Tasks and Challenges of The National Cryptographic Environment Implementation in Small Countries

Karel Dolník
Karel.Dolnik@army.cz

Oldrich Pekárek
Oldrich.Pekarek@army.cz

Military Security Office
Prague, Czech Republic

Abstract

There are numerous types of equipment for cryptographic protection of information. This paper discusses reason for implementing a national cryptographic environment, and the accompanying, challenges and opportunities. Implementation of NCE is a strategic matter for all countries but for small ones it is very difficult to be self-sufficient.

Keywords: national cryptographic environment.

1. Introduction

One of the basic tasks of the Cryptographic Security Branch of the Military Security Office in Prague is to implement of the national cryptographic environment (NCE) in computer, information, and communication systems requiring cryptographic information protection.

NCE is a system of unique cryptographic methods and tools developed by a state administration authority to be used primarily within its own organization, possibly within the state administration of a respective country.

NCE is implemented mainly within the systems handling classified information to provide their cryptographic protection. This entails the protection of information transmitted by telephone, fax and radio as well as of information transmitted within information and communication systems at different layers of an OSI model (application, network, link) for various transmission technologies and protocols (TCP/IP, HDLC, X.25, ATM, ISDN, G.703, etc.) and for the cryptographic protection of the information processed and stored directly in computers. The above list shows the need for a very wide spectrum of national cryptographic algorithms and equipment, and therefore the national cryptographic environment is utilized primarily by economically and technologically developed subjects.

2. Motivation for implementation of NCE

At present, cryptography is becoming a public affair, the computer capabilities of particular subjects are increasing (either by using new and more capable or original, but significantly cheaper, technologies or by utilizing computer capacities of large networks – mainly the Internet). This increases the number of qualified attackers (students – hackers, virus creators, foreign intelligence, and international terrorist and extremist groups) as well as the motivations for attack (individual prestige, industrial espionage, and economic crime). Besides the visible attempts to paralyze the functioning of information and communication systems, it is possible to conduct hidden long-term attacks against confidentiality, integrity and authenticity of information. NCE implementation significantly reduces the risk of these threats, even in the case of an attack by a team of qualified attackers possessing great computer capacity.

Original mechanisms are not always used in implementing NCE. Instead, the so-called cloning of standard algorithms is often carried out, that is, professional modification of one or of combination of several standards, so that the adjustment does not reduce the level of the security provided. Very often a higher level of provided security may be reached by using the technique called ”cryptographic concreting”, that is, reinforcement of algorithms (for example, increasing the number of iterations, extending the key length, and adding additional security mechanisms). However, these elements may increase the requirements to compute the algorithm. Nonetheless, the need to build NCE indicates the priority of information security, and therefore the more stringent requirements are mostly acceptable. The above-mentioned constructions (cloning and cryptographic concreting) can assure the security of cryptographically protected information, even in the case of breaking through the initial standard algorithm, and thus they provide the operators of the system adequate time to replace the cryptographic security mechanisms.

One theoretically simple cryptographic technique is the so-called ”brute force attack” . It is usually based on constructing special deciphering equipment or on cumulating of computer means to achieve the highest speed for conducting individual cryptographic operations. Such equipment then goes through the possible cryptographic key space and searches for the one that corresponds to the cryptogram obtained by the attacker through bugging or through using some other techniques. By using the key, it is then able to decipher not only the specific cryptogram but also all other cryptograms encrypted at the time of the key’s validity. However, the construction of such deciphering equipment is very costly, and therefore this type of attack is carried out primarily against commonly used cryptographic algorithms – standards. The usage of this special deciphering equipment constructed to decipher the standards is ineffective for breaking through protections within the unique national cryptographic system, and the construction of such costly deciphering equipment (millions of US dollars) to break through individual nationally unique cryptographic mechanisms is not effective.

Although we can generally agree on Kerckhoff’s thesis stating that the security of a cryptographic system is based on key classification, the experience in breaking through the DES public standard, whose cryptoanalysis has become a prestigious matter for leading cryptologists all over the world, is sufficient motivation for classification of the national cryptographic algorithms and mechanisms and for their implementation within HW modules of the black-box type with a self-destruction system installed to avoid unauthorized handling. On the other hand, a lower level of classification is used for particular technical details and descriptions of mechanisms employed within individual NCE cryptographic systems than for the information processed within the system; otherwise, the usage of cryptographic protections would be laborious (primarily from the viewpoint of personnel and technical security). However, not making the algorithm public will decrease the probability of possible attacks against the cryptographic system only by the lay public.

3. Advantages and disadvantages

NCE implementation involves both advantages and disadvantages.

NCE advantages are:

- possibility to set the best–fitting level of security protections for individual cryptographic systems,
- sufficient time to replace the algorithm if the standard is penetrated (as long as its clone is concerned),
- the fact that the necessary requirement for launching a successful cryptographic attack is detailed knowledge of the cryptosystem (algorithm), which is not made public within NCE; lower risk of taking advantage of possible mistakes caused by technical equipment or staff,
- the fact that the construction of special deciphering equipment is less effective for NCE than it is for widely used standard algorithms (for instance, in the banking sector).

However, the disadvantages are:

- the need for a wide spectrum of national cryptographic equipment and mechanisms,
- the fact that, unlike the public standards, the national means used by smaller subjects have not been reviewed in detail by experts, and thus some of their shortcomings could have been overlooked,
- the need for extensive a wide research, development, and a technological base to expand and assess one's own security mechanisms,
- large investments required, low profitability of small-series production and repairs,
- time–consuming development process: proposal, approval, development, production, and implementation.

4. Various methods of implementation

Building NCE is typical for large and economically and technologically developed countries, since this task requires a broad research and development base, the necessary funds, and advanced technological capacities within the country. NCE implementation is typical for state administration systems and state security agencies (armed forces, the police, and intelligence services) in developed countries. Most of the cryptographic equipment producers are aware of this alternative and enable replacement of algorithms delivered by them with proprietal ones.

Several years ago the Czech Republic, together with other countries, rid itself of Soviet influence, making it necessary to replace Soviet cryptographic equipment with a national apparatus. Moreover, the Czech Republic is building an all-military data network, which will interconnect individual local military computer networks and stations and enable the exchange of information which is to be protected. Meeting these needs by using only national equipment exceeds the capabilities of smaller states. Therefore, they have to use equipment from foreign producers.

There are three different procedures to introduce cryptographic protection:

1. **complete own development of cryptographic algorithms and devices** – the most difficult method, need for a broad research and development base and own advanced technological capacities, costly small-series production, need for own production and repairs, time required – about six years,
2. **implementation of own cryptographic elements into procured cryptographic equipment** - joint-venture, most of the producers are aware of this possibility, need for own research and development base, analysis of the delivered equipment, necessary cooperation with a supplier, extensive guarantees from the supplier concerning further deliveries and repairs of the delivered equipment, time required – about four years,
3. **procurement of equipment and implementation of national key management** - thorough analysis of delivered equipment and primarily its cryptographic elements, required extensive guarantees from a supplier concerning further deliveries and the repair of equipment equipment, quick and simple solution is counterbalanced by the fact that the equipment's security is based partially on reliability of the supplier, time required – about two years.

All the procured as well as local equipment must undergo a detailed expert cryptotechnical security analysis. In order to do so, it is necessary to monitor new trends and findings in the area of cryptology and computer possibilities of current and future technologies.

The best proven procedure is the second one: to procure cryptographic equipment, to retain the communication component, and add the cryptographic component, usually in the form of a chip or module, while the producer will often provide tools to nationalize the equipment.

It is often appropriate to combine procedures number two and three, that is, to procure cryptographic equipment and use it to protect lower-classification information (for which the development of the equipment as a whole or of its cryptographic component may be inefficient) and later carry out a nationalization of cryptographic environment and use for protection of more highly classified information.

In order to attain a higher level of security, it is possible to conduct multi-level encrypting on various layers of the OSI model (application, network, and link). With respect to different transfer protocols and speeds, different cryptographic equipment with various algorithms and keys is used for protection. This significantly enhances the overall quality of security provided (a strong higher-order ”extension” of a real key occurs). A typical example of multi-level encryption is to secure the communication system of a classification level on the network (or link) layer; then, for the data transfer of a higher classification level, cryptographic securing on an end-to-end application layer is used. That makes the transfer within a communication system (the most vulnerable part of the system) double encrypted (usually by various algorithms with keys of various lengths).

When introducing cryptographic protection, it is useful to keep in mind the information life cycle, that is, the period during which it is to be protected. The field operational tactical systems have an information life cycle of a couple hours, minutes, or just seconds, whereas during archiving some important information, the life cycle may even be several decades. That must be reflected in the level of protection of the information, which must be sufficient during the entire information life cycle. When implementing security measures, it is necessary to determine the level of information security according to a qualified assessment of computing capability of equipment in the coming decades.

5. Space for modern technologies and inventions

When implementing the NCE, normally the older well-tested methods are used as a starting point rather than modern technological novelties, which entail a higher risk of revealing security holes, weak points, and new ways of analysis. In other wordds, it is necessary to presume the enemy monitors all communication on insecure channels, and if he penetrates the security mechanismsbeing used, he is able to decode individual classified pieces of information retrospectively. This principle is not applicable in general, because during implementation of digital signature the situation is completely different. Individual users of the system identify and authenticate one another by their signatures and certificates. If a threat that a private key is to be compromised emerges, (that is, there is a real risk of breaching the security of the security mechanisms being used), the user may revoke his certificate and pass on different, more secure means of his identification (longer keys, and different mechanisms). The enemy is consequently able to forge the user’s digital signature, but it is of no use to him, because in the current time frame the users use different keys and certificates and do not trust the former ones. That is why the development of a digital signature is reflected in the practice in a much more rapid manner.

The introduction of algorithms on the basis of elliptical curves may serve as an example of that. Until recently, the exclusive tool for creating a digital signature was the RSA algorithm. These days, for digital signatures, asymmetric algorithms defined above elliptical curves are rapidly being introduced. This presents s number advantages. Compared to the RSA algorithm, they are faster, but most notably they utilize significantly shorter keys, which is especially expedient when, for example, stored on chip cards. The following chart indicates (approximately) the necessary key lengths in bits providing comparable information security for symmetric algorithms, the RSA algorithm, and an algorithm of discreet logarithm above elliptical curves (ECDSA):

Symmetric algorithms	80	112
RSA	1024	2048
ECDSA	160	224

6. Conclusions

The creation of a National Cryptographic Environment is a strategic matter for any country. Although the process is long and technologically and financially demanding, it guarantees the national sovereignty and independence of a country. Therefore, if a smaller country is willing to develop its own National Cryptographic Environment, it is necessary to involve the entire research and development base, that is, military and civilian research institutes and universities.