THE PROBLEM OF DATA ENCRYPTION IN INTERNATIONAL RELATIONS

Лазєбна А.Д.
National Aviation University, Kyiv
Науковий керівник: к. політ. н. Поведа О.П.s

The problem of leaking confidential information and hacking the database is very relevant to contemporary international relations. It is often the case that political differences lead to information struggles for truth and power. The Government could not contain the situation at an adequate level, and the media made matters worse, at such times it was no longer possible to control the citizens of one country or another, and then the hackers began to attack. A prime example is the White House, which is attacked every year, and it’s getting harder to contain attacks.

This occurred in 2010. The Wikileaks site specializes in publishing secret documents and information which became available as a result of «leaks». More than 90,000 reports and intelligence reports published there on the conflict in Afghanistan were produced during the last six years of the military operation, during which more than 300 British and more than 1,000 American soldiers were killed.

This leak of classified information was perhaps the largest in US history. [1]

Obviously, every country needs its own reliable database, so we’ll take cryptocurrency as an example. Here’s how it works, it is easier than it might seem, the system itself works on blockchain technology (distributed register system). In this system all information is written in blocks. In this blocks we have hash. A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size into a fixed-size bit array.The result produced by a hash function is called a «hash sum» or simply a «hash», and the input data is often called a «message».A cryptographic hash function must be able to resist all known types of cryptanalytic attacks [2]. When the block closes (maximum amount of information reached) a new block appears. And so each new block contains the information of the previous block, right down to the first block. The point is that the blocks are connected linearly, so you can go back from the newest block and go through the whole story, right down to the original block. The system cannot be hacked because the logs of these blocks are distributed to all members of the system. Information can be downloaded up to 8 MB in a single block, but a government person will have to carry a ssd drive and an electronic device, where all information will be created. After creating an electronic file, the algorithm will automatically seal and send the information to the web [2].

Since blockchain security is directly linked to the computing capacity involved in the network, there is a risk that the attacker will gain control of most of the hashing power - then he can confirm the blocks faster than the rest of the network, And that’s the way to double spending with impunity. Double spending is a method of cryptocurrency fraud, where a transaction is sent to blockchain, in exchange for funds goods or services, and then a new copy of the blockchain is made just before the transaction, which, by controlling most of the hashing power of the network, is recognized as the main. Thus, the blockchain no longer contains this transaction, and the same coins can be spent again. However, control of most of the hashing power does not allow the attacker to create coins from the air, gain access to other people’s purses, or otherwise compromise the network, so the damage from this attack is limited. The worst can be a loss of confidence in the attacked network and a drop in the cost of the tokens. Such a majority attack is very expensive, so the real danger exists only in small networks. Large cryptocurrencies like Bitcoin should not be afraid of a 51% attack: anyone who controls the vast majority of hashing capacity would be more profitable simply to mail blocks and receive bitcoins than to damage the network, because once the attack is known, The value of the tokens that were stolen will drop dramatically [2].

The advantages of this solution are that: first, the information will be sent instantly, because it will be a closed server. The second is automatic control by algorithms. The third is the possibility of anonymity. The fourth is high-level cyber defense. Among the shortcomings it is necessary first of all to note the human factor and necessity of ssd drive up to 150 GB.

The human factor is that a public official may commit treason or incorrect data collection, but even so, he will not be able to extract the data and pass it on behind the grid. Human beings are also affected by social and domestic factors. Every event in a society influences it, every random change in the habitual mode of life affects your well-being, all of which strongly affects your responsibility, attention, concentration, and overall ability to work.

The features of the DES algorithm are a 56-bit key; the message can be encrypted by one program and decrypted by any other program corresponding to the DES; high processing speed is achieved by simple algorithm and high persistence. But my example is more new and practical, because the use of this encryption format has been going on since 2009, and so far there has been no successful hacking attack, as I said earlier, block recordings are distributed to all participants of the system [3].

The use of this security system will lead to better protection of government data and reduce the likelihood of leakage of information, thus resulting in a productive shift in international policy and relations between countries.

In conclusion, it is important to add that this is all a theory, and how the system will behave in practice is a completely different matter. We took the cryptocurrency as an example, but it can't compare to government data. We also need to understand that humanity is evolving every minute, and that what it is not now may come tomorrow.

References:

1. Утечка секретных документов "угрожает безопасности США" [Електронний ресурс]. Режим доступу: https://www.bbc.com/russian/international/2010/07/100721_us_wikileaks
2. Blockchain Explained [Електронний ресурс]. Режим доступу: https://www.investopedia.com/terms/b/blockchain.asp
3. Шифрование файлов[Електронний ресурс]. Режим доступу: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/shifrovaniye/

,