Encryption: A broken promise?

Have you ever observed a small padlock symbol in your browser when you access websites to conduct financial transactions or access your corporate office mail? Have you also seen this padlock symbol in your contact information on some private messenger platforms?

In Human Computer Interaction domain, the padlock symbol informs us that the site or concerned communication medium is 'encrypted'. This implies that data on your site or concerned communication media is unintelligible for everyone except the sender, receiver and the party offering encryption. In case of end to end encryption, the data is unintelligible for the party offering encryption as well. For example, HTTPS is used to provide encryption over sensitive applications on the Internet whereas some popular message applications are based on The Signal Protocol.

Encryption facilitates confidentiality of communication between sender and receiver. It builds trust between communicators. Trust is the basis of all our financial transactions and regular interactions. Thus, encryption plays a critical role in facilitating global trade and communication over the Internet. Unfortunately, this confidentiality can be used by certain players to violate the law, carry out nefarious activities and antagonise certain law enforcement agencies.

As per Thomas Reid's 'Essays on Intellectual Powers of Man' published in 1785,the strength of any chain lies in its weakest link. Accordingly, the strength of any padlock or associated encryption mechanism depends on its ability to make data unintelligible for third parties.

This ability can be weakened by following threats

a. Engineering means i.e. coming up with an accurate guess on the nature of the data by analysis and modern tools via persistent trials and errors. e.g. Use of quantum computing or client side media scanning.

b. Legislative means i.e. coming up with new laws to make data intelligible for law enforcement agencies e.g. Investigatory Powers Act (UK;2016),Assistance and Access Act(Australia;2018)

c. Legal means i.e. using existing laws to make data intelligible for law enforcement agencies e.g. FBI VS Apple Inc

d. Tangential means i.e. any means that can indirectly compromise the unintelligibility of data e.g. content filtering mechanisms that can make encryption untenable e.g. India

As Internet expands to encompass all aspects of our daily life via technologies like IoT and Extended Reality, the unintelligibility of our data is a critical for safeguarding the privacy and security of its users. Governments and law enforcement agencies across the globe are calling for adoption of one or more of the above means to stop perpetuation of online crimes by identifying the perpetrators. But encryption advocates strongly feel that adoption of any of the above means can compromise the efficacy of encryption as a whole. Afterall, backdoors or ghost protocols created for good actors(e.g. law enforcement agencies)can also be misused by bad actors. In some cases, the 'good' actors in a particular country can also be viewed as 'rogue' by other countries or cause driven organisations.

Is encryption a promise meant to be broken? Who is a better guardian of trust in online community- the benevolent technology players or the omniscient, law abiding state? At ISOC

India Mumbai Chapter, we propose a multi-stakeholder approach that prioritize end user interests over sovereign or business interests. Mandating laws to break encryption is an easy way out and something that we wouldn't recommend as a solution to solve all online woes of the society. Community transformation via education, awareness building and improving the overall consciousness of community is more a sustainable solution and we would prefer to work on it.