Security Analysis and Trust Models in Wireless Networks

Lela Mirtskhulava

lela.mirtskhulava@tsu.ge
Department of Computer Sciences
Faculty of Exact and Natural Sciences
Iv. Javakhishvili Tbilisi State University
University str., 13, Georgia

In the given work, we analyse the serious weaknesses recently discovered in WPA2 (Wi-Fi Protected Access 2) in October 2017 and KRACK (Key Reinstallation Attack) attack on WPA2 announced by Computer Science Scientists. The KRACKs were introduced to abuse design flaws in cryptographic protocols to reinstall an already-in-use key. Several types of cryptographic Wi-Fi handshakes are affected by the attack. There are different forms of trust to address different types of network security problems and reduce risk in certain conditions.

This paper explores the trust models applied by various cryptographic schemes: a) the web of trust employed by Pretty Good Privacy (PGP) where users using their own set of trusted public keys, b) Kerberos, a secret key distribution scheme using a trusted third party, c) certificates, which allow a set of trusted third parties to authenticate each other and, by implication, each other's users. Each of the above mentioned trust models differs in complexity, scope, scalability and general applicability. Which model of trust to apply in certain circumstances and types of wireless networks are discussed in the given paper. It describes the major security issues and their techniques of building trust model by monitoring network behavior. It is intended to use secure and faster cryptographic solution for Wi-Fi networks security by using an open source public-key NTRU cryptosystem that uses lattice-based cryptography. NTRU can implement the NTRUEncrypt public key encryption algorithm in Java. NTRUEncrypt is lattice-based and known as unbreakable even with quantum computers. On the other hand, commonly used cryptosystems like RSA or ECC, can be broken by quantum computers. Therefore, NTRU is significantly faster than other public-key cryptosystems.