МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 131–142

УДК 519.719.2

Analysis of Russian key-agreement protocols using automated verification tools

A. M. Semenov

National Research University Higher School of Economics, Moscow

Получено 06.III.2016

Abstract. We study several Russian key-agreement cryptographic protocols for compliance with specified security properties in view of possible adoption of these protocols as standardized solutions intended to be used in the Russian Federation. We have used a number of automatic cryptographic protocol verification tools available in the Internet such as Proverif, AVISPA-SPAN and Scyther, to simulate examined protocols. We find a number of vulnerabilities and propose ways to fix them.

Keywords: cryptographic protocol, key-agreement cryptographic protocol, automated verification tool

Анализ российских протоколов выработки общего ключа с использованием средств автоматической верификации криптографических протоколов

А. М. Семенов

Национальный исследовательский университет «Высшая школа экономики», Москва

Аннотация. Работа посвящена изучению соответствия ряда российских криптографических протоколов определенному набору свойств безопасности. Анализ проводился в связи с возможной стандартизацией в Российской Федерации этих решений. С помощью доступных в сети Интернет программных средств автоматической верификации криптографических протоколов, таких как Proverif, AVISPA-SPAN и Scyther, проведен анализ указанных протоколов, найден ряд уязвимостей и предложены пути их исправления.

Ключевые слова: криптографический протокол, протокол выработки общего ключа, средства автоматической верификации криптографических протоколов

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 131–142 (Russian)

References

[1] *Properties (Goals)*, http://www.avispa-project.org/delivs/6.1/d6-1/node3.html.

[2] Cheremushkin A. V., *Cryptographic protocols: basic properties and vulnerability*: Publ. centre “Akademija”, 2009 (in Russian).

[3] Nesterenko A. Yu., “A new key agreement protocol based on Diffie–Hellman scheme”, *Sistemy vysokoi dostupnosti*, **8**:2 (2012), 81–90 (in Russian).

[4] Nesterenko A. Yu., “On an approach to the construction of secure connections”, *Mathematical aspects of cryptography*, **4**:2 (2013), 101–111.

[5] Dolev D., Yao A. C., “On the security of public key protocols”, *IEEE Trans. Inf. Theory*, **29**:2 (1983), 198–208.

[6] Blanchet B., “An efficient cryptographic protocol verifier based on Prolog rules”. In: “*Proc. 14th IEEE Computer Security Foundation Workshop (CSFW)*”, 2009, 82–96.

[7] Armando A. et al., “The AVISPA tool for the automated validation of Internet security protocols and applications”, *Lect. Notes Comput. Sci.*, **3576** (2005), 281–285.

[8] Cremers C. J. F., *Scyther — Semantics and Verification of Security Protocols*, Ph. D. Thesis, Eindhoven Univ. Technology, 2006.

[9] Matyukhin D. V., “On some properties of common key establishment schemes using infrastructure of public keys in a context of development of standardized cryptographic solutions” (2011) (in Russian), http://www.ruscrypto.ru/accotiation/archive/rc2011/.

[10] Nesterenko A. Yu., “On a protocol of common key computation” (2012) (in Russian), http://www.ruscrypto.ru/accotiation/archive/rc2012/.

[11] Grebnev S. V., “On the possibility of standardization of a key establishment protocol” (2014) (in Russian), http://www.ruscrypto.ru/accotiation/archive/rc2014/.

[12] Boyd C., Mathuria A., *Protocols for Authentication and Key Establishment*: Springer Science & Business Media, 2003.

[13] Cremers C., Mauw S., *Operational Semantics and Verification of Security Protocols. Information Security and Cryptography*, Heidelberg etc.: Springer, 2012.

[14] Lowe G., “A hierarchy of authentication specifications”. In: “*Proc. 10th IEEE Computer Security Foundation Workshop (CSFW)*”, Piscataway, CA: IEEE, 1997, 31 – 44.