Encrypt All The Things: A Digital Rights Campaign

Encrypt All The Things is the campaign to promote the Data Security Action Plan. The Data Security Action Plan consists of seven security-enhancing steps designed to ensure a minimum layer of data protection on private networks and communication channels. The seven steps of the Data Security Action Plan address network traffic, data at rest, credentials and authentication techniques, system vulnerabilities, security algorithms, use of client-to-client encryption, and consumer education.

In the wake of the continued disclosures regarding government surveillance, the majority of the reform conversation has revolved around the need for increased transparency of government requests for data. However, many of the disclosures highlight the ease by which unauthorized actors can access large amounts of personal information without any judicial process or oversight. It is now time to expand the public discourse beyond transparency to include a conversation about how to properly secure data on privacy networks.

The implementation text following each item in the Data Security Action Plan is meant to provide additional, supplemental information and resources, but is not part of the Data Security Action Plan.

Data Security Action Plan and Implementation Text

1. Implement strict encryption measures on all network traffic

Transport layer security, or TLS, is a means to encrypting web traffic and authenticating websites to prevent so-called "man in the middle" attacks. When a server communicates with a browser using encryption it becomes very difficult for an outside party to access the information that is passing over the internet. Strict transport security layer protocols cannot be downgraded to remove the encrypted layer. Current best practice is to maintain strict transport layer security with perfect forward secrecy on all traffic, including internal traffic and traffic the server introduces to the user.

2. Execute verifiable practices to effectively secure user data stored at rest

User data collected and stored by any entity, including information from or about individuals, should be robustly protected. The current primary method of protection is through an encryption regime for all stored data, although other methods may be possible to reach the same result. Any method employed should be measurable in order to continually test the security of the information. Existing data protection compliance regimes may provide guidance on security measures for data.

3. Maintain the security of credentials, and provide robust authentication safeguards

Breaches of user data in online services have had a broad impact on the privacy and security of users. Because many individuals still use easy-to-guess passwords or share passwords across multiple online accounts, these data breaches can be especially devastating to users. User credentials should never be stored or sent in plain text, but instead stored in a secure manner, for example, through hashing and salting using slow algorithms. The salting process will ensure that should there be a data breach, passwords cannot be easily recovered. Two-factor authentication can help preserve the integrity of user accounts, but must be voluntary and individuals who wish to maintain their anonymity should be able to do so.

4. Initiate a notification and patching system to promptly address known, exploitable vulnerabilities

All vendors should have a patching regime to keep servers up to date with security patches. Patching regimes for client-side applications should be implemented properly as to not introduce new vulnerabilities to the users. Users should always have an option to make updating a manual process, subject to explicit consent. Updates that result in greater collection of user information should never be pushed through without clear and express notification and consent. Companies should be transparent about vulnerabilities to the extent that it will allow users to minimize exposure and risk.

5. Use algorithms that follow security best practices

Weak or insecure algorithms and implementations of algorithms can be exploited by bad actors to access otherwise protected information. In order to ensure that companies follow security best practices in protecting user communications and data, they should disable the use of insecure algorithms and publicize which algorithms they use to ensure thorough vetting by the security community.

6. Enable or support use of client-to-client encryption

Services that support the use of client-to-client encryption give individuals greater control to protect the security of communications from unintended recipients. Through the use of open protocols, not only can the security of the protocol be verified, but client-to-client secure communications can be built on top of those protocols.

7. Provide user education tools on the importance of digital security hygiene

Protecting individual data and communications is not enough if the users don't understand the risks they face, the rights they enjoy, and the different security options available to them. User education tools should empower individuals toward these goals.

Contact

To publicly support the Data Security Action Plan or to provide comments or suggestions for the implementation text, please send an email to DSAP@accessnow.org, or call +1 (888) 414 0100

Access is an international human rights organization that defends and extends the digital rights of users at risk around the world.