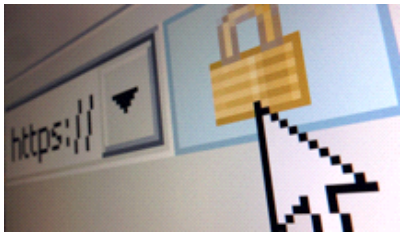
Western fears of encryption lack substance

Tuesday, December 22 2015

In formal comments to the UK Parliament yesterday, Apple pushed back against the Draft Investigatory Powers Bill, which would require the company to provide the government with access to its users' communications. In the wake of the terrorist attacks in Paris, the political debate on law enforcement 'going dark' due to encryption has resurfaced again in the United States and United Kingdom. However, governments have yet to demonstrate evidence of a loss of security capability because of encryption.



A lock icon, signifying an encrypted Internet connection (Reuters/Mal Langsdon)

What next

The demand of mandating access to communications will encourage other governments to seek similar capabilities. This will add cost and complexity to engineered technical solutions, and introduce new vulnerabilities. If law enforcement needs access to encrypted communications content, investment in capabilities to attack endpoints (laptops, mobile phones) is an alternative solution. Such a capability would raise demand for increased cooperation between cybersecurity providers and government.

Analysis

Encryption refers to the process used to protect data so only parties with a decryption key can read it. It is one of the key technologies used to provide security against cyber threats.

Defining the debate

From a technical viewpoint, there are two different types of encryption: encryption of data at rest (stored data) and data in motion (communication). Both types of encryption are widely used today and are cornerstones in the assurance of confidentiality and integrity of data.

Data at rest

Encrypting data at rest -- for example, the data on a smartphone hard drive -- is a first line of defence against anyone extracting data from storage. It renders the stealing of devices less attractive. Many businesses hold sensitive, personally identifiable customer data, the protection of which is often strengthened by storing it in an encrypted format.

Data in motion

Encrypting data in motion can be thought of as providing a tunnel from one device to another, through which to send data across the internet securely. The state of the art of this technology is called end-to-end encryption: only the parties communicating with one another have access to the content of the communication.

Another technical feature protecting the long-term confidentiality of communications is called 'perfect forward secrecy'. This relies on the encryption keys for each session being discarded and new keys generated.

The technical argument

Impact

- The 'going dark' debate may be being used to distract from security agencies' existing surveillance capabilities.
- The debate's outcome could have a severe negative effect on consumer trust in internet-based businesses.
- Businesses will see opportunities in relocation to jurisdictions with robust laws that do not weaken cryptographic systems.

Cryptographers argue against providing the government with the set of keys to decrypt any piece of communication because doing so requires trusting a third party and losing the feature of perfect forward secrecy.

New vulnerabilities

Designing such a large system is in itself a complex undertaking. Its implementation would also likely contain weaknesses attackers could exploit. A compromise of such law enforcement decryption keys, by criminals or hostile states, would make all communications available to the attackers.

Slippery slope?

Furthermore, any technological solution that would allow interception and decryption of communications would be in demand by many governments. If one law enforcement agency has access to encryption keys, other law enforcement agencies are likely to want the same access.

For businesses, this raises the challenge of how to implement globally functioning communication services without compromising the confidentiality of their customers' communications to a foreign government.

The political debate

The technical difficulty of implementing such systems raises the question of why FBI Director James Comey in the United States and UK Prime Minister David Cameron express fears of 'going dark', or demand access to all types of encrypted data (see UNITED STATES: Paris attacks reopen encryption debate - November 30, 2015).

Following the revelations of former NSA contractor Edward Snowden, companies have implemented strong encryption technologies into their products. The security agencies claim this rendered interception for accessing communications content less effective ('going dark').

Data-rich environment

However, there is reason to challenge this claim.

There is a vast amount of data about individuals that is not protected by encryption.

The total amount, the depth, and the breadth of information about different areas of a person's life that are affected by internet-based technologies (banking, shopping, leisure, etc) is growing. Much of the data people generate is stored unencrypted in the cloud, accessible to the cloud service provider.

Security agencies already tap into a vast amount of unencrypted data

Furthermore, many internet-based services do not hide the fact that communication between two endpoints has taken place, thereby generating metadata disclosing intimate details of people's activities.

This metadata, generated even in the case of encrypted content, has become more insightful than the communications content.

However, intelligence agencies are worried that they are losing access to content that they have been used to since the era of telephone intercepts. Similar worries existed in the transition to mobile phone intercepts. In that case, the FBI was successful in lobbying for a bill (CALEA), mandating access to customer traffic (which every carrier has to provide today).

The analogy, however, is flawed in a data-rich environment where much more information can be collected than previously.

No evidence

Furthermore, security services have yet to present evidence as to the extent to which their investigations are prevented by the adoption of encryption technologies.

In the Paris attacks, intelligence agencies have presented no evidence publicly that they were hindered by encryption. The attack was planned and executed by an individual known to authorities, who had (unsuccessfully) tried an attack earlier in 2015, and publicised it in the Islamic State group magazine (Dabiq). Publicly available intelligence had pointed to the risks of such an attack, even naming the individual. The group also seemed to mostly communicate in person, aiming to evade authorities' surveillance of technology (see EU: Security agency is unlikely despite terror risks - December 21, 2015).

Rather than encryption being the challenge, the security agencies use the encryption debate to legitimise their existing capabilities. The Snowden revelations have shown that some capabilities are on a shaky legal basis (very broad interpretations of a current legal regime): the new legal regimes are trying to create a sound legal basis.

High costs

The costs of legally mandating businesses to provide only services accessible to law enforcement are large. Providing internet-based services relies on customer trust -- a quality that is faster lost than earned. Barring an international adoption of the same legislation, service providers are likely to move to more privacy-sensitive jurisdictions.

The futility of mandated access is exacerbated by the availability of open-source implementations of strong cryptographic algorithms. While a country could mandate access to domestic service providers' products, it would be impossible to deny criminals the adoption of freely available secure messaging platforms.

Mandating access to communications content may prove an ineffective solution

Alternative to encryption access

There is an alternative to weakening encryption: attacking the endpoints (phones, laptops). To build that capability, governments would need to invest in upskilling and retraining police forces for internet-based investigations, as they are competing with intelligence agencies and commercial cybersecurity providers for the same talent. In the United Kingdom, the new intelligence unit focusing on the criminal use of the 'dark web' may represent a step in this direction (see UNITED KINGDOM: New security strategy has cyber focus - December 14, 2015).