Kleptography

From Wikipedia, the free encyclopedia

Kleptography is the study of stealing information securely and subliminally and it was introduced by Adam Young and Moti Yung in the Proceedings of Advances in Cryptology—Crypto '96.[1] Kleptography is a subfield of cryptovirology and is a natural extension of the theory of subliminal channels that was pioneered by Gus Simmons while at Sandia National Laboratory.[2][3][4] A kleptographic backdoor is synonymously referred to as an asymmetric backdoor. Kleptography encompasses secure and covert communications through cryptosystems and cryptographic protocols. This is reminiscent of, but not the same as steganography that studies covert communications through graphics, video, digital audio data, and so forth.

Contents

Kleptographic attack

Meaning

A kleptographic attack is an attack which uses asymmetric cryptography to implement a cryptographic backdoor.[5] For example, one such attack could be to subtly modify how the public and private key pairs are generated by the cryptosystem so that the private key could be derived from the public key using the attacker's private key. In a well-designed attack, the outputs of the infected cryptosystem would be computationally indistinguishable from the outputs of the corresponding uninfected cryptosystem.[6] [7]If the infected cryptosystem is a black-box implementation such as a hardware security module, a smartcard, or a Trusted Platform Module, a successful attack could go completely unnoticed.

A reverse engineer might be able to uncover a backdoor inserted by an attacker, and when it is a symmetric backdoor, even use it herself.[8] However, by definition a kleptographic backdoor is asymmetric and the reverse-engineer cannot use it. A kleptographic attack (asymmetric backdoor) requires a private key known only to the attacker in order to use the backdoor. In this case, even if the reverse engineer was well-funded and gained complete knowledge of the backdoor, it would remain useless for her to extract the plaintext without the attacker's private key.[9]

Construction

Kleptographic attacks can be constructed as a cryptotrojan that infects a cryptosystem and opens a backdoor for the attacker, or can be implemented by the manufacturer of a cryptosystem. The attack does not necessarily have to reveal the entirety of the cryptosystem's output; a more complicated attack technique may alternate between producing uninfected output and insecure data with the backdoor present.[10]

Design

Kleptographic attacks have been designed for RSA key generation, the Diffie–Hellman key exchange, the Digital Signature Algorithm, and other cryptographic algorithms and protocols.[10] SSL, SSH, and IPsec protocols are vulnerable to kleptographic attacks.[11] In each case, the attacker is able to compromise the particular cryptographic algorithm or protocol by inspecting the information that the backdoor information is encoded in (e.g., the public key, the digital signature, the key exchange messages, etc.) and then exploiting the logic of the asymmetric backdoor using their secret key (usually a private key).

A. Juels and J. Guajardo[12] proposed a method (KEGVER) through which a third party can verify RSA key generation. This is devised as a form of distributed key generation in which the secret key is only known to the black box itself. This assures that the key generation process was not modified and that the private key cannot be reproduced through a kleptographic attack.[12][13]

Examples

Four practical examples of kleptographic attacks (including a simplified SETUP attack against RSA) can be found in JCrypTool 1.0,[14] the platform-independent version of the open-source CrypTool project.[15] A demonstration of the prevention of kleptographic attacks by means of the KEGVER method is also implemented in JCrypTool.

The Dual_EC_DRBG cryptographic pseudo-random number generator from the NIST SP 800-90A is thought to contain a kleptographic backdoor. Dual_EC_DRBG utilizes elliptic curve cryptography, and NSA is thought to hold a private key which, together with bias flaws in Dual_EC_DRBG, allows NSA to decrypt SSL traffic between computers using Dual_EC_DRBG for example.[16]

References

1. A. Young, M. Yung, "The Dark Side of Black-Box Cryptography, or: Should we trust Capstone?" In Proceedings of Crypto '96, Neal Koblitz (Ed.), Springer-Verlag, pages 89–103, 1996.
2. G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," In Proceedings of Crypto '83, D. Chaum (Ed.), pages 51–67, Plenum Press, 1984.
3. G. J. Simmons, "The Subliminal Channel and Digital Signatures," In Proceedings of Eurocrypt '84, T. Beth, N. Cot, I. Ingemarsson (Eds.), pages 364-378, Springer-Verlag, 1985.
4. G. J. Simmons, "Subliminal Communication is Easy Using the DSA," In proceedings of Eurocrypt '93, T. Helleseth (Ed.), pages 218-232, Springer-Verlag, 1993.
5. Esslinger, Bernhard; Vacek, Patrick (20 February 2013). "The Dark Side of Cryptography: Kleptography in Black-Box Implementations" (http://www.infosecurity-magazine.com/view/30852/the-dark-side-of-cry

ptography-kleptography-in-blackbox-implementations/). *Infosecurity Magazine*. Infosecurity Magazine. Retrieved 18 March 2014.
6. Young, Adam (2006). "Cryptovirology FAQ" (http://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html). *Cryptovirology.com*. Retrieved 18 March 2014.
7. Easttom, Chuck (2016). "An Overview of Cryptographic Backdoors" (https://www.academia.edu/14152138/Cryptographic_Backdoors). *academia.edu*. Retrieved 22 September 2016.
8. Esslinger, Bernhard; Vacek, Patrick, 2013, The Dark Side of Cryptography, "... manipulation of this sort could be revealed through reverse engineering ..."
9. Esslinger, Bernhard; Vacek, Patrick, 2013, The Dark Side of Cryptography, "... sophisticated kleptographic attacks can indeed prevent [...] discovery."
10. A. Young, M. Yung, *Malicious Cryptography: Exposing Cryptovirology*, John Wiley & Sons, 2004.
11. http://kleptografia.im.pwr.wroc.pl/ SSL attack by Filip Zagórski, and prof. Mirosław Kutyłowski
12. A. Juels, J. Guajardo, "RSA Key Generation with Verifiable Randomness" (https://web.archive.org/web/20120315234258/http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/kegver/kegver.ps), in: D. Naccache, P. Pallier (Eds.), Public Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, Springer, 2002.
13. A. Juels, J. Guajardo, "RSA Key Generation with Verifiable Randomness" (Extended version) (https://web.archive.org/web/20130512223201/http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/kegver/kv-extended.pdf)
14. https://github.com/jcryptool JCrypTool project website
15. http://www.kes.info/archiv/online/10-4-006.htm B. Esslinger, *Die dunkle Seite der Kryptografie -- Kleptografie bei Black-Box-Implementierungen*, <kes>, #4 / 2010, page 6 ff. (German language only)
16. Green, Matthew (September 18, 2016). "The Many Flaws of Dual_EC_DRBG" (https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/). Retrieved November 19, 2016.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Kleptography&oldid=791205426"
