RISK OF WIRING OF BIOMETRIC IDENTIFICATION SYSTEMS

Veronika Hartova, Jan Hart
Czech University of Life Sciences Prague
nverca@seznam.cz

Abstract. The biometric identification systems are used in many applications that often include monitoring and recording of sensitive information. One of the major risks that may occur are data transmission risks - when alarm information is affected, the system can no longer be relied upon. When installing biometric readers, many security risks that undermine the security of the entire building may arise. Risks that arise due to poor installation or different sabotage techniques are always a serious danger for guarded premises and may threaten guarded property. In order to avoid incorrect configuration of the entire system, it is important to ensure that the reader is installed and configured according to the manufacturer's recommendations. Errors often occur during installation arising from ignorance of how the system works and where its weaknesses are. As soon as the weaknesses of the used systems are known, countermeasures can be created against them. The problem of electric sabotage affects a large proportion of biometric systems. In the time of increasing property crime, it is highly important for biometric identification systems to be able to resist used electrical sabotage within the guarded area reliably and free of error. These tests are important both from an informative perspective and due to the possibilities of development of potential counter-measures which could lead to their improvement and an enhancement of their level of security.

Keywords: biometrics, systems, risks.

Introduction

Nowadays, biometric recognition systems are becoming more and more popular as security elements. They are primarily installed in places that require strict control over access to a given facility or to relevant information. Apart from the functionality of the systems, potential electrical sabotage of these systems is a very important factor to be borne in mind. Installation of reader devices may present many security risks which can compromise the security of an entire facility. Risks arising due to incorrect installation or various sabotage techniques present a serious threat to guarded areas. These risks may also threaten guarded property [1].

To avoid incorrect settings of the entire system, it is essential that the reader device is set up and installed according to the manufacturer's recommendations. These recommendations are not a perfect description of how to install the system, but merely the essentials for basic set up of the system. Errors often occur during installation, arising from a lack of knowledge of how the system works and where its weaknesses lie. Once the weaknesses of the systems used have been established, counter-measures may be created [2].

Materials and methods

First various types of connection had to be specified and then multi-criteria data analysis could go ahead.

Wiring for reader devices can be divided according to the type of connection logic of separate readers to the system as a whole.

Systems with central logic use a central unit containing a database of users. First, the input data are sent (coded) to the central unit via a Wiegand protocol. The unit evaluates the data and compares them with the database. If the data correspond with a user registered in the database the central unit reacts according to the relevant settings (opens the door, permits access and so on) and also contacts the reader device in question and sends it information of this reaction (coded).

Classic readers use a 26-bit protocol (Wiegand 26). This comprises 8 bits for the Facility Code, 16 bits of data from the reader and two parity bits. This makes any cyber attack more complicated than with other types of connection logic. A module must be located at the bus that can read and record (and later send) data sent by the reader to the central unit – see Fig. 1. After reading the coded data, the data must be deciphered (i.e. determine the correct decoding algorithm). Once it has managed to decipher this message, it can create a signal and enter it into the bus via the module. This method is so demanding that any potential perpetrator must have excellent electronics, programming and coding skills [3-5].

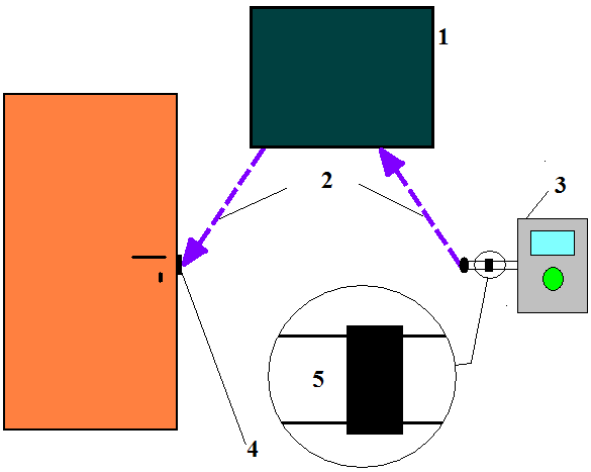

Fig. 1. **Sabotage of the system with central logic:** 1 – central unit; 2 – inaccessible wiring; 3 – reader; 4 – electrical lock; 5 – module for scanning the bus

Direct control systems are frequently used because these do not require purchase of a costly central unit. The reader device is used as the central unit. The reader device contains its own database of users and performs their authorisation independently. What is more, it serves as the end element that directly controls door opening or launches other end devices [3; 4].

If the reader device controls the electric lock directly, it is enough to substitute the reader device with a corresponding power supply, see Fig. 2. This power supply must meet the requirements for the relevant type of electric lock [4].

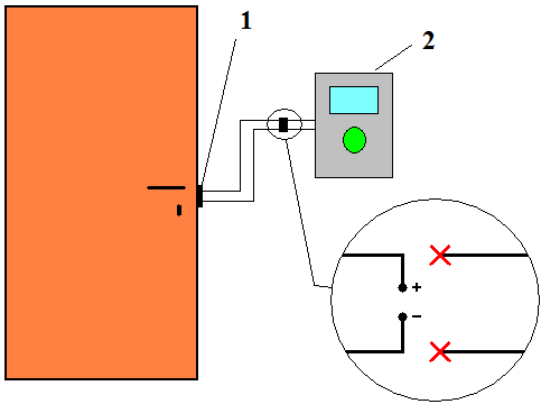

Fig. 2. **Sabotage of the system with direct control:** 1 – electrical lock; 2 – reader

Systems using an intrusion and hold-up alarm system (I&HAS) are mainly used in facilities with an already intrusion and hold-up alarm system installed. Like in direct control systems, the database is inside the reader device itself. The fundamental difference is the reader devices connected to the intrusion and hold-up alarm system central unit which reacts to disconnection (or closing) of a loop circuit. Readers connected in this way are also protected against sabotage [4; 5].

In order to be able to sabotage a reader connected in this way, you would first have to realise the principles and methods of the alarm system connections. Intrusion and hold-up alarm systems commonly use N.C. (Normally Closed) loop circuits for ordinary security and N.O. (Normally Open) for fire emergencies. There also exist several basic methods of connecting loop circuits to the intrusion and hold-up alarm system. The following types of loop circuits are used:

- simple,
- ATZ (Advanced Technology Zoning – balancing resistance),
- EOL (End Of Line – end resistance),
- EOL and ATZ.

Sabotage of the reader devices using intrusion and hold-up alarm systems is complicated mainly because there is not just one sabotage procedure, but several different variations of resulting bridging

may take place – see Fig. 3. These variations differ from each other by the method of connecting up the short-circuit loop and you need to know precisely what type of power supply is used before attempting to use a certain method of sabotage [3-5].

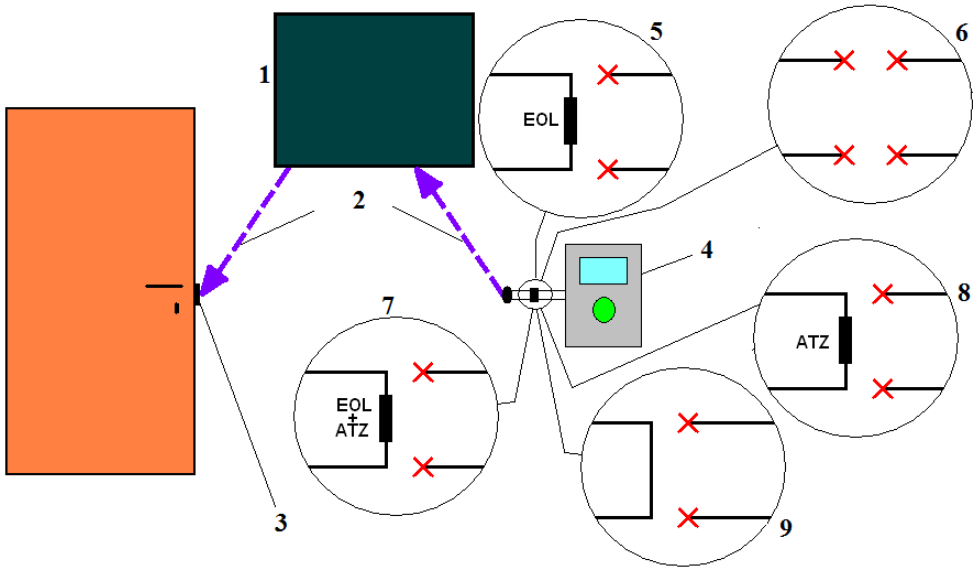

Fig. 3. **Sabotage of the system with I&HAS:** 1 – I&HAS; 2 – inaccessible wiring; 3 – electrical lock; 4 – reader; 5 – with EOL and without ATZ or with EOL ATZ N.O.; 6 – without EOL and ATZ or with EOL and without ATZ N.C.; 7 – with EOL and ATZ N.C.; 8 – without EOL and with ATZ N.C.; 9 – without EOL and with ATZ or without EOL and without ATZ N.O.

Results and discussion

All variations of the above sabotage techniques were tested apart from bus decoding. Decoding via Wiegand 26 protocol was not executed due to subsequent bus protection. If this communication were decoded, this decoding algorithm could be used for sabotage of all classic reader devices, which would compromise their security.

The resulting complexity of the individual types of electronic sabotage of reader devices is presented in Table 1. The parameters were set from the point of view of a saboteur, who needs a certain length of time, technical equipment and to perform the sabotage and who in the course of the sabotage attempts to avoid any risk of being detected.

Table 1

Complexity of the various kinds of sabotage

		Time of sabotage	Technical equipment	Risk of detection
Systems with central logic		several days	Professional	Great
Direct control systems		3 minutes	Basic	Zero
System with I&HAS	**Simple loop (N.C.)**	1 minutes	Basic	Little
	Simple loop (N.O.)	3 minutes	Basic	Little
	with ATZ (N.C.)	5 minutes	More advanced	Great
	with ATZ (N.O.)	3 minutes	Basic	Great
	with EOL (N.C.)	3 minutes	Basic	Medium
	with EOL (N.O.)	5 minutes	More advanced	Great
	with EOL and ATZ (N.C.)	7 minutes	More advanced	Great
	with EOL and ATZ (N.O.)	5 minutes	More advanced	Great

Hypothesis: use of a different connection with an end element other than a Wiegand bus, while using a central unit system compromises input protection security.

Weighting coefficients were set for separate types of the evaluated parameters on the basis of the conducted tests. Points were allocated in the course of this using a points-based evaluation method in a multi-criteria analysis of the variations, the following point scores were allocated in the following manner. Weightings were allocated for the sabotage time, technical equipment and risk of detection from lowest to highest (the shortest sabotage time, the least need for technical equipment, and the lowest risk of detection came in the first place), while where equal values arose, the resulting points score created an average.

The resulting summation of the weighting coefficients appears in Table 9. This table also shows the resulting value of the weighting classification. The resulting summation of weightings is indicated by the sum of the points in the separate lines in Table 2.

Table 2

Weighting coefficients for complexity of the various kinds of sabotage

		∑ weights	Ranking
Systems with central logic		27.5	**10**
Direct control systems		7.5	**2**
System with I&HAS	**Simple loop (N.C.)**	6.5	**1**
	Simple loop (N.O.)	9.0	**3**
	with ATZ (N.C.)	22.0	**6-8**
	with ATZ (N.O.)	14.0	**5**
	with EOL (N.C.)	10.5	**4**
	with EOL (N.O.)	22.0	**6-8**
	with EOL and ATZ (N.C.)	24.0	**9**
	with EOL and ATZ (N.O.)	22.0	**6-8**

The resulting summation of the weighting coefficients clearly demonstrates that the greatest risk for connection of reader devices is connecting a reader device as a direct control system and using an intrusion and hold-up alarm system using a simple loop circuit. Conversely, using a system with central logic appears to be the most secure option.

In practice, this means that it is important to abandon the use of the direct control and intrusion and hold-up alarm system connection systems and to move over exclusively to central logic systems.

With respect to the indisputable results of the points-based evaluation method in multi-criteria analysis of variations, the hypothesis is confirmed.

With the existing systems, systems for classification and detection of short circuit faults must be given consideration; for example, the author Fathabadi, H. addresses a similar topic in his article "Novel filter based ANN approach for short-circuit faults detection, classification and location in power transmission lines". The issue of biometric system security has been addressed by Adámek, M., who in his article "Security of biometric systems" talks of the overall security of such systems and points out their failings [6; 7].

Conclusions

The resulting summation of the weighting coefficients clearly demonstrates that the greatest risk for connection of reader devices is connecting a reader device as a direct control system and using an intrusion and hold-up alarm system using a simple loop circuit. Conversely, using a system with central logic appears to be the most secure option. In practice, this means important to abandon the use of the direct control and intrusion and hold-up alarm system connection systems and to move over exclusively to central logic systems. For the user, apart from system reliability as such, it is also very important how to connect up a given system and to consider the risk of such a connection. The manufacturers should concentrate on that branch to avoid potential unwanted attacks on recognition systems as a whole.

Acknowledgements

It is a project supported by the IGA 2016 "The University Internal Grant Agency" (Innovation of systems for verification of a person according to his characteristic).

References

1. Fathabadi H. Novel filter based ANN approach for short-circuit faults detection, classification and location in power transmission lines. International Journal of Electrical Power and Energy Systems, vol. 74, 2016, pp. 374-383.
2. Křeček S. Handbook of security technology. Blatná: Circetus, 2006. 313 p. (In Czech)
3. Cumming, N., Security: A Guide to Security System Design and Equipment Selection and Installation. Elsevier Science, 1994, 338 p.
4. Petruzzellis T. Alarm Sensor and Security. McGraw-Hill Professional Publishing. 1993, 256 p.
5. Staff H., Honey G. Electronic Security Systems Pocket Book. Elsevier Science. 1999, 226 p.
6. Adámek M., Matýsek M., Neumann P. Security of biometric systems. 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, vol 100, 2015, pp. 169-176.
7. Capel V. Security Systems & Intruder Alarms. Elsevier Science, 1999, 301 p.