ISOC Armenia chapter, as a member of the Global encryption coalition, organized **Global Encryption Day** workshop

October 6, 2023

REPORT

Objectives

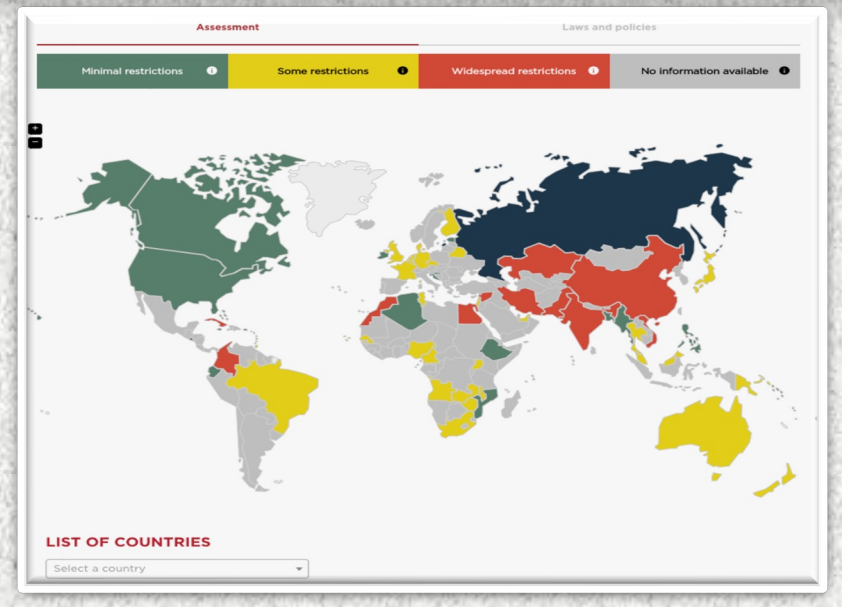
The ISOC Armenia chapter is an active member of the Global Encryption Coalition, strongly promoting robust encryption practices.

We acknowledge that encryption should be a central and actively discussed topic in all of our events concerning internet security and safety.

Topics and speakers

Securing Digital Communication and Privacy

Igor Mkrtumyan,
ISOC Armenia President



In the presentation of Mr. Mkrtumyan, it was stated that the encryption is essential for protecting our communications, data, and financial transactions.

Types of encryptions were numbered, including:

- Symmetric encryption: Uses the same key for both encryption and decryption.
- Asymmetric encryption: Uses two different keys: a public key and a private key.
- End-to-end encryption (E2EE): Data is encrypted at the sender's end and decrypted at the recipient's end.

Benefits of encryption were emphasized. Among them:

- Privacy: Encryption protects our privacy by making it difficult for unauthorized people to access our sensitive information.
- Security: Encryption helps to protect our devices and data from hacking and other cyberattacks.
- Freedom of expression: Encryption allows us to communicate freely and express ourselves without fear of being censored or monitored.

Special attention was paid to the threats to encryption:

- Government surveillance: Some governments are trying to weaken encryption so that they can more easily monitor their citizens.
- Technological advances: As technology advances, it becomes easier for attackers to break encryption algorithms.
- Weak passwords and security practices: Many people use weak passwords and security practices, which makes it easier for attackers to gain access to their encrypted data.

End-to-end encryption of different messengers were analyzed.

Laws on encryption of different countries were analyzed, among them the Law of the Republic of Armenia on Electronic Communications**.** Some articles of the law cause concern among the Armenia IT community. They are the following:

Law of the Republic of Armenia on Electronic Communications

Article 49. Confidentiality of customer information

1. Every operator and service provider shall be obliged to treat and keep as confidential information regarding the type, location, purpose, destination, quantity, and technical conditions of services used by its customers.
2. An operator or service provider shall be entitled to disclose such information:
   (1) in cases and in the manner provided for by law, in connection with surveillance, inquest, or criminal prosecution with regard to a criminal offense or threat to national security.
   (2) upon the written consent of the customer.
   (3) where the disclosure is necessary in defense of the operator or service provider (proceedings are pending against that operator or service provider). The customer may request that such disclosure be made on a confidential basis at an in-camera proceeding.
3. An operator or service provider shall not be liable for any damage caused as a result of disclosure of information made pursuant to part 2 of this Article.

Article 50. Interception, recording, or disclosure of messages

1. A person other than a party to a message transmitted by any electronic communications means may intercept, record, or disclose the content of such message only upon the written consent of the parties to the message or upon a court order in cases and in the manner provided for by law.

2. In addition to the provisions of part 1 of this Article, operators of public or private electronic communications networks and providers of public or private electronic services as well as their employees or representatives may intercept or redirect messages or signals, without disclosing them, where such interception or redirection of signals is conditioned by the exercise of their official duties.

3. In cases and in the manner provided for by law, all operators and service providers shall be obliged to provide access to law enforcement and national security personnel to any communications equipment, facilities, switches, routers, or other similar equipment, including wiretapping devices.

Certainly, in various countries, there exist diverse legal frameworks regarding encryption, and sometimes these laws, rather than enhancing people's security, can inadvertently lead to the loss of sensitive information.

The different legal approaches and regulations can create unintended consequences that compromise data security and privacy.

End-to-end encryption of famous messengers were analyzed.

A question was asked to the participants “What can we do to protect encryption?” The responses included:

- Support strong encryption laws.
- Use E2EE services.
- Use strong passwords and security practices.

At the end it was underlined that encryption is essential for protecting our privacy and security online. It was stated that we all need to do our part to protect encryption so that we can continue to communicate freely and express ourselves without fear of being monitored or censored.

Encryption and Business

Safeguarding Information in the Digital Age

Encryption and Business

Areg Shmavonyan,
InfoTec Cybersecurity LLC

Types of Encryption

- Encryption at rest: Protects stored data
- Encryption in transit: Secures data during transmission
- Examples: SSL/TLS, VPN, SSH

The Importance of HTTPS

- HTTPS: Hypertext Transfer Protocol Secure
- Encrypts communication between browser and website
- Protects against data interception and tampering
- Provides authentication and data integrity

Dangers of Public WiFi

- Risk of unauthorized access
- Data interception and snooping
- Potential for malware and hacking
- Use VPN and avoid sensitive transactions

Encryption for Storage Devices

- Flash drives, hard drives, phones, and laptops
- Encrypts data to prevent unauthorized access
- Examples: BitLocker, FileVault, VeraCrypt

Everyday Encryption Uses

- **Device Protection**: Use BitLocker (Windows) or FileVault (Mac) before selling or traveling with devices.
- **Secure File Sharing**: Send sensitive data using password-protected zip tools like WinZip or 7-Zip.
- **Unreadable Data**: Encrypted files display as scrambled content, ensuring privacy.

Encryption for Emails

- Secure communication via encrypted emails
- Protects sensitive information
- Prevents unauthorized interception
- Examples: PGP, S/MIME

Practical Email Encryption Steps

- Enable Encryption: Use built-in features in platforms like Outlook and Gmail.
- Train staff to spot encrypted emails, often marked with a lock symbol.
- Ensure Secure Domain: TLS indicates a secure domain.
- Regularly refresh software and encryption tools.

Benefits of Encryption in Business

- Enhances customer trust and confidence
- Mitigates financial losses from data breaches
- Supports compliance with data protection regulations
- Protects intellectual property
- Educate: Teach staff to identify secure vs. harmful emails.

Encryption in cloud

Sergey Abrahamyan,
PhD, professor, AUA.

The art and science of protecting information by encoding it in a code or cipher that only the intended recipient can read and understand is known as cryptography. This tradition has a long history and is still essential to many aspects of modern life, including preserving computer passwords, encrypting sensitive information on bank cards and facilitating secure online transactions. Cryptography has always been crucial in preserving the secrecy and accuracy of data, and it is still developing to meet the security demands of the modern digital era.

A Brief History of Cryptography was presented.
Cryptography in cloud computing was analyzed. Some obvious drawbacks of cloud computing were mentioned. Among them is the possibility that client data can be read by:
1. Malicious hackers
2. Storage owners
Homomorphic Encryption was described starting from the early history. Two types of encryption were highlighted:
- Symmetric Encryption, where encryption and decryption use the same key.
- Asymmetric Encryption, where encryption uses a public key and decryption uses the secret key.
The first and most popular asymmetric encryption, RSA, was explained.
Homomorphic Encryption (Rivest-Adleman-Dertouzos'78) and bootstrapping method were presented.

Photo-report

Sum up

A discussion on encryption challenges in Armenia took place, accompanied by the following recommendations:
Keep the global encryption map updated at gp-digital.org/world-map-of-encryption.

In the event that government requirement for obtaining encryption keys becomes unavoidable, mandate that responsible government personnel hold certifications in cybersecurity and encryption.

Information regarding the event was posted on ISOC Armenia chapter's websites and Facebook pages.

Isocchapter.am

https://chronicle.isocchapter.am/

https://www.facebook.com/isocarmeniachapter

https://www.facebook.com/ArmenianInternetSociety