremely hard to protect against and comprises a major category of the "arms race" of the cybersecurity industry defending against evolving attack techniques.

Encryption

Data that is encrypted is locked in a digital form that can be transmitted and/or stored in otherwise untrusted networks and computers, keeping the data secure and only accessible by the intended parties. A simple example is putting an access password on a single Microsoft Word document: the data could be stored or sent anywhere but in theory only the people who know the password could view it. Another example is iCloud storage of data, which is encrypted both **in transit** and **at rest** – although Apple can access that data, not only you! There's a lot of sophisticated technology in this critical area of cybersecurity, and it's evolving fast.

EUD

End user device: the computer, tablet, smartphone, or other hardware (for example a voice interface like Amazon Echo) through which customers interact with digital services. Robust cybersecurity concepts need to take account of the fact that these devices may have their own security weaknesses, or simply get lost or stolen.

Firewall

IT hardware devices and/or software which control access into and out of a network. Complex rules of permission can be applied based on origin and destination of network traffic, and usage patterns. Setting up and administering firewalls and other elements of network security is an important and active role in cybersecurity for IT operations. Individuals make use of firewalls, although likely without being aware of it, in their home broadband modem/routers, and in their mobile and PC operating systems. If you use a **VPN** for your work, this is part of a system of granting only authorised users access to certain resources based on network access controls.

Fuzzing

A software testing practice which, in the wrong hands, can become a method of attack: a large number of chaotic inputs are fed into a software system as fast as possible, discovering bugs and vulnerabilities faster and in different ways compared to logical path-based human testing.

HTTPS

The internet runs on the hypertext transfer protocol (HTTP) and the secure version of this standard is called HTTPS, an innovation that sparked a revolution in ecommerce and banking as it enables confidential financial data such as credit card numbers to be exchanged online with confidence. You may notice that some websites are marked with an warning or open padlock icon meaning outdated HTTP technology is being used, instead of the correct HTTPS approach, which is often denoted in browsers with a green locked padlock – and you can see the URL (web address) starts with "https://". HTTPS ensures data exchanged between your browser and servers is encrypted and cannot be spied on if intercepted. The current technology used is called **TLS** (Transport Layer Security), which has superseded a perhaps more familiar initialism – **SSL** (Secure Sockets Layer).

Hacker

An informal term referring to anyone gaining access to and exploiting technology in ways that are unintended by the designers and owners. The most important thing to bear in mind is that a malicious hacker does not have to be targeting you, to be a threat to you or those around you. Good cybersecurity habits are precautionary and try to add layers of difficulty for anyone looking to compromise or damage your privacy and the digital systems in your life.

Originally, hacker just meant someone with an experimental attitude towards software and IT, hence the term "hackathon" can apply to any kind of technology event, not just ones relating to cybersecurity.

IDS

Intrusion detection system: just as a motion-sensitive burglar alarm will deter intruders and alert people about a break-in, computer systems should have defence systems which monitor for suspicious activity and report it to administrators.

IoT

The Internet of Things – referring to modern gadgetry which has internet connectivity built-in. A common joke in technology circles is that "The S in IoT stands for security..." – in other words IoT devices are notorious for lacking responsible cybersecurity standards and being hard to secure. Both businesses and households should be extremely wary of allowing untrusted devices to connect to their networks and to have access to private data.

Keylogger

A malicious tool which records all keystrokes (or on-screen typing) in a computer operating system: since most passwords are typed in, this represents a major security problem. Keylogging can be done by malicious software or be used by bad actors in the form of hardware such as a USB stick plugged into a PC.

Malware

Software with a malicious purpose or effects, including varieties such as viruses, worms, keyloggers, ransomware, botnet applications and more. Any computer (or tablet or smartphone) using any operating system can suffer from malware. Many examples of malware are both difficult to detect and hard to remove.

Multifactor authentication

The requirement to log in (or authorise an action in software) using more than just one factor. A password is one factor: if it's compromised then, ideally, this should not be enough to let an attacker gain access. Additional authentication factors include one-time passcodes (**OTPs**, via an app or over SMS), biometrics, and hardware security keys. Everybody should make use of multifactor authentication wherever it is available (and this includes daily logins such as Google, Facebook, Amazon, and Twitter as well as more obvious candidates where it's likely mandatory like banking).

NCSC

The UK National Cyber Security Centre. This government body provides excellent educational and best practice resources to both individuals and organisations. https://www.ncsc.gov.uk/

OWASP

The Open Source Foundation for Application Security: based in the USA, this foundation publishes research and best practices around cybersecurity and is a recommended authoritative resource for those interested in digging deeper into this area. https://owasp.org/

Patching

Patching is the updating of installed software, to add new features, correct bugs, and more importantly to guard against newly discovered vulnerabilities. All software should be kept as up-to-date as possible because of the ever-changing nature of cybersecurity threats: the longer systems are unpatched, the more likely they are to be vulnerable to exploitation.

PCI DSS

Payment Card Industry Data Security Standard is a set of rules and operational standards followed by any organisation which handles credit and debit card data. For professionals in cybersecurity, the precautionary principles in PCI DSS provide a good reference for more general security policies and training aimed at safeguarding data and controlling access to IT systems.

Pentest

Short for penetration test: carried out in permitted, controlled scenarios, cybersecurity professionals simulate a variety of attack routes to validate the security of a specific piece of software or more general business system (or even location), and discover and disclose vulnerabilities, which can then be fixed.

Phishing

The practice of sending emails or other messages with links which appear to lead to legitimate websites or applications and typically try to trick the user into logging in, thinking they are visiting their bank (etc) – while in fact stealing their login credentials. Phishing messages can also be used to deliver malware by tricking the user into downloading files or installing malicious applications. Variants include "vishing", stealing credentials by impersonating an institution over a voice call'; "smishing", phishing over SMS; "spear phishing", in which a particular key individual is targeted rather than a mass indiscriminate malware campaign; and "whaling" which is an attack specifically focused on senior or critical staff members in an organisation e.g. a Chief Financial Officer.)

Ransomware

Malicious software which encrypts your data and asks for a ransom to unlock it. The risk of data loss should be addressed with secure backup solutions, and individuals and organisations should strictly refuse to pay ransoms as this merely rewards the criminals and incentivises them to attack others.

SCA

Strong Customer Authentication – a set of requirements which is coming into effect for all UK and EU banks and payment forms as part of **PSD2** (the second Payment Services Directive), effectively standardising and strengthening the login security requirements for consumer payment actions. Examples include the requirement to confirm a bank transfer via a one time passcode sent via SMS, or to enter a bank card PIN after a certain number of contactless payments.

Security theatre

A derogatory term for practices aimed at giving the impression of strict controls, but which lack sufficient substance versus actual threats, and therefore risk giving a false sense of security or simply diverting resources away from other necessary precautions.

Social engineering

A broad term covering activities of malicious actors beyond IT and software, but possibly related to cybersecurity, such as tricking people into giving up confidential information or credentials, or even manipulating people into acting on behalf of an attacker.

Vulnerability

A potential security weakness in software or IT systems. No systems are perfect, so both attackers and defenders of computer systems are constantly in a race to discover and defend against new potential weaknesses. Vulnerabilities should be fixed or mitigated wherever possible, even if there is no evidence they are currently being exploited.

Zero day

A vulnerability which is as-yet unknown to the developers and administrators of the target systems: because they don't know, they have had zero days to analyse and fix it… meanwhile, malicious actors who have discovered it and kept it secret, might exploit this for days, weeks, or years until they are found out!

CREALOGIX

These definitions are provided by CREALOGIX – digital engagement software provider to the world's leading private banks and wealth management firms. Crealogix provide the software for JM Finn's award-winning client portal and are therefore a paid supplier. https://crealogix.com/uk/