Volodymyr Nazarenko, lecturer, Department of Computer systems, networks and cybersecurity
National University of Life and Environmental Sciences of Ukraine
ORCID: 0000-0002-7433-2484
E-mail: volodnz@nubip.edu.ua

RESEARCH OF THE ALGORITHM SUBSTITUTION ATTACKS UNDER MASS SURVEILLANCE: CASE STUDY

Abstract. After mass surveillance by different Governmental organizations became open to public, followed by publication in various internet resources and platforms, concerns for security of existing encrypted protocols have risen. This study paper focuses its attention on general overview and analysis of existing algorithm-substitution attacks of private keys encryption protocols.
Keywords: privacy, information security, asa, surveillance, cryptography.

Introduction.

The notion of ASA is not new. Back in 1990 Young and Yung presented a paper on kleptography, which is similar to ASA, but proved, recently, to work in Public Key Encryption protocols [1]. General notion is that software that can support different open-source communication protocols and is nondeterministic by nature, is vulnerable to ASA, while software that uses deterministic encryption schemes and do not provide randomness is secure against such types of attacks [2].

To better understand the notion lets first have a look at the typical ASA. ASA algorithmic process can be described as following:

- The real encryption algorithm E takes, as usual, user key K, message M, and associated data A.
- It returns a ciphertext C
- The subverted algorithm Ee that substitutes for E takes the same inputs but also an additional, big-brother key, Ke. It also returns a ciphertext.

Structure of the cryptography algorithm-substitution attacks of private keys encryption protocols study can be divided in five main stages:

1. Description of on algorithm-substitution attacks, how it works for private key settings
2. The goal of Mass surveillance is not only to substitute user algorithm with its own, but also make it impossible for user to detect any changes to encrypted message.
3. Present mechanisms of attacks and algorithm-substitution. Describing types of symmetric encryption schemes that fall under this type of attack
4. Showcase mechanism for protection against these types of attack and describes theoretical model for secure algorithm.
5. Summary, that states that randomized and stateless schemes are prone to ASA, while deterministic and stateful provides counter measures.

For study purposes we use a multi-user environment. The easiest way for the attacker is to change E with its own Ea, at it is open choice. Even though such substitution will lead to attacker obtaining K through Ka. The receiver of such a message will know that this message has been compromised. But the goal of the attacker is also to hide its presence. That is why it will try to make encrypted cypher text to look like real one. Meaning message decrypted by Ea can be easily decrypted by the algorithm D. To summarize, original and subverted cipher messages should be indistinguishable to users who know only real key K.

On contrary, to prevent big brother from successfully mounting ASA original algorithm should make it impossible for him to distinguish subverted message from real one, by using its own key Ka. To sum up, both these require indistinguishability of real and subverted cipher texts to an attacker, but to protect message, attacker should not know user key K.

Overview of ASA mechanisms.

Most types of symmetric encryptions schemes, which are randomized and stateless, are vulnerable to ASA. Main goal of ASA is to get user key K from subverted cipher message, while begin undetected by end user.

Freedom of choice of compunction protocols (open API), as well as verifiability of mandated randomness makes ASAs possible. That is why Black box setting, allowing freedom choice of IV - be either random or be explicit, are extremely insecure against ASA. IV, being insecure, can lead to attacker obtaining communication session key. Variable length padding in it turn allows Attacker to use it to create channel for key transmission.

We can classify ASA attacks in 3 categories:

1. Initial vector (IV)-replacement attacks. In this type of attack IV when subverted communicates user key K, using encryption message with attackers key Ka.
2. Presents generalized ASA type of attack- biased-ciphertext attack. For this attack to succeed it needs to produce ciphertext that is end-user system can't distinguish from real one. Its biases are that without (subverted) key Ka, it is impossible to detect subversion.
3. Practical examples which show that SSL/TLS, IPsec, and SSH are very vulnerable to generic ASA attack.

Protection against ASA.

Given the definition of successfull attack, for scheme to be considered protected against ASA, it to be state-full and deterministic. However not every of such schemes are fully protected. As in public key setting, key is generated deterministically, allowing to attack to predict future instances [3]. Allowing message to be decrypted by trial-encryption. Use of states allows system to be protected against such type of attack.

Important note – privacy and authenticity of the base scheme are not helpful in achieving security against ASA. As in surveillance environment attacker obtains original key K, by subverting algorithm Ea., so it alters authenticity and privacy.

In order to achieve a reliable, encrypted channel for symmetric encryption and to overcome ASA - deterministic, stateful schemes, both for sender and receiver must be implemented. Security can be achieved by relying on combinatorial properties of the scheme. To be secure, base scheme (symmetric encryption) should have unique cipher texts. If this scheme meets decryptability condition, it is secured against ASA.

Following above statement for scheme to be considered secure against ASA: ASA will fail in differentiating real from subverted ciphertexts and won't be able to recover the message or a user's key. One important not, subverted ciphertexts, must, still, remain decryptable by the decryption algorithm of the base scheme. In order to show real benefits of protection, paper presents notion of unique cipher text with symmetric encryption schemes. It presents simple construction based on a variable-input-length PRP, which yields practical results. The paper shows that nonce-based symmetric encryption scheme can be transformed into a unique

ciphertext stateful deterministic scheme while preserving efficiency. Using existing nonce-based encryption schemes like CCM, GCM, or OCB, this yields practical designs of surveillance resistant symmetric encryption.

Restricted scope of the study and research.

This research work has restricted scope, as it considers the case of only symmetric encryption schemes (SES) [4]. When in real world environment security systems use SES as part of larger security mechanisms, which is often more prone to attacks, by the subversion. This system uses nonce to check authenticity, which can be used by an attacker to obtain session key. Another example is SSL/TLS, where nonce can be used to predict next session's keys, with the help of PRNG being backdoored.

Also, papers do not take timing information into account, as fine-grained timing behavior of the encryption algorithm can be used to get encryption key. The subverted algorithm Ea can later timing information for the end-host to create channel to transfer obtained key K. (Timing Analysis of Keystrokes and Timing Attacks on SSH).

As a result of limited scope paper cannot consider all possible type of ASA attacks, however it provides strong theoretical foundation for future study under following steps:

1. Symmetric encryption is foundation of secure communications
2. Presented model is typical for software subversion, namely, crypto library
3. Research shows that not all schemes succumb to direct ASA attacks, forcing attacker to use other, more complicated schemes
4. This research can be further used to create real-world secure protocols and mechanisms. For instance, these systems can have tasks of authenticated key exchange.

REFERENCES

1. Young, A., & Yung, M. (1997). Kleptography: Using cryptography against cryptography. In Advances in Cryptology—EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings 16 (pp. 62-74). Springer Berlin Heidelberg.
2. Bellare, M., Jaeger, J., & Kane, D. (2015, October). Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1431-1440).
3. Fischlin, M., & Mazaheri, S. (2018, July). Self-guarding cryptographic protocols against algorithm substitution attacks. In 2018 IEEE 31st Computer Security Foundations Symposium (CSF) (pp. 76-90). IEEE.
4. Berndt, S., & Liśkiewicz, M. (2017, October). Algorithm substitution attacks from a steganographic perspective. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1649-1660).

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE

FACULTY OF INFORMATION TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

PROCEEDINGS

МАТЕРІАЛИ

XI International scientific conference

XI Міжнародної науково-практичної конференції

GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2023

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 November 2023

Kyiv, NULES of Ukraine

15-16 листопада 2023 року

Київ, НУБіП України

Kyiv 2023

Київ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XI Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 листопада 2023 року

Київ, НУБіП України

Київ 2023

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 20.11.2023)

Укладач: к.е.н., доцент Харченко В.В.

Збірник матеріалів XI Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2023", 15-16 листопада 2023 року, НУБіП України, К. НУБіП України, 2023. 117 с.

Відповідальність за зміст публікацій несуть автори.