Encryption

An Internet Society Public Policy Briefing

11 August 2022

Introduction

Encryption is all around us. It is used to protect data sent from all types of devices across all sorts of networks. In addition to protecting the electronic keyrings that store passwords for computers and spreadsheets that are "for your eyes only", encryption is used to protect the information that is being exchanged every time a person uses an ATM, conducts a purchase from a smartphone, makes a call from a mobile phone, or presses a key fob to unlock a car. It is a versatile technology, increasingly pervasive in our daily lives, and critical to the security of much of what we do.

Encryption, the process of scrambling or enciphering data so it can be read-only by someone with the means to return it to its original state, is commonly used to protect both data stored on computer systems and data transmitted via computer networks, including the Internet. For data communicated over a network, modern encryption scrambles data using a secret value or key known only by the recipient and the sender. For stored data, the key is typically encrypted using a PIN or password known only to the device owner.

Encryption and related techniques are also used to build increased security for financial transactions and to protect the private communications of end-users. Examples include establishing whether data has been tampered with (data integrity), increasing users' confidence that they are communicating with the intended receivers (authentication), and forming part of the protocols that provide evidence that messages were sent and received (non-repudiation).

Key Considerations

In practice, encryption takes the following broad forms:

- **Symmetric encryption** uses an identical key to encrypt and decrypt the message. Both the sender and the receiver have access to the same key. While fast and efficient for computers, symmetric encryption must ensure that the key is reliably delivered to the recipient and does not fall into the wrong hands.

- **Asymmetric encryption**, also known as public-key encryption, is a one-way form of encryption. Keys come in pairs, and information encrypted with the public key can only be decrypted with the corresponding private key. The recipient publicly publishes a key for the sender to encrypt their data. The recipient then uses a private key to decrypt the data. It is similar to a locked mailbox in which mail can be pushed through a slot for delivery but retrieved only by the owner with a key. Public-key encryption is more secure than symmetric encryption because the key doesn´t need to be transferred.

- **End-to-end (E2E) encryption** is a form of encryption in which only the sender and intended recipient can read the message. The most important aspect of end-to-end encryption is that no third party, even the party providing the communication service, has knowledge of the encryption key. Examples of end-to-end encryption protocols include Pretty Good Privacy (PGP) and Off-the-Record Messaging (OTR). Examples of end-to-end encryption communication services include Apple's iMessage, Signal, ProtonMail, WhatsApp and Threema. The Electronic Frontier Foundation has published a Surveillance Self Defense[1] guide that provides information and toolkits on the features of various services and devices.

- **Data-at-rest encryption** is any form of encryption that protects data physically stored in a digital form (e.g., on computers, storage disks, mobile devices, or Internet of Things).

In practice, encryption is applied in a layered approach. For example, a user encrypts his or her email using PGP or Secure/Multipurpose Internet Mail Extensions (S/MIME), and the email provider (e.g., Gmail) encrypts the transmission of the email using HTTPS.

It is important to note that encryption does not necessarily render all communications data unreadable. For example, communications metadata—including sender and recipient identifiers, message length, location, date and time — can be exposed in clear text.

Challenges

The widespread availability of encryption, as well as its versatile nature and use by different actors, presents a number of challenges.

- **Freedom of speech, anonymity, and abuse.** Encryption technologies facilitate anonymous communication, a potential lifeline for citizens and activists under oppressive regimes and individuals in vulnerable communities, such as victims of domestic abuse, those in witness protection programs, and undercover police officers.

[1] https://ssd.eff.org/en

The same technology, however, also can help bad actors hide activities and communications by using anonymity tools for cyberbullyi ng and other forms of online abuse.

The Internet Society acknowledges the legitimate objective of nation-states to protect their citizens but cautions against attempts to regulate technology in order to hinder criminals from communicating confidentially. This approach runs the risk of making it impossible for law-abiding citizens to protect the confidentiality of their data and communications and putting in jeopardy their rights to privacy, freedom of expression, and opinion. As described in our Collaborative Security report[2], the overall objective of security should be to foster confidence on the Internet and ensure the continued success of the Internet as a driver for technical innovation, and economic and social benefit.

- **The security–privacy conundrum.** Policy debates about encryption frequently present the issue as security versus privacy, a matter of balancing the responsibility of governments to protect their citizens versus the rights of citizens to protect their privacy from government, commercial, or criminal intrusion. The Internet Society contends that security and privacy are not necessarily irreconcilable concepts. On the contrary, they can be mutually reinforcing user trust stems from a sense of both privacy and security. For example, trust that a message is secure (will only be read by its intended recipient) helps a variety of Internet services, most notably e-commerce, to flourish.

- **Encryption backdoors.** This refers to the idea that a tool can help an authorized third-party gain access to and decrypt encrypted data without access to keys. But such backdoors also would allow covert access to content. The technical consensus[3] is that introducing backdoors by any of the currently proposed techniques puts legitimate users at risk and is unlikely to prevent criminals from communicating clandestinely. Bad actors will likely find alternative means of communicating, while average users may not have the same tools. This could both leave criminal communications immune from observation and leave user communications vulnerable to observation and interception by governments or bad actors, who have discovered how to exploit the backdoors.

[2] http://www.internetsociety.org/collaborativesecurity.

[3] Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, IAB Statement on Internet Confidentiality, W3C TAG Finding: End-to-End Encryption and the Web, W3C TAG Finding: Securing the Web, https://www.m3aawg.org/news/keys-under-doormats-authors-receive-m3aawg-jd-falk-award-for-clarifying-insecurity-of.

- **Tamper-resistant technology.** In the context of encryption, tamper-resistant technology is designed to make it difficult for attackers to modify devices, applications, or data, and to make any tampering evident. Used in conjunction with encryption, antitampering measures can help prevent (1) entry to a device after repeated login attempts; and (2) the installation of encryption backdoors, rootkits (malicious code designed to access different areas of a computer without authorization), and other malicious software. In recent years, there has been a trend towards greater use of tamper-resistant technology and mechanisms that automatically erase data under certain conditions (e.g., after 10 failed attempts to correctly enter a password). While tamper-resistant technology helps protect the integrity of technology, it may also present difficulties for law enforcement attempting to gain access to the communications and data of suspects.[4]

Guiding Principles

The Internet Society offers the following guiding policy principles:

- **Confidentiality and anonymity**. To support the unhindered expression of human rights, including privacy and freedom of expression, individuals should be able to communicate confidentially and anonymously on the Internet.

- **Data security**. Just as individuals have the right to protect their offline assets and property, they should have the right to use encryption and other tools to protect their data, digital assets, and online activities. We encourage the open development and wide availability of data-security technologies.

- **Trust.** User trust is critical to the Internet's continued growth and evolution and increasing numbers of users are realizing the value of using secure and privacy-respecting applications and services. We encourage the provision of reliable mechanisms for authentication, data confidentiality, and data integrity as vital technical building blocks for trusted products and services. We also believe legal frameworks should support individuals' human rights, including the right to privacy.

- **Encryption.** Encryption should be the norm for all Internet traffic. Designers and developers of digital products and services are strongly encouraged to ensure that users' information, whether stored or communicated, is encrypted by default. Where possible, end-to-end encryption should be made available.

[4] https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

- **Tamper-resistant technology.** Tamper-resistant technology should continue to be developed and implemented in support of encryption. Governments should not mandate the design of vulnerabilities into tools technologies or services. Likewise, governments should not require that tools, technologies, or services be designed or developed to allow third-party access to the content of encrypted data.

- **Responsible disclosure of vulnerabilities.** Governments should support the work of security researchers and others in identifying and responsibly disclosing security and privacy vulnerabilities and should avoid creating or stimulating a market for "zero-day" vulnerabilities.

- **Deployment.** Increased deployment of security mechanisms, such as encryption, will result in challenges in network management design, development, management, and usability. Network management, intrusion detection, and spam prevention will face new functional requirements, and economic and policy challenges should be expected.

- **Multistakeholder solutions.** Criminals can communicate confidentially and anonymously. Successfully confronting the repercussions of this requires the concerted action of multiple stakeholders. The Internet Society reaffirms its commitment to facilitating the engagement of all stakeholders and to playing an active and technically informed role in the development of solutions.

Convening Global Stakeholders

In 2020 the Internet Society was proud to join Global Partners Digital and the Center for Democracy and Technology as a founder member of the Global Encryption Coalition, which has now risen to over 300 organizational and individual members, and which hosted the inaugural Global Encryption Day on 21st October 2021.

The Internet Society signed the "Secure the Internet" petition,[5] affirming its support for the petition's principles, namely that governments should not do the following:

- Ban or otherwise limit user access to encryption in any form or otherwise prohibit the implementation or use of encryption by grade or type.

- Mandate the design or implementation of backdoors or vulnerabilities into tools, technologies, or services.

[5] https://www.securetheinternet.org/

- Require that tools, technologies, or services be designed or developed to allow for third-party access to unencrypted data or encryption keys.

- Seek to weaken or undermine encryption standards or intentionally influence the establishment of encryption standards except to promote a higher level of information security.

- Mandate insecure encryption algorithms, standards, tools, or technologies.

- By private or public agreement, compel or pressure an entity to engage in activity that is inconsistent with the above tenets.

The Internet Society continues to lend its voice to open letters and stakeholder coalitions in support of strong reliable encryption. You will find an up-to-date archive of such statements here: https://www.internetsociety.org/open-letters/

Additional Resources

The Internet Society's fact sheets and briefing papers related to this issue are freely available on the Internet Society website, and many can be found via our encryption resources page: https://www.internetsociety.org/issues/encryption/resources/

The Internet Society's encryption related news releases and media coverage can be found on our newsroom page: https://www.internetsociety.org/newsroom/?tx_category=encryption

The Internet Society's blog posts on encryption can be found on our blogposts page: https://www.internetsociety.org/blog/?tx_category=encryption