Packet fragmentation as data protection method in automated systems

D E Gorokhov, V V Ryabokon, A A Kuzkin, V S Sherbakov and M A Kutsakin

The Academy of Federal Guard Service of Russian Federation, 35,
Priborostroitel'nya str., Orel, 302034 Russian Federation

E-mail: lebedenko_eugene@mail.ru

Abstract. The paper gives a detailed description of the information transfer covert channels and their main types. One of the most popular protection methods, the one with the software and the hardware applied to traffic encryption, against the information disclosure threat is considered. Experimental data obtained from the statistical analysis of the encrypted traffic and contributing into the identification of different modern info-communication services by the IP-package distribution and the time intervals between their arrival are collected and provided. A detailed classification of the information transfer covert channels is looked upon under the regulating documents in the in-formation protection sphere. An overall mechanism of a covert channel functioning in the automated systems is described. The areas to counteract the covert channels as an information disclosure threat are specified. The authors put forward a protection method employing IP fragmentation. A diagram of a pilot stand for the videoconference systems which was tested during the experiment is presented. The parameters and the characteristics of the obtained results are described. The results are analysed, and the possible applications of IP fragmentation as a method to counteract the information transfer covert channels in the videoconference systems are offered.

1. Introduction

Informatization which is based on a wide exploitation of the information resources, information technologies, and information communication services is one of the mainstream areas in scientific and technological development in the modern society. Different business companies, public institutions, ministries, public bodies extensively use information communication systems in their everyday activities, which becomes an indispensable prerequisite for the efficient work flows. These systems significantly save the time and costs on routine tasks, including posting the information about a company, organizing business meetings, exchanging the documents, etc. The information communication services are provided via the telecommunication networks with packets switching under TCP/IP protocol stacks.

2. Data Protection

The exploitation of the information technologies in the company’s business activities is often connected with the transfer of sensitive information (for example, personnel’s personal data, commercial secrets, etc.). This information is secured from its disclosure by both software and hardware means of traffic encryption (VPN gateways, VPN gateway routers, software like OpenVPN,
PGP, etc.). These means transfer the information via crypto tunnels, thus creating a vertical private network (VPN) in a public network (figure 1). Encryption prevents an attacker from accessing the confidential information in case it is captured in a public network. Together with the protection of the transferred data, the crypto tunnels hide the structure of the private networks as the original IP headers are encrypted.

Crypto tunnels are a reliable data security tool applied to prevent information disclosure. However, in some cases, a perpetrator may not need to have an access to the content of the transferred data. To provide a destructive effect (for example, to do a denial-of-service attack or to collect the information about an encrypted communication channel), one should know what kind of information communication service is being provided at the moment and what users are provided with this service. The easiest way the perpetrator can do this is to passively observe and identify the moments in time when the information is transferred via a crypto tunnel. The obtained data can be compared with the public data (for example, the times of the videoconference sessions) to identify what official people exploit an encrypted communication channel. These actions are typically referred to passive attacks [1, 2].

![Figure 1. Encryption-based transfer of the confidential information.](image)

Statistical analysis of the encrypted traffic can provide the perpetrator with additional information about the transferred data [3]. This can be explained by two facts. First of all, the traffic of different information communication services have different statistic characteristics (traffic of information communication services is considered to be a set of IP packets generated by one instance (client) of an applied app and sent to another instance (client) of this app). Secondly, these characteristics are not changed by encryption, which is supported by the experimental data.

Main properties aimed to identify the information communication service which is traffic are the intensity (speed) of the transferred data, IP packet sizes, time intervals between IP packets. Figure 2 shows the histograms of IP packet sizes and time intervals between packet arrival for different services (videoconference, IP-telephony, data transfer).

Figure 2 clearly shows that the histograms for each service differ.

### 3. Classification of covert channels

Exploitation of the covert channels to transfer the information is one more critical issue in data protection from its disclosure with encrypted traffic means [4–6]. Under GOST R 53113.1 [7], a covert channel (CC) is a communication channel which is not supposed to exist by an information technology system developer and which can be employed to violate the security policy. A possibility for the covert channels in the computer networks is determined by the hardware platforms developed.
by foreign manufacturers with no design documents, as well as by the software with no original texts. The means which function in private networks and are employed to process the confidential information (PC, terminals for IP-telephony, videocommunication, etc.) cannot be trusted. This leads to a threat arising for the protected data transfer by modulating the characteristics of the transferred traffic. The encryption does not change these characteristics; therefore, the perpetrator can employ crypto tunnels to obtain the sensitive information even from a public network.

Figure 2. Histograms of IP packet size distribution and time intervals between packet arrival for different information communication services.

Therefore, the histograms for the specified characteristics for the encrypted traffic will be the same. Thus, it will be possible to identify an information communication service by traffic in a cryptochannel.

Threats which arise from the existence or a possibility for covert channels in an automated system (AS) can be divided into two groups:

- confidential information leakage from an AS;
- negative functional external impact on an AS performance.

Figure 3 illustrates a model describing the work of a covert channel [7]. The following notations are used: 1 is the perpetrator (security violator) who wants to get an unauthorized access to the sensitive information or an unauthorized impact on an AS; 2 is the sensitive information; 3 is the subject with an authorized access to 2 and 5; 3’ is the agent of the perpetrator in a closed loop and interacting with 2 on behalf of the subject 3; 4 is an operator who monitors the information exchange between 3 and 5 and is outside the closed loop separating the information object from the external environment; 5 is the subject inside the closed loop which interacts with 3.

Interaction between the subjects 3 and 5 is authorized within an AS. The task of an agent 3’ is to maintain a regular interactive communication with a perpetrator. The Agent should transfer the sensitive information 2 to the perpetrator 1 or to impact a critical function 2. The interaction channel
between the perpetrator 1 and the agent 3’ is a covert one, because the subjects 3 and 5, an operator 4 do not detect any information or command transfer.

The covert channels can be classified by the information transfer mechanism [7] (figure 4).

A storage covert channel uses the memory bits to encode the information by a sender and to read this information by a recipient. These storage covert channels are concealed as an outside observer does not know about the location of the hidden information. The data security system developers do not consider this memory reuse approach for storage covert channels, that is why these channels are not likely to be detected by the security measures. One can define two types of storage covert channels (figure 5).

![Figure 3. General view of a covert channel functioning in an AS.](image)

![Figure 4. Classification of covert channels.](image)

![Figure 5. Types of covert storage channels.](image)

Covert channels based on information hiding in structured data embed the data in the information objects with a formally declared structure and processing rules. The examples are the files in any text editor with hidden fields in an edit mode which could be used to embed the hidden information.
Covert channels based on information hiding in unstructured data embed the data in the information objects with no regard to the formally declared structure (e.g., encoding the hidden information in less critical bits of an image, which is not visually detectable).

A timing covert channel means that a subject sending the information uses the transmitted information to simulate a time-varying process, while the subject who receives the information can desimulate the transmitted signal and observe the information-carrying process in time. For example, the central processor in a multitasking operating system (OS) is a divisible information-computational resource for applications. The apps can simulate the processor occupancy time and transfer the data to each other.

Statistical covert channels are divided into two types by their bandwidth capacity (figure 6).

![Figure 6. Types of statistical covert channels by their bandwidth capacity.](image)

Statistic covert channels are used to transfer the information of changes in the parameters of probability distributions for any characteristics of a system which can be looked upon as irregular and be described by probability statistical models. These channels are hidden, because the information recipient is more confident in defining the distribution parameters for the observed characteristics of a system than an outsider with no knowledge about the covert channel structure. For example, a real but low-probability combination in the transmitted packet in the defined time interval can indicate a failure in a computer network.

A hidden statistic channel based on information hiding in unstructured data with a higher bandwidth and packet length value modulations is one of the most popular channels due to its simplicity and potential bandwidth capacity.

Covert channels can be avoided in two areas (figure 7):

- eliminating the differences in statistic characteristics of information communication service traffic;
- generating a dummy traffic during the intervals with no useful traffic.

![Figure 7. Actions to be protected from covert channels.](image)

The first area deals with standardizing the traffic when IP packets of similar sizes are transferred with no regard to the volume of the transmitted information (payload size should be similar for all IP packets) with similar time intervals between the packet arrivals to the communication channel.

When the IP packet sizes and the time intervals between them are balanced, then the statistic covert channel no longer exists. In this case the communication channel carries the packets with similar sizes in similar time intervals (that is, as a continuous flow). The information rate turns out to be constant and depends on the pre-defined packet sizes and time between them. Its value is calculated as follows:
where \( l \) is a pre-defined IP packet size in bytes; \( \Delta t \) is the time interval in seconds between the packets.

Traffic padding is the second approach to be used as a protection tool from the covert channels. International Telecommunication Union in its recommendations ITU-T X.800 [8] states that traffic padding is generating dummy communication samples, dummy data blocks and/or dummy data in data blocks. The same recommendation describes particular security mechanisms, including traffic padding mechanisms. Traffic padding mechanisms can provide different protection levels from the covert channels, as well as from the traffic analysis procedure. Dictionary of cryptographic terms [9] writes that traffic padding is a mechanism to fill in the gaps between the transmitted messages or their parts to hide the transmitted information in the overall flow of the transmitted data.

4. Experiment procedure

To examine the protection efficiency from the covert channels, let us consider the most popular and the simplest statistic covert channel with packet length value modulation. Let us assume that it runs in perfect conditions which presuppose a possibility to manipulate its own data alphabet generated from all possible values of packet lengths, as well as an error-free run in the communication channel. In this case, the network with the Ethernet-based packet commutation will have the alphabet of \( N = 1412 \) possible values which can be used to transfer \( K = \log_2(N) = 10.464 \) bits of information.

Let us evaluate the potential speed of this covert channel in perfect conditions. In this case, we take videoconference as an applied service which is by far one of the most popular information communication services with high requirements to the channel bandwidth. To do this, the network in figure 8 was developed.

A 10-minute videoconference session was organized as an experiment. The incoming traffic in the form of dumps was collected by a sniffer app Wireshark via a span port of a Cisco Catalyst 3750 switch. Further analysis of the obtained dumps gave the following experimental findings shown in table 1.

| End terminal                     | Number of packets in a dump | Min. size of a frame | Max. size of a frame | Average size of a packet |
|----------------------------------|-----------------------------|----------------------|----------------------|-------------------------|
| Polycom HDX 7000                | 110405                      | 60                   | 1158                 | 803.07                  |
| Tandberg Profile 7000 MXP       | 115041                      | 60                   | 1158                 | 812.65                  |

Histograms of packet size distributions for subscriber terminals are very much alike, they are given in figure 9.
The speed of a covert channel for information transfer can be about 2 kbit/s in perfect conditions, i.e. 0.002% of the main channel speed, with regard to the average speed of 190 packets/second and the amount of information K=10464 bits/packet.

Thus, this 10-minute session gave a security offender a chance to transfer the amount of information comparable with the content of a Microsoft Word or pdf text document. This can be implemented by standardizing, by filling in all the packets to their maximum value (1412 bytes), or, vice versa, to reduce the sizes of the packets by fragmentation.

The first option requires additional technical tools which will be used by both the sender and the receiver and will encapsulate the original IP packets to the packets with the maximum length. Along with that, a significant part of the bandwidth will be used to transfer useless information. Therefore, the second option is considered to be the most promising alternative. Fragmentation is typical for IP protocols, therefore, it does not require additional technical tools. MTU (maximum transfer unit) value can be pre-defined at the end terminal or at the switch panel / router closest to it. If the maximum size of a packet is reduced, this will shorten the alphabet for a covert channel, which results in lower bandwidth. However, it should be noted that the according to the equation (1) the information flow speed in the main channel will be reduced too.

5. Conclusion

It is necessary to perform additional studies to select the adequate value of the packet size - on the one hand, to minimize the covert channel bandwidth, and, on the other hand, to maintain the information speed of the main channel - rather than get straight to the fragmentation to combat the statistic covert channels. Together with this, one should examine the impact of fragmentation on the quality of the applied real-time services, such as IP-telephony, videocommunication, videoconference, which is an area for further studies and will be discussed in future works.

References

[1] Kiraly C, Teofili S, Bianchi G, Cigno R Lo, Nardelli M and Delzeri E 2008 Traffic flow confidentially in IPsec: protocol and implementation The International federation for information processing 262 311-24

[2] Cabuk S, Brodley C E and Shields C 2004 IP covert timing channels: design and detection Proceedings of the eleventh ACM conference on computer and communications security 178-87

[3] Yao L, Zi X, Pan L and Li J 2009 A study of on/offtiming channel based on packet delay distribution Computers and security 28(8) 785-94

[4] Grusho A A 1999 O suschestvovanii skrytyh kanalov Diskretnaya matematika 11(1) 24-8

[5] Arkhangelskaya A V and Kogos K G 2013 O podhode k protivodeistviu utechke informatsii po

Figure 9. Histogram of packet size distribution for the video terminals.
skrytym kanalam Bezopasnost informatsionnyh technologij 4 10-20

[6] Arkhangelskaya A V and Kogos K G 2014 Propusknaia sposobnost skrytyh kanalov, osnovannyh na modulyatsii dlin peredavaemyh paketov, pri uvelichenii dlin paketov sluchainym Metody i technicheskie sredstva obespecheniya bezopasnosti informatsii (Saint Peterburg) 40-2

[7] GOST R 53113.1-2008 Information technology (IT). Protection of information technologies and automated systems from the information security threats from the covert channels. Part 1. General Provisions 2008 http://docs.cntd.ru/document/1200075568

[8] ITU-T Recommendation X.800: Data communication networks: open system interconnection (OSI); security, structure and applications 1991 https://www.itu.int/rec/T-REC-X.800-199103-I

[9] Pogorelov B A and Sachkov V N 2016 Dictionary of cryptographic terms (Moscow) 91