UDC 004.056.53(045)

A.O. Korchenko Cand. Of Sci., P.O. Vikulov
(National Aviation University, Ukraine)

Etalons models of linguistic variables for spoofing attacks detection systems

One of the most promising developments for detecting threats is the method of forming linguistic etalons for intrusion detection systems, which does not yet describe the method of forming parameters etalons for spoofing attacks. Keywords: attacks, cyber-attacks, anomalies, methods of formation of linguistic etalons, intrusion detection systems, detection systems.

The development of information technology in the modern world is inextricably linked with the improvement of destructive software. Among the various ways to influence a user is especially dangerous that by masking under really existing software or web service, they try to access the personal data of the user or use its resources or software for fraudulent purposes. Recently, the number of such attacks has increased significantly, therefore, the issue is urgent regarding the creation of special means of detection and counteraction, aimed at identifying both already known types of cyber-attacks and those that will be created in the future.

For this purpose, a model of etalons for linguistic variables was developed to detect spoofing attacks, which, by assessing the state of the information system and the process of forming parameter etalons: the number of detections in spam bases, the number of spam words in the topic, and the number of spam words in the message, will formalize the process obtaining standards for the given linguistic variables of the given environment in solving tasks for detecting attacks in computer systems. Similar models can be used to increase the effectiveness of cyber-attack countermeasures aimed at detecting spoofing attacks in computer networks.

To date, the evolution of computer information systems is impossible without the parallel development of destructive software, which is aimed at the resources of information systems (RIS). A significant amount of such software is created to gain access to user's personal data, or to use fraudulent use of its information systems. This type of cyberattacks may consist of masking software offenders under existing systems and services in order to mislead the user and gain access to his data and resources. The activation of such attacks requires the creation of specialized means of detection and counteraction, which will be equally effective against both existing and promising cyber-attacks.

That is, such means can function in a weakly formalized environment [1]. Methods, models and systems based on fuzzy sets [1, 7] can be used to construct and improve existing tools for detecting anomalies in computer information systems that arose as a result of the implementation of cyber threats. Based on this, the development of appropriate technical solutions that can function in fuzzy conditions and a poorly formalized environment, will enable to identify and counteract new, modified and promising types of cyber threats.

There are very effective developments that can be used to detect cyber threats, one of such developments is the method of forming linguistic etalons for intrusion detection systems. [2, 5, 7]. In the described method, the mechanism of the process of forming parameters standards for spoofing attacks is not disclosed. Taking this into account, the actual task is to create models that will improve the process of obtaining linguistic

parameters etalons for intrusion detection systems.

To date, spoofing attacks are among the most dangerous means of implementing hacker attacks. The spoofing software misleads the user by masking under the real-world software or web service to attack, the attacker can use different types of spoofing attacks: email spoofing, IP spoofing, ARP spoofing and GPS spoofing.

Email spoofing is an attack type which essence is to forge email data (sender's address, subject, text or attachments). A letter is sent to an e-mail user, which is almost the same as letters sent by software developers or web services. A similar letter usually contains a link or an attachment that a user can open, resulting in an intruder having access to user's personal data, such as logins and passwords, bank account numbers, personal information, etc.

Ip spoofing is usually part of the Denial of Service attack, the main purpose of spoofing in this process is to mask the real IP address of the attacker, whereas the user receives packets that overload the system from an address that is not real, which complicates counteract this type of cyberattack.

ARP spoofing - cyberattack, based on the APR (Address Resolution Protocol) protocol, is used to monitor and intercept traffic within a local network. In most cases, the attacker connects his MAC address to the IP address of the attacked network. In the case of successful substitution - the attacker has the ability to access all packets that pass through the network switch. It should be noted that the implementation of this cyberattack is limited to networks using the ARP protocol.

GPS spoofing is an attack type that aims to substitute data in the GPS receiver. An intruder broadcasts in close proximity to the user, a GPS signal with a bit more power than a real GPS satellite, which results in the user receiving data not about the actual location of the receiver, but about what was sent to him by the attacker. It's worth noting that this kind of cyberattack is relatively complicated, since GPS data is calculated relative to the satellite signal delay - the attacker needs to have information about the exact location of the user, to correctly set the delay. In case of successful GPS spoofing - the user will get the effect of a "magnet near the compass" - the attacker will gradually change the data on the actual location, on the counterfeit.

Let's consider one of the most common types of spoofing, which is aimed at forgery of emails. Typically, a fake address is part of a larger-scale phishing attack whose purpose is to obtain user access data for certain services or software, but similar attacks can also be used to distribute unlicensed software.

The main purpose of email spoofing is to get the user to trust the received email. Therefore, such letters have a design and filling as much as letters that are sent by real services. Usually, such spoofing letters contain a link that will lead the user to a fake website or web service, which will also be as similar to a real prototype. Such services may include paid web services, online banks, and more. After switching to such a site, the user is more likely to enter his personal data (login, password or bank details). Which will be immediately available to the attacker and can be used by them for illegal actions on a real web service or website. In this case, the user receives a notification of the refusal to process the data.

Since direct detection of spoofing attacks is a rather complicated task, for the identification of such cyber-attacks, it is necessary to investigate possible changes in the parameters of the described environment, the values of which during a cyberattack will be

significantly different from the norm.

To identify the attack described, it is most efficient to use the following parameters: The number of detections in spam bases ("NDSB"), the number of spam words in the topic ("NSWT") and the number of spam words in the message ("NSWM"). For an attack to be successful, the attacker needs only to know the email user whose data he needs, and a site that will simulate the work of the real web service to which the user will be redirected using the information from the email.

If the normal operation of the email client of the user - the value of the described parameters exceeds the permissible limits, this may be a signal that this email is part of the spoofing attack.

Based on the specified NDSB, NSWT, and NSWM parameters and their generated reference values, as well as taking into account [3, 4, 6] it is possible to build a subset of basic detection rules that will be used to detect spoofing attacks.

Conclusions. The proposed models in this issue, which, using the expert assessment of the state of the information system and the implementation process of forming NDSB, NSWT and NSWM parameters, allow formalizing the process of obtaining reference values of certain values, which makes it possible to construct rules for detecting spoofing attacks. Such models can be used to increase the effectiveness of information security tools aimed at countering spoofing attacks in computer information systems.

References

1. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.
2. Korchenko A.A. The formation method of linguistic standards created for the intrusion detection systems, Zahist ìnformacìï, T.16, №1, 2014, pp. 5-12.
3. Korchenko A.A. The tupel model of basic components' set formation for cyberattacks, Legal, regulatory and metrological support information security system in Ukraine, 2014, V.2 (28), pp. 29-36.
4. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.
5. Akhemetov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for of intrusion detection systems // Journal of Theoretical and Applied Information Technology, 2016. Vol.87. №.2. – Pp. 221-232.
6. Mikolaj Karpinski, Poland, Anna Korchenko, Pavlo Vikulov, Ukraine, Roman Kochan. The Etalon Models of Linguistic Variables for Sniffing-Attack Detection // Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017), Romania, Bucharest, September 21-23, 2017: Vol. 1. – Pp. 258-264.
7. Improved method for the formation of linguistic standards for of intrusion detection systems / B. Akhmetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva // Journal of Theoretical and Applied Information Technology. – 2016. – Vol.87. No.2. – pp. 221-232.