Encryption

An Internet Society Public Policy Briefing

03 June 2016

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 key-rings 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.

Electronic 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 secret value typically is known only by the data 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 the evidence that messages were sent and received (nonrepudiation).

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.

Encryption technologies enable Internet users to protect the confidentiality of their data and communications from unwanted observation and intrusion. Encryption is also a technical foundation for trust on the Internet. It promotes freedom of expression, commerce, privacy, user trust, and helps protect data from bad actors. For these reasons, the Internet Society believes that encryption should be the norm for Internet traffic and data storage.

Because bad actors can use encryption to hide their activities or hijack users' data (e.g., via ransomware[1]), members of both government security agencies and the law enforcement community have expressed concern about the negative impact encryption could have on their ability to protect citizens and enforce the law.

The Internet Society recognizes the concerns of law enforcement and remains firm in its conviction that encryption is an important technical solution that all Internet users—individuals, governments, businesses, and other communities—should use to protect their communications and data. We believe that legal and technical attempts to limit the use of encryption, well-intentioned or not, will negatively impact the security of law-abiding citizens.

- **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 needn't be transferred.

- **End-to-end encryption** is any 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 include the protocols Pretty Good Privacy (PGP) and Off-the-Record Messaging (OTR). Examples of end-to-end encryption communication services include Apple's iMessage ,Telegram, and Threema. The Electronic Frontier Foundation has published a secure messaging scorecard[1] that provides information on the features of various services.

- **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, and data used for law enforcement—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. The same technology, however, also can help bad actors hide activities and communications by using anonymity tools for cyberbullying 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 very real risk of making it impossible for law-abiding citizens to protect the

1 See https://www.eff.org/secure-messaging-scorecard.

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 in the Internet and ensure the continued success of the Internet as a driver for economic and social innovation.

- **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 intrusions. 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.

- **Tamper-resistant technology.** Related to encryption, tamper-resistant technology is designed to make it difficult for attackers to modify technology, 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 bad actors pursuant to a judicial order[4].

2 See http://www.internetsociety.org/collaborativesecurity.
3 See 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, M3AAWG blog post: MAAWG Endorses "Keys Under Doormats" End-to-End Encryption Recommendations, and WITSA press release: Global ICT Industry Opposes Backdoor Decryption.
4 This issue is at the heart of a recent case in the US District Court for the Central District of California involving the US Federal Bureau of Investigation and Apple.

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. Working towards this is an important addition to ongoing efforts by the technical community to address pervasive monitoring. Designers and developers of digital products and services are strongly encouraged to ensure that users' data, whether stored or communicated, are encrypted by default. Where possible, end-to-end encryption solutions should be made available. In addition, network and service operators are encouraged to deploy encryption where it is not yet deployed, and firewall policy administrators are urged to permit encrypted traffic.

- **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. Governments should also support the work of security researchers and others in identifying and responsibly disclosing security and privacy vulnerabilities in technology.

- **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.

In addition, the Internet Society has signed the "Secure the Internet" petition[5] to show 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.
- 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.

Additional Resources

The Internet Society has published a number of papers and additional content related to this issue. These are available for free access on the Internet Society website and many can be found from our main encryption page at https://www.internetsociety.org/encryption

Internet Society news releases

- Internet Society responds to reports of the U.S. Government's Circumvention of Encryption Technology, https://www.internetsociety.org/news/internet-society-responds-reports-us-government's-circumvention-encryption-technology
- Internet Society Commends Internet Architecture Board Recommendation on Encryption-by-Default for the Internet, https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default
- Internet Society submission to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression and Opinion regarding the use of encryption and anonymity in digital communications, http://www.internetsociety.org/doc/internet-society-submission-un-special-rapporteur-protection-and-promotion-right-freedom

5 See https://www.securetheinternet.org/.

Blog posts

- Freedom of Speech: Rethinking the Role of Encryption, https://www.internetsociety.org/blog/2013/05/freedom-speech-rethinking-role-encryption

- Encryption Backdoors Decrease Trust In The Internet, https://www.internetsociety.org/blog/tech-matters/2015/05/encryption-backdoors-decrease-trust-internet

- Strong Support From The UN Special Rapporteur David Kaye For Anonymity And Encryption, http://www.internetsociety.org/blog/public-policy/2015/06/strong-support-un-special-rapporteur-david-kaye-anonymity-and-encryption

- No keys under the doormat please, https://www.internetsociety.org/blog/public-policy-tech-matters/2015/08/no-keys-under-doormat-please

- The Fundamental Tension Between Safety And Privacy (And The UK's Proposed Encryption Ban), https://www.internetsociety.org/blog/public-policy/2015/01/fundamental-tension-between-safety-and-privacy-and-uks-proposed

- Internet Society Supports the Let's Encrypt Initiative to Increase End-to-End Encryption, https://www.internetsociety.org/blog/tech-matters/2015/10/isoc-supports-lets-encrypt-initiative-increase-end-end-encryption

- Imagine an encrypted world! A workshop at IGF, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/11/imagine-encrypted-world-workshop-igf-2015

- Encryption and law enforcement: aiming for trust, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/12/encryption-and-law-enforcement-aiming-trust

- Let's Encrypt Enters Public Beta to Increase Encryption on the Internet, https://www.internetsociety.org/blog/tech-matters/2015/12/lets-encrypt-enters-public-beta-increase-encryption-internet

- Internet Society signs "Secure the Internet" Online Petition, http://www.internetsociety.org/blog/tech-matters/2016/02/internet-society-signs-secure-internet-online-petition

- Encryption Backdoors Come In All Guises - Reacting to Apple's Customer Letter, https://www.internetsociety.org/blog/public-policy/2016/02/encryption-backdoors-come-all-guises-reacting-apples-customer-letter

Workshop papers and reports

- Barriers to Deployment: Probing the Potential Differences in Developed and Developing Infrastructure, https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_27.pdf