Cryptographic failures and challenges

Technology, Information Technology

Cryptographic Failures and Challenges Affiliation Cryptography is a technique used in keeping and passing on information in a particular outline such that, only for whom the data is proposed can understand and process it. However, just like any other inventions, there are instances where the system fails, either due to hacking or general failure. In this case, private information is compromised and it can lead to disclosure of crucial data to the public.

A recent such occurrence was witnessed in Taiwan, where scientist unearthed a flaw with the country's secure digital ID system. The error enabled attackers to masquerade as some citizens who depend on it to register their cars, pay taxes, as well as file immigration documents. The crippling weaknesses discovered in the Taiwanese Citizen Digital Certificate Program spread uncertainty that certifications intended to guarantee cryptographic security used by governments and enemies cannot circumvent other delicate organizations. The scientists revealed what they termed a ' fatal flaw' in the hardware random number generator which in normally used to make sure that the numbers that make the raw materials of crypto keys are not based on noticeable patterns. Randomness is considered a fundamental element in ensuring enemies does not hack the cryptographic keys reinforcement in the smartcards provided to the Taiwanese citizens.

For the over 2 million 1024-bit RSA keys examined, about 184 keys were developed so defectively, they could be hacked in a few hours by use of known mathematical techniques and standard computers. However, if the keys had been developed right, hacking them so fast would have needed a huge supercomputer. It, therefore, reveals the feebleness of cryptographic protections that millions of individuals increasingly depend on to protect

their business-sensitive secrets and most personal secrets. The case is an example of one of the many cases revealing weaknesses in encryptions.

In conclusion, cryptography is very vital as it invention was meant on secrecy and, therefore, there should be some ways of ensuring that they uphold their mandate. In addition, since most of the breakings done are usually linked with poor generation of raw materials or codes, persons involved should be kept on their toes so that they ensure to work correctly as needed.

Reference

Goodin D., 2013, retrieved from http://arstechnica.com/security/2013/09/16/fatal-crypto-flaw-in-some-government-certified-smartcards-makes-forgery-a-snap/