УДК 621.311

ANALYTICAL REVIEW OF METHODS OF INFORMATION SECURITY IN WIRELESS NETWORKS

© 2017 С. М. Толстых, А. Г. Юрочкин

Воронежский институт высоких технологий
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации

This paper discusses features of information security in wireless networks. Network security threats can be associated with natural phenomena and technical devices, but only people embedded in the network to intentionally obtain or destruction of information, and they pose the greatest threat.

Keywords: information security, wireless network, analysis, user.

Attacks on the confidentiality of information relate to the theft or unauthorized viewing of data. This can happen in many ways, such as the interception of data while in transit or simply the theft of equipment on which the data might reside. The goal of compromising confidentiality is to obtain proprietary information, user credentials, trade secrets, financial or healthcare records, or any other type of sensitive information.

Attacks on the confidentiality of wireless transmissions are created by the simple act of analyzing a signal traveling through the air. All wireless signals traveling through the air are susceptible to analysis.

This means there is no way to have total confidentially because one can still see a signal and subsequently record it. The use of encryption can help reduce this risk to an acceptable level. The use of encryption has its own flaws, as seen later in this book. For the most part, the encryption is secure itself, although how it is implemented and how key management is handled may produce flaws that are easily exploited.

Availability is allowing legitimate users access to confidential information after they have been properly authenticated. When availability is compromised, the access is denied for legitimate users because of malicious activity such as the denial-of-service (DoS) attack.

Receiving RF signals is not always possible, especially if someone does not want you to.

Using a signal jammer to jam an RF signal is a huge problem that has been facing national governments for years. Looking for the availability of RF local area networks (LANs), one notices that performing a DoS attack is easy to accomplish. This is due to the low transmit power and poor frame management techniques included in most of the current day wireless standards.

Integrity involves the unauthorized modification of information. This could mean modifying information while in transit or while being stored electronically or via some type of media.

To protect the integrity of information, one must employ a validation technique. This technique can be in the form of a checksum, an integrity check, or a digital signature. Wireless networks are intended to function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.

If integrity is not upheld, it would be possible for an attacker to substitute fake data. This could trick the receiving party into thinking that a confidential exchange of data is taking place when in fact it is the exact opposite. Wireless networks have adapted to this type of threat over time.

One can see this advancement as new security standards emerge, creating increasingly complex integrity checks. Classification of threats and attacks in wireless.

Because wireless networks use air and space to send and receive information (signals are open to any person who is within range), data security is a very important aspect of information security system. Without proper protection of confidentiality and integrity of information during transmission between workstations and access points, we cannot be sure

Толстых Светлана Михайловна – ВИВТ АНОО ВО, студент pertsevole@yandex.ru.
Юрочкин Анатолий Геннадьевич – Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, д. т. н., профессор, e-mail: pk@vrn.ranepa.ru.

that the information will not be intercepted by an attacker, and also the workstations and access points will not be tampered with by another person.

The wide proliferation of wireless devices and their cheap cost led to the fact that a gap arises in the perimeter of network security. Specificity of the wireless network assumes that the data can be intercepted and changed at any time.

For fairly standard wireless adapter and others requires specialized equipment.

In any case, these threats are realized quite simply, and to confront them require efficient cryptographic mechanisms for protecting data.

By their nature, wireless networks cannot provide high availability. Various natural occurrences, technological and human factors can effectively disrupt the normal functioning of the radio channel.

This fact must be taken into account when designing a network and the wireless network should not be used to organize the channels for high availability requirements.

Vulnerability is understood as a system of protection of its property (architectural, or other deficiency), which can be exploited for unauthorized access to information. In other words, the vulnerability - it is a "channel" unauthorized access to protected information.

In this case, the vulnerability of any system of protection is a threat of an attacker unauthorized access to information, through the implementation of the attack (or attacks, which generally can radically different) to the vulnerability of the system of protection.

Thus, the vulnerability of a system protection - it is a system attribute, and the presence (absence) in its characteristic of the security vulnerabilities of the system.

It is obvious that in general the cause of vulnerability (the existence of "channels" Unauthorized Access) may be either incorrect implementation of protection mechanism, or lack of mechanisms for the conditions of the protected information object.

Generally speaking, the properties of correctness and completeness of implementation (enough for use) are fundamental properties of any technical system, including properties and information protection systems.

Situation analysis shows that the main reasons for uncertainty move to wireless networks are the information security issues, which for individual level, and for the system as a whole have not been determined.

Preparation for security of wireless networks must first establish that may threaten them.

Immediately it should be noted that wireless networks are different from the cable only in the former, two-the physical and partly channel -seven-level model of Open Interconnection Systems.

Higher levels are implemented in accordance with the same principles as in wired networks, but the real network security is provided at these lower levels.

The following are considered as the major threat of security in wireless networks: Violation of physical integrity of the network; interception of traffic; intrusion into the network.

Network security threats may be natural phenomena and technological devices, but the only people being introduced into the network to intentionally obtain or destroy information, and they pose the greatest threat of all.

When considering the vulnerabilities of 802.11 networks can distinguish two groups of threats: threats, on the signal level and threats to the information level. The presence of vulnerabilities on the signal level does very problematic defense information level at which must be prevented:

Deliberate distortion of the transmitted and received data;

interception of information that can be used to harm user;

interception management of communications or information system.

Besides, has not yet developed a detailed model of the threats that exist in digital wireless access networks, and methods to combat them.

It should be noted that a high degree of security of the channel on the signal level is not a guarantee of an equally high information security throughout the system.

This is because the main indicator of success of the single component system is the realization of its objective function. Signal level is lower and provides neutralization of the conflict or the threat of a component only on the site.

ЛИТЕРАТУРА

1. Ермолова В. В. Архитектура системы обмена сообщений в немаршрутизируемой сети / В. В. Ермолова, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 79-81.

2. Кульнева Е. Ю. О характеристиках, влияющих на моделирование радиотехнических устройств / Е. Ю. Кульнева, И. А. Га-

щенко // Современные наукоемкие технологии. – 2014. – № 5-2. – С. 50.

3. Львович И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. № 3. – С. 469-470.

4. Болучевская О. А. Свойства методов оценки характеристик рассеяния электромагнитных волн / О. А. Болучевская, О. Н. Горбенко // Моделирование, оптимизация и информационные технологии. – 2013. – № 3. – С. 4.

5. Ерасов С. В. Оптимизационные процессы в электродинамических задачах / С. В. Ерасов // Вестник Воронежского института высоких технологий. – 2013. – № 10. – С. 20-26.

6. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В.А.Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

7. Львович Я. Е. Проблемы построения корпоративных информационных систем на основе web-сервисов / Я. Е. Львович, И. Я. Львович, Н. В. Волкова // Вестник Воронежского государственного технического университета. – 2011. – Т. 7. – № 6. – С. 8-10.

8. Шутов Г. В. Оценка возможности применения приближенной модели при оценке средних характеристик рассеяния электромагнитных волн / Г. В. Шутов // Вестник Воронежского института высоких технологий. – 2013. – № 10. – С. 61-67.

9. Петращук Г. И. Менеджмент в предоставлении телекоммуникационных услуг / Г. И. Петращук // Успехи современного естествознания. – 2011. – № 7. – С. 175.

10. Ерасов С. В. Проблемы электромагнитной совместимости при построении беспроводных систем связи / С. В. Ерасов // Вестник Воронежского института высоких технологий. – 2013. – № 10. – С. 137-143.

11. Кострова В. Н. Оптимизация распределения ресурсов в рамках комплекса общеобразовательных учреждений / В. Н. Кострова, Я. Е. Львович, О. Н. Мосолов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 8. – С. 174-176.

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

© 2017 S. M. Tolstyh, A. G. Yurochkin

Voronezh Institute of High Technologies
Russian Academy of national economy and public administration
the President of the Russian Federation

В данной работе рассматриваются особенности обеспечения информационной безопасности в беспроводных сетях. Сетевые угрозы безопасности могут быть связаны с природными явлениями и техническими устройствами, однако только люди внедряются в сеть для намеренного получения или уничтожения информации, и они представляют наибольшую угрозу.

Ключевые слова: информационная безопасность, беспроводные сети, анализ, пользователь.