

AN ELECTRICAL ECHO USING TO ENHANCE THE SECURITY OF TWO-FACTOR AUTHENTICATION

Ovcharenko D.R., Antipov I. E.

e-mail:diana.naidonova@nure.ua

Scientific supervisor – Antipov I. E

Kharkov National University of Radio Electronics, Dep. CRETISS,
Kharkov, Ukraine

These theses discuss the existing vulnerability in the SS7 protocol, which threatens two-factor authentication of bank clients by phone. An attacker can surreptitiously enable call forwarding from the victim's phone to their own, thus gaining access to the victim's bank account. It is proposed to measure the electric echo time delay in order to detect call forwarding. Experimental data are provided, demonstrating the effectiveness of this method in combating fraudsters.

Two-factor authentication for accessing online banking platforms has become commonplace. The customer enters their phone number and password but gains access to banking services only after answering a call from the bank to this number and confirming the action. This procedure has been introduced by almost all banks to ensure security.

Unfortunately, vulnerabilities in the SS7 protocol used in mobile communications may compromise the security of two-factor authentication [1]. The attack works as follows: an attacker, exploiting SS7 protocol vulnerabilities, can enable the forwarding of incoming calls to their phone number without the victim's knowledge (Fig. 1). The procedure for implementing this threat is discussed in detail in [2].

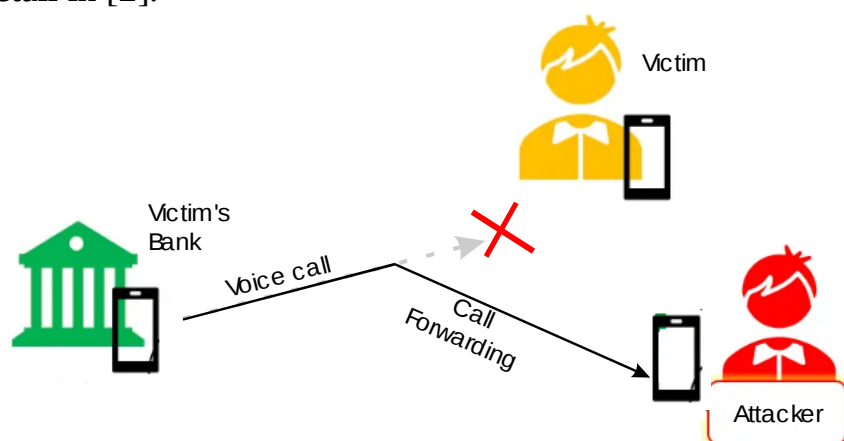


Fig. 1

Thus, a necessary condition for this attack is the voice calls forwarding.

It should be said that the activation of call forwarding does not happen unnoticed. In most mobile phones, the call forwarding activation indicated by an icon similar to shown in Fig. 2.



Fig. 2

The call forwarding function is used quite rarely, so most users are unlikely to notice the appearance of such an "icon" on their phone screen. Moreover, if this occurs only for a short time or at night, the intruders' actions may remain unnoticed.

However, call forwarding can be detected. A change in the voice traffic route affects the signal transmission delay. This change can be identified by measuring the delay of the electrical echo, as proposed in [3]. Experiments conducted by the author have shown that call redirection significantly increases the echo signal delay time.

Several echo delay measurements were conducted for calls within the networks of different Ukrainian mobile operators, for calls between different networks, and for call forwarding. Some results are presented in Fig. 3.

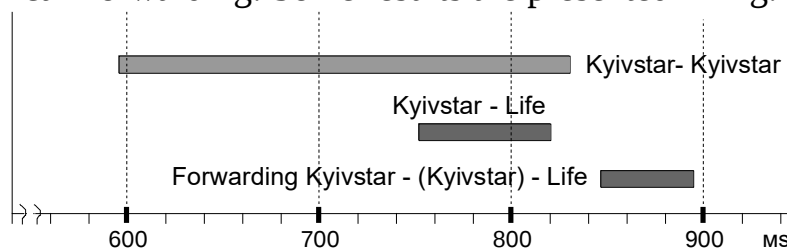


Fig. 3

As can be seen, the typical echo delay time for calls within the Kyivstar network, or from the Kyivstar network to the Life one, does not exceed 830 ms. At the same time, call forwarding increases the delay to almost 900 ms.

Thus, to implement verification by the bank, it is necessary to provide for sending a signal to measure the electrical echo delay. If the echo delay is within the limits allowed for this direction, the customer gets access to banking services. If it differs significantly, then, depending on the bank's policy, it is possible to provide for:

- blocking access;
- authentication via SMS. (SMS forwarding is not available in Ukrainian mobile networks);
- additional client identification (by voice, by answers to security questions, etc.)

References:

1. Primary security threats for ss7 cellular networks <https://www.ptsecurity.com/upload/ptcom/SS7-VULNERABILITY-2016-eng.pdf>.
2. A step by step guide to SS7 attacks <https://www.firstpoint-mg.com/blog/ss7-attack-guide/>
3. Ovcharenko D.R., Khizhnyak P.P. About the possibilities of the electric echo use for the technical information security tasks // 27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 3. – Харків: ХНУРЕ. 2023. – С 196-197.