Glossary

Published by

DeNardis, Laura, et al.
Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties.
Mattering Press, 2022.
Project MUSE. https://dx.doi.org/10.1353/book.121036.

GLOSSARY

Build: In software development, the term may refer either to the process by which source code is converted into a stand-alone form that can be run on a computer, or to the form itself. One of the most important steps of a software build is the compilation process, where source code files are converted into executable code. See also https://www.techopedia.com/definition/3759/build

Chat-over-email: An approach to designing instant messaging applications using email transfer protocols, such as SMTP and IMAP, often with an implementation of PGP on top, to offer end-to-end encryption. The most well-known projects of a chat-over-email app are Delta Chat, COI, Spike and MailTime.

Client-server: Computer networking model where the machines that communicate are not equivalent: one is a server, permanently on and waiting for connections, the others are clients, who connect when they have something to ask.

Client-side implementation: 'Client-side' means that the action takes place on the user's (the client's) computer, as opposed to 'server-side' which means that the action takes place on a web server.

Constant bit rate encoding: In telecommunications, the term indicates a situation in which the rate at which data is consumed by a codec (a device that encodes or decodes a data stream) is constant.

(Cryptographic) deniability: Encryption technique that allows 'denying' the existence of an encrypted file or message, in the sense that an adversary is unable to prove that the associated data exists.

Double Ratchet: **Key management** algorithm developed by the creators of Signal (Trevor Perrin and Moxie Marlinspike) in 2013, which manages the ongoing renewal and maintenance of short-lived session keys after a first key exchange. It is a 'double' ratchet because it combines a cryptographic component with a key derivation function.

End-to-end encryption: Only the communicating parties can read the message, which is encrypted in transit *and* on users' terminals.

Ephemeral key exchange: See **key exchange**. With ephemeral methods, a different key is used for each connection.

Ephemeral (or disappearing) messaging: Mobile-to-mobile transmission of multimedia messages that automatically disappear from the recipient's screen after the message has been viewed. See also https://searchcio.techtarget.com/definition/ephemeral-messaging

Forking: Forking a piece of software during its development process means that developers take a copy of its source code and start independent development on it, creating a separate piece of software. An act of forking is generally not merely a technical issue, but involves a (governance/organisational) change, possibly conflictual, in the developer community.

Forward/future secrecy: A cryptographic feature of the last generation of instant messaging apps, ensuring that a user's **session keys** will not be compromised even if the private key of the server *is* compromised. In particular, it is meant to protect past sessions against future compromises of secret keys or passwords.

F/OSS (Free and Open-Source Software): Software that anyone is freely licensed to use, copy, study and change in any way, and whose source code is openly shared so that people are encouraged to voluntarily improve the design of the software.

Gossiping/gossip protocol: A process of peer-to-peer communication between computers which ensures that data is disseminated to all members of a group; in the absence of a central registry, the only way to spread data is to rely on each member to pass it along to their neighbours. Thus, gossip protocols are based on the way epidemics spread, and are also called epidemic protocols.

Group messaging: Holding a conversation via a messaging application between two or more people.

Hash: A function that converts an input of letters and numbers into an encrypted output of a fixed length.

Header (email): A code snippet in an HTML email, which precedes the body of the email and contains information about the sender, recipient, the email's route to get to the inbox and a number of authentication details. See https://sendpulse.com/support/glossary/email-header

Interoperability: The ability of programs (messaging apps or any kind of software) to exchange data and communicate smoothly with each other.

IP address: A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address has the two main functions of acting as a host or network interface identifier and providing location addressing.

IPv6: The most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Key exchange (v. key discovery): In **public key cryptography**, key exchange is the method by which cryptographic keys are exchanged between two parties; key verification is any way that lets you match a key to a person, making sure that it is indeed that person who uses the key (see e.g. https://ssd.eff.org/en/glossary/key-verification)

Key management: All operations related to the management of cryptographic keys in an encrypted system, including their generation, exchange, storage, use, destruction and replacement.

Latency: In engineering, latency is the time interval between a stimulation and a response, or, from a more general point of view, a time delay between the cause and the effect of some change in the system being observed.

MAC (media access control) address: A unique identifier assigned to a network interface controller (a hardware component connecting a computer to a network) to use as an address in a communication.

Mail User Agent: a computer application that allows a user to send and retrieve email – colloquially called an email program.

Man-in-the-middle attack: In computer security, MITM is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Mesh networks: A network model in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data.

Metadata: Succinctly defined as 'information about information', the data providing information about one or more aspects of the data itself. Metadata is used to summarise basic information about data, which can make tracking and working with specific data easier.

Mixnet (mix network): Routing protocols that create hard-to-trace communications by using a chain of servers known as *mixes,* which take in messages from multiple senders, shuffle them and send them back out in random order to the next destination. *De facto,* this breaks the link between the source of the request and the destination, making it harder for third parties to trace end-to-end communications.

Network-layer protection: The network interface layer is the physical interface between the host system and the network hardware, which defines how data packets should be formatted for transmission and routings. This layer has several security vulnerabilities unique to it, needing specific protection responses.

Non-repudiation: Assurance that someone cannot deny the validity of a particular operation; in cryptography, the concept refers to a service that is able to provide proof of the origin of data as well as their integrity.

OMEMO: stands for 'OMEMO Multi-End Message and Object Encryption', an encryption protocol developed to solve specific limitations and problems that existed both in OpenPGP and in OTR. It provides future and forward secrecy and deniability and gives the possibility of message synchronisation and offline delivery.

Open standards and protocols: non-proprietary, open source, well-documented protocols that have been standardised by relevant institutions and are available to be reused and shared by the wider developer community. Open standards are usually believed to ensure better **interoperability** and improve further collaboration between projects based on open standards.

Out of band (data): The data transferred through a stream that is independent from the main data stream ('in band'). An out-of-band data mechanism provides a conceptually independent channel, which allows any data sent via that mechanism to be kept separate from in-band data.

OTR (Off-the-Record Messaging): A cryptographic protocol that provides encryption for instant messaging conversations. In addition to authentication and encryption, OTR provides **forward secrecy**. Version 4 of the protocol (OTRv4) is currently being designed by a team led by Sofía Celi and reviewed by Nik Unger and Ian Goldberg.

Passive attack: An attack on a network in which the attacker does not – as it cannot – interact with any of the parties involved, thus attempting to break the system solely based upon observed data.

Pastebin: A type of online content hosting service where users can store plain text.

Patent disclosure: A public claim of data about an invention; more generally, any part of a patenting process in which data regarding an invention is disclosed to the public. A patent disclosure is used by individuals such as inventors and attorneys, seeking to prepare a patent application. A patent disclosure provides information on the invention and its originality/uniqueness. See also https://www.upcounsel.com/patent-disclosure.

Peer-to-peer (p2p): Computer networking model where two machines or two humans communicate directly to exchange messages, files, or other data.

Primitive (cryptographic): Well-established, low-level cryptographic algorithms, frequently used as a basis to build cryptographic protocols.

Protocol: Referring to the Internet, this word indicates a set of criteria and procedures that provide the conceptual model of the network of networks, as well as the set of specifications that explain how data should be regrouped into packets, addressed, transmitted, routed and received.

Public-key (or asymmetric) cryptography: Cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys known only to the owner.

Public-key infrastructure: The set of roles, policies and procedures needed to create, manage, distribute and use public-key cryptography.

Pull request: In software development, a pull request is a method of submitting contributions to an open development project, which occurs when a developer (or an expert user) asks for changes committed to an external repository to be considered for inclusion in a project's main repository.

PGP (Pretty Good Privacy): An encryption programme that provides privacy and authentication for online communications. PGP is used for signing, encrypting and decrypting texts, e-mails, files, directories and disk partitions, as well as increasing the security of e-mail communications.

Security vs Usability: A widely discussed hypothesis according to which it is extremely hard to design truly secure communication systems and still keep them user-friendly.

Server Name Indication (SNI): An extension to the Transport Layer Security (TLS) computer networking protocol by which a client indicates which hostname it is attempting to connect to at the start of the handshaking process.

Server-side archives: When an e-mail program uses this option, the mail server archives to the mail server itself, or to another server designated as the archive server. This is opposed to client-based archiving, when the individual workstations process mail file archiving. Mail is archived either to the mail server, a designated server, or to its local workstations.

Server-side encryption: Data is encrypted on the server (of the company providing the messaging services).

Social graph: A graph (representation of a structure) representing social relations between a set of entities, e.g. individuals.

TLS (Transport Layer Security): Cryptographic protocol designed to provide communications security over a computer network. TLS aims primarily to provide data integrity and privacy between two or more communicating computer applications.

Two-factor authentication: In an Internet-based service, this is a method of confirming users' claimed identities by using a combination of *two* among these different factors: (1) something they know, (2) something they have, or (3) something they are.

XMPP: Extensible Messaging and Presence Protocol, originally named Jabber and created by the eponymous community, is a communication protocol based on XML (Extensible Markup Language). Unlike most instant messaging protocols, XMPP is defined in an open standard and uses an open systems approach for its development and application. https://xmpp.org/

UI/UX design: User experience design is the process of influencing user behaviour by acting upon some features of a product, such as usability and accessibility. User interface design is the design of the graphical layout of an application – all the items the user interacts with. The two processes are generally considered as part of a whole.

Untrusted server problem: Being able to provide security even in the event of a 'worst case scenario' server breach, where an attacker has full control of server resources, including the ability to read and modify back-end application code and data and remain undetected for at least some time.

Upcycling (of protocols): An approach to designing instant messaging applications by reusing existing open standards and protocols, instead of creating new ones. This approach is said to increase interoperability and help engage bigger communities of developers, as it is based on open standards or well documented protocols.

Usable security: The interdisciplinary research field that addresses the usability of secure communication technologies.

MATTERING PRESS TITLES

Engineering the Climate: Science, Politics and Visions of Control
JULIA SCHUBERT

With Microbes
EDITED BY CHARLOTTE BRIVES, MATTHÄUS REST AND SALLA SARIOLA

Environmental Alterities
EDITED BY CRISTÓBAL BONELLI AND ANTONIA WALFORD

Sensing In/Security
EDITED BY NINA KLIMBURG-WITJES, NIKOLAUS POECHHACKER & GEOFFREY C. BOWKER

Energy Worlds in Experiment
EDITED BY JAMES MAGUIRE, LAURA WATTS AND BRITT ROSS WINTHEREIK

Boxes: A Field Guide
EDITED BY SUSANNE BAUER, MARTINA SCHLÜNDER AND MARIA RENTETZI

An Anthropology of Common Ground: Awkward Encounters in Heritage Work
NATHALIA SOFIE BRICHET

Ghost-Managed Medicine: Big Pharma's Invisible Hands
SERGIO SISMONDO

Inventing the Social
EDITED BY NOORTJE MARRES, MICHAEL GUGGENHEIM, ALEX WILKIE

Energy Babble
ANDY BOUCHER, BILL GAVER, TOBIE KERRIDGE, MIKE MICHAEL, LILIANA OVALLE,
MATTHEW PLUMMER-FERNANDEZ AND ALEX WILKIE

The Ethnographic Case
EDITED BY EMILY YATES-DOERR AND CHRISTINE LABUSKI

On Curiosity: The Art of Market Seduction
FRANCK COCHOY

Practising Comparison: Logics, Relations, Collaborations
EDITED BY JOE DEVILLE, MICHAEL GUGGENHEIM AND ZUZANA HRDLIČKOVÁ

Modes of Knowing: Resources from the Baroque
EDITED BY JOHN LAW AND EVELYN RUPPERT

Imagining Classrooms: Stories of Children, Teaching and Ethnography
VICKI MACKNIGHT