Cryptography

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

Do you know your rights in the UAE? Can you imagine paying a huge fine for swearing or using the middle finger emoji in a text message? In 2015 the UAE introduced cybercrime and hate speech laws, resulting in newspaper headlines such as *Man Gets 500,000 AED Fine Over Text Messages.* As of 2017 you can relax, because if you are amongst the one billion people who use WhatsApp, you may have noticed that the app now has end-to-end encryption. The latest version of WhatsApp with a 256-bit encryption feature means that only the sender and the recipient can read the messages, and the high level of secure encryption technology makes it impossible for even the producers of WhatsApp to access messages. This is not a popular development for authorities in the UAE, where voice calling on WhatsApp is still disabled.

The use of technology which encrypts information such as VPNs is illegal in the UAE if used to commit a crime, and large fines and jail terms are possible. Throughout the MENA region, VOIP blocking is evident; the UAE blocked the Snapchat video feature, and Saudi Arabia blocked WhatsApp, Facebook calling and Facetime. The government-owned telecommunications providers Etisalat and Du in the UAE benefit economically from encrypted calling services and since national security remains the most pressing concern, VOIP services provided are centralised with an easy backdoor for the authorities.

Recently, the UK government has yet again been refused by WhatsApp in their appeal for backdoor entry, joining other governments who want access to business, political and

social activity on the Internet to monitor for crime and terrorism. Globally there are varying approaches, with Japan and the Netherlands supporting strong encryption, whereas others such as Turkey and Pakistan have laws against it. The UK government passed the Investigatory Powers Act in 2016, giving police, security services and the government more access to private data, which is claimed to give them power to keep the public safe. Opposed by companies such as Apple and Twitter, the act requires internet companies to save data on users for 12 months and to break into devices if requested by the government. Apple's CEO claimed 'the bill could give the government the power to demand Apple alters its messaging service works", and claimed the public should be able to keep personal data private. Over an 11month period, the FBI failed to gain access to more than half of the devices it targeted. In response to terror attacks, law enforcement agencies in the UK want access to encrypted communications and the US is also exploring similar measures "to make it harder for terrorists to use technology to escape from justice", according to Obama. The FBI wants to debate the use of encryption on communications with technology companies, reasoning that it can compromise safety. The companies argue they are using AI technology to monitor for security concerns.

There is international competition to develop the strongest crypto algorithms, which would be challenging for other governments to break. Two neural networks named Alice and Bob have been shown to develop their own encryption methods using AI by Google Brain project researchers. Alice and Bob managed to keep information secret from a third network called Eve. Privacy and security are now the main feature of apps and software, for example SnapChat has end-to-end encryption, PGP (Pretty Good Privacy) uses an algorithm to protect emails, texts and files. PGP was restricted by the American government and in 1993 they introduced an encryption service with government access called Clipper chip, which quickly failed. PKC can protect against message forgery and spoofing, or changing messages, as a signature can verify the sender. Users have private and public keys to decode information, and a well-used public key can be trusted more, unless it has been falsely distributed. It allows users privacy in communications and financial transactions.

Weak encryption has been suggested as a compromise for governments and technology companies, although history has shown weak encryption doesn't work with the Clipper chip and weak encryption has been criticized for being pointless. Fair or responsible encryption might be the answer, which allows strong encryption but certain information could be decrypted with a court order. However, the user might not co-operate, or might be in

another country and so not fall under the same regulations. Also, the algorithm might be unbreakable. Meanwhile technological developments continually change the possibilities such as Chrome Canary by Google, a new browser designed to protect users from next-next-generation cryptographic attacks. Recently, quantum-based random number generators are being developed which could offer the most secure encryption keys. WhatsApp has said that end to end encryption will be more widely used in the future as 'it will ultimately represent the future of personal communication.'

References

Altaher, N. (2016, April 10). *WhatsApp encryption: Online criminal activity no longer tapped*. Retrieved from Gulf News : http://gulfnews.com/news/uae/crime/whatsapp-encryption-online-criminal-activity-no-longer-tapped-1.1707921

Carey, S. (2016, November 2). *Snooper's Charter: What you need to know about the Investigatory Powers Act*. Retrieved from Computer World : http://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/

Denning, D. (1996, January 6). *The Future of Cryptography .* Retrieved January 14, 2017, from Internet Security Review : http://encryption_policies.tripod.com/us/denning_1095_future.htm

Everington, J. (2016, April 18). *WhatsApp locks in security with encryption of messages.* Retrieved January 14, 2017, from The National : www.thenational.ae/business/technology/whatsapp-locks-in-security-with-encryption-of-messages

Gallagher, S. (2015, December 15). *What the government should've learned about backdoors from the Clipper Chip .* Retrieved January 14, 2017, from Ars Technica: http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-

Griffin, A. (2016, November 18). *Investigatory Powers Bill: 'Snoopers Charter 2' to pass into law, giving Government sweeping spying powers*. Retrieved from The Independent : http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html

Masudi, F. (2016, July 21). *Ordinary residents are majority of ransomware victims*. Retrieved from Gulf News : http://gulfnews.com/news/uae/crime/ordinary-residents-are-majority-of-ransomware-victims-1.1866436

Slack, A. (2015, June 18). *WhatsApp Can Land You in Jail in the UAE*. Retrieved from InfoSecurity: https://www.infosecurity-magazine.com/slackspace/whatsapp-can-land-you-in-jail-in/