Zuzana Kurillova - Lukas Fischer - Thomas Hoch*

BEHAVER - BEHAVIOURAL PATTERNS VERIFICATION FOR PREVENTION OF PHYSICAL PENETRATION USING IDENTITY THEFT

Nowadays every provider of critical infrastructure is obliged to use alarm systems - mainly simple surveillance CCTV cameras - to increase security and safety of those objects. Yet such systems have proven ineffectual in preventing security disrupting situations, such as identity theft, as the most they can do is offer evidence to identify perpetrators of criminal acts once they have occurred. To use them for crime prevention, specially trained personnel need to monitor all screens constantly on the look-out for potentially dangerous activity - which is financially and time-consuming and prone to mistakes.

This study aims at developing semi-automatic video surveillance technologies, which are able to detect events of changed behaviour of employees in relation to their standard behaviour - this means for example cases of identity theft, possible blackmail of a person, or safety disrupting cases - an employee might be sick or under influence of drugs what may lead to potentially dangerous acts.

Keywords: *behavioural patterns, CCTV surveillance cameras, crime prevention, identity theft*

1. Introduction

Nowadays, protected premises are mandatorily equipped with closed-circuit television (CCTV) infrastructure, which proves to be ineffectual for the prevention of identity theft. Resource constraints often make it impossible to have human monitoring of all the CCTV screens all of the time in order to recognize any inappropriate access in protected premises of soft targets. Criminals, using stolen proofs of identification such as cards, documents or passwords can freely enter, unrecognized by the CCTV monitoring operatives. Biometrics controls are not always applicable due to technical, economical and ethical reasons.

Use of identity theft is one of the most probable scenarios in targeting of the protected premises. To emphasize the importance of the BehaVer project, the following quote is used from Mr Alan Gooden, former (to 2017) National Identity Crime Operational Lead UK Policing & Identity Security Adviser to Home Office UK Government Dept.: *" In my experience it is extremely difficult to quantify with any confidence the full extent of any form of Identity Theft / Impersonation owing to the way that crimes are recorded. This is because the Identity Theft is an enabler to the resultant offending / crime and as a consequence is not recorded as the crime in and of itself.*

It is however clear that Identity Theft and Impersonation is an increasing threat to society within multiple forms of criminality most notably theft and fraud and it follows that acting as an enabler to corruption and insider threats within high value / risk institutions the threat is equally and proportionately increased and will continue to be so for the foreseeable future. Identity related crime is responsible for losses within all sectors of the economy including business, charity, government, as well as enabling terrorist threats. The targeting of staff members by organised crime groups, coercing them into providing sensitive information or to help the criminals facilitate criminal activity is a very real concern. Law enforcement requires enhanced tools to address this burgeoning threat as a matter of urgency" [1].

The principal aim of this project is to put in place robust, real time identity verification measures and intervention strategies to stop an attacker with the stolen identity of an authorized person before the attack.

Currently three levels of identity control are identified:

- virtual (specified by logins and passwords, PINs, certificates or digital signatures [2], [3], [4]),
- document-based (defined by documents or identification cards like a passport, badge, drivers licence and similar [5]), and

* [1]Zuzana Kurillova, [2]Lukas Fischer, [2]Thomas Hoch
[1]Department of Security and Safety Research, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Software Competence Center Hagenberg GMBH, Austria
E-mail: Zuzana.Kurillova@fbi.uniza.sk

 https://doi.org/10.26552/com.C.2018.2.78-82

- human-biometrics-based (e.g. via fingerprint [6], [7] or retina).

The strongest protection can be reached when there is a combination of multiple identity controls. For example - a combination of a password (something to know), an identity card (something to have) and a biometrics check (something to be) [8] should decrease the possibility of identity theft to the lowest possible measure.

However - both virtual, document-based identification and even some biometrics controls can be duped or they are not applicable due to technical, economic or ethical reasons. For example, face recognition can be easily circumvented [9], while duping of behaviour needs intensive observation of the person, which makes these kind of attacks time consuming.

2. BehaVer framework

The proposed solution described in this paper, the BehaVer framework, will offer an easy to implement solution for identity control of authorized persons in the protected premises that can be tailored for the adaptation within existing CCTV infrastructure. The proposed software based solution uses deep learning of big data extracted from the cameras and intelligent video surveillance to recognize changes of the actual behaviour of the authorized persons in comparison to their standard behavioural patterns.

The BehaVer framework is technically easy to implement in the protected premises (and therefore a robust yet economically viable solution). Video surveillance by the CCTV cameras for example is already wide spread and is installed for the daily use inside the protected premises. As such, only the software needs to be installed and some slight changes in the working environment are recommended in order for the benefits of the BehaVer system to be realised. This software, together with a standard for prevention of physical penetration using identity theft and an e-learning platform, will offer an effective, financially viable and technically accessible solution for protected premises EU-wide [10].

Moreover, the proposed software also offers the effective use of already installed CCTV infrastructure in the protected premises to increase security and safety of those facilities. So far, such systems have proven ineffectual in preventing security disrupting situations, such as identity theft. Rather, they have been utilised only as means of evidence gathering to identify perpetrators of criminal acts - once they have occurred. The use of behavioural detection systems for the crime prevention, such as identity theft, requires specially trained personnel to monitor all screens constantly on the look-out for potentially dangerous activity - which is financially untenable, time-consuming, as well as being prone to mistakes. Security personnel would, for example, need to monitor all authorized persons and their privileges in the protected premises all the time at all the locations.

The primary goal of this project is to develop the **BehaVer software** to prevent identity theft based on video surveillance of physical behavioural patterns (i.e. how the person usually behaves), especially when other identity control mechanisms are outmanoeuvred or are not deemed applicable or sufficiently robust. The project will propose a novel technology that can be used to check physical identity of authorized persons based on analysis of usual behavioural patterns of authorized persons - how do they park a car in the parking lot - how do they show their badge or - which door they normally use etc. In the case of a stolen identity of an authorized person in the protected premise, the proposed BehaVer software could recognize that the person's actions were inconsistent with usual patterns of behaviour and thus detect and raise awareness of a potential threat in real time. Based on big data analysis of video surveillance of the authorized persons' daily behavioural patterns, the BehaVer project will develop novel technologies that are very difficult to overcome or manipulate. With the amount of data collected, the technology will become more and more accurate, due to constant learning of behavioural patterns of the authorized persons. Furthermore, the technology will be cost-effective and easy to implement in protected premises, as it uses already existing infrastructure of surveillance cameras that are mandatorily installed in the protected premises, but so far ineffectively used.

The secondary goal of the project is to develop a **standard for prevention of the physical penetration using identity theft**. It will present the knowledge and implementation of selected methods and useable approaches. The application of this standard in protected premises will support the prevention of identity theft.

The tertiary goal of the project is to develop an **e-learning platform for prevention of the physical penetration using identity theft** based on the above mentioned standard and software. In a user friendly way, the BehaVer e-learning platform will present the knowledge collected in the project to be used for further education of stakeholders. It will also be used as a training repository and toolkit for the education of practitioners before the field demonstration of the BehaVer software (Figure 1).

3. Technology for prevention of the physical penetration using identity theft

In the following section the technology for prevention of identity theft of an authorized person will be described, to explain the proposed solution. The technology is based on:

- Surveillance from the CCTV cameras that are already mandatorily installed in protected premises,
- Token, in the form of a mobile phone, is carried by the authorized person - this helps re-identification of a person at each checkpoint. (At this stage of development, the token is still necessary. One of the aims of the project will be to eliminate this token from the technical infrastructure - so that

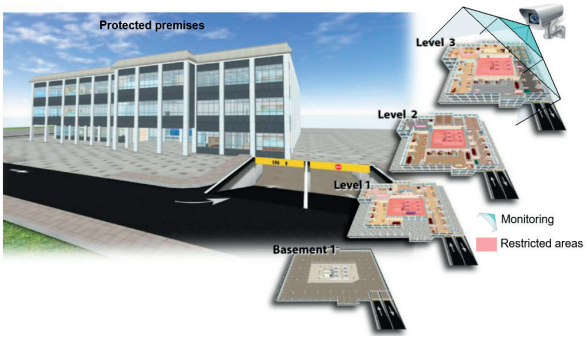

Figure 1 *Premises containing monitored restricted areas protected and/or operated by practitioners and other strategic operators*

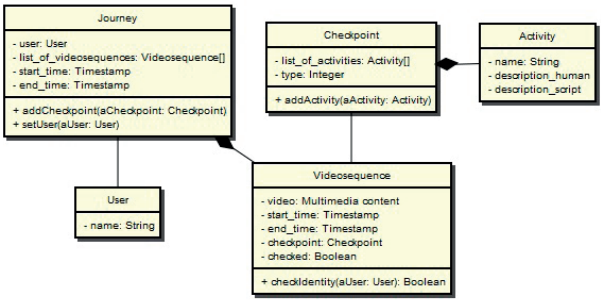

Figure 2 *Object-oriented diagram of the information system. Each journey contains video sequences of the user's presence near a checkpoint*

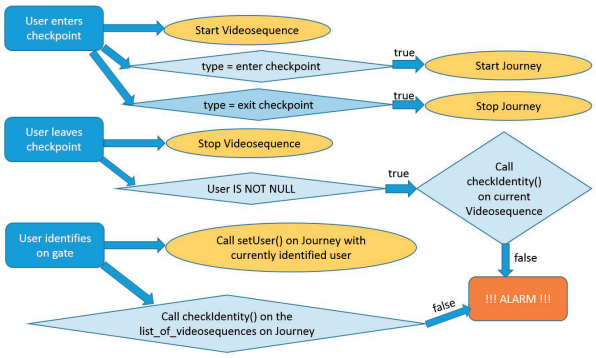

Figure 3 *Event-driven diagram to describe the system*

the person can be re-identified on different cameras without the token.)

- Prototype software that will process the real-time data from the cameras and the token and analyse them accordingly to the techniques developed in the project. It will compare previous behavioural patterns with the actual one of the authorized person. The output of the prototype software will be determination if the behaviour of the authorized person is consistent or inconstant with established behavioural patterns. Finally, in the event of a change, a notification will be sent to authorised security personnel in order to initiate further checks and validation.

The protected premises contain various "checkpoints" - these are places where CCTV cameras are installed. Each time an authorized person enters the area under control, it means he or she will approach an entering checkpoint with a CCTV camera, the "journey" will be created and started in the system. This journey will contain all the video sequences of the authorized person until he or she leaves the controlled area at the exit checkpoint (Figure 2).

Each checkpoint contains a list of "activities", selected from the Key Behavioural Pattern (KBP) list which are analysed (parking the car, entering the doors, showing the badge). These activities are described in a human language to be understandable for the technical staff and in the script language (Motion Description Language - MDL), to be understandable for the computer (see Activity in Figure 2).

Event-driven architecture [11] will be used for implementation of the system, as it really suits the nature of the mechanism - where the activity is triggered by the events that occur in the surveillance area. As detailed in Figure 3, a user (authorized person) either:

- Enters the checkpoint area,
- Exits the checkpoint area, or
- Identifies himself/herself at the gate (for example with a card, password and/or biometrics)

When an authorized person enters a checkpoint, the video sequence will start. When he or she leaves the checkpoint, the recording will stop. In the spots before identification of the authorized person at the gate, those video sequences are only recorded. When the authorized person identifies at the gate (by an object, like a card, knowledge, like a password and/or a biometrics), the Journey will be matched with the User and the *checkIdentity* process can start - on all the previous activities of the user (in the parking lot, entering the area).

The *checkIdentity* process will be based on comparison of the behavioural patterns of the examined authorized person with the current activity. The behavioural patterns will be the result of the big data analyses of the previous daily behaviour of the user and deep learning processes will give the sensitivity of the differences of the behaviour.

With every other checkpoint after the gate, the *checkIdentity* process will be performed for each activity defined in the checkpoint. Authorised security personnel will be notified immediately, if the patterns do not match with the pre-recorded behaviour (in the limits of the sensitivity). The process of constant deep learning will be optimized to prevent false cases, but to identify the real emergency cases.

4. Methodology

The essence of this project is firstly the creation of a software tool to prevent identity theft of an authorized person, based on intelligent video surveillance of daily behavioural patterns recorded on surveillance CCTV cameras. If the actual behaviour

of the authorized person changes in comparison to the behavioural patterns - there is a potential of identity theft and appropriate security authorities will be notified. Secondly, it aims to create a standard for the prevention of physical penetration using identity theft. The third goal is to create an e-learning platform that presents the knowledge accumulated by the project in a user-friendly way. These three outputs will provide a strong prevention foundation against the physical penetration to protected premises using identity theft.

The following steps need to be taken to create the software:

- Data Collection and Requirements Analysis - Firstly, all the relevant data is collected from practitioners to describe the current state, such as daily activities of the authorized persons in protected premises and requirements of the practitioners that can be provided by the better tools in prevention of identity theft.
- Key Behavioural Patterns (KBP) - In this step behavioural patterns of authorized persons in various types of daily activities are defined. This step focuses on the psychological analysis and listing of subconscious behavioural patterns that can uniquely define a concrete authorized person. Then, a machine-readable language (Motion Description Language - MDL) for the KBP description is defined and the KBP are described in this language.
- Specifications of the Software Prototype - This is a preparatory phase for implementation of the prototype. The two technologies will be created as the background for implementation of the software prototype. The first technology is developed for optimal recognition of the KBPs from the video sequences in the surveillance cameras. The second technology is based on deep learning that follows the daily KBP of individual authorized persons and learns the specificities of each of them so that he or she is uniquely defined in the system. Afterwards, models of the future software prototype will be created based on the analysis of practitioners' requirements and the above-mentioned technologies in order to be implemented.
- Software prototype implementation - In this step the software prototype is implemented based on the specifications and the user manual is created.
- Software Prototype Testing - Laboratory tests and real-environment tests of the software prototype are performed. Test results are repeatedly reported back. The technical parameter recommendations are noted to be included into the user manual.
- Field Demonstrations - An e-learning platform will be implemented to present the BehaVer software and the standard at the sites of the practitioners and validate if the final product meets their needs.

The following steps need to be taken to create the standard:

- Analysis of identity theft tools - Analysis of possible security incidents in the protected premises will be performed based on physical penetration using identity theft, with help of the practitioners' experience.
- Risk assessment - The likelihood and consequences of the specified scenarios and strategies for the treatment will be evaluated. This will include the description of used cases when the newly developed software can be used.
- Identity theft prevention measures - The newly developed software will be described here as an effective solution.
- ©EN standardization - A framework for prevention of the physical penetration using identity theft will be created and the standardization process will be initiated.

5. Conclusion

In this paper a solution for prevention of the physical penetration using identity theft - the BehaVer framework was introduced, consisting of a software tool, a standard and an e-learning platform that will be implemented in the future BehaVer project.

The BehaVer project proposal was submitted as a H2020 RIA project under the call Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism. In the case of support, it is believed that the project has potential to solve the above mentioned problem of prevention of the physical penetration using the identity theft. Ideally, the BehaVer software and standard would be adopted by the practitioners, such as operators of critical infrastructure [12] and operators of any monitored restricted areas with certain level of anonymity and limited number of authorized persons. Thus, the prevention of such crimes, using the software and the recommendations from the standard, would reduce possible investigative costs and costs caused by the harm of the attacker [13], as well as reduce societal distress and the impact on victims and their relatives. Furthermore, it is believed that the standard for prevention of the physical penetration using the identity theft would be accepted by the scientific community and research organizations and thus it would cultivate and advance technological innovations for prevention of more terrorist endeavours that include identity theft.

References

[1] GOODEN, A.: National Identity Crime Operational Lead UK Policing & Identity Security Adviser to Home Office UK Government Department. "Quote to BehaVer". E-mail to prof. HARAN, M., 2017-08-14.

[2] CUIJPERS, C., SCHROERS, J.: eIDAS as Guideline for the Development of a Pan European eID Framework in FutureID. Proceedings of Open Identity Summit 2014, Germany, 237, 23-38, 2014.
[3] TRABELSI, S., SENDOR, J., REINICKE, S.: PPL: PrimeLife Privacy Policy Engine. Proceedings of IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY 2011), Italy, 184-185, 2011.
[4] SABOURI, A., RANNENBERG, K.: ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life. Proceedings of International Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation, Greece, 2014.
[5] LIU-JIMENEZ, J., SANCHEZ-REILLO, R., BLANCO-GONZALO, R., FERNANDEZ-SAAVEDRA, B.: Making Stronger Identity for EU Citizens. Proceedings of 49th Annual IEEE International Carnahan Conference on Security Technology (ICCST 2015), Taiwan, 333-339, 2015.
[6] GAWANDE, U., GOLHAR, Y., HAJARI, K.: Biometric-Based Security System: Issues and Challenges. Studies in Computational Intelligence, 660, 151-176, 2017.
[7] RAJESWARI, P., VISWANADHA RAJU, S., ASHOUR, A. S., DEY, N.: Multi-Fingerprint Unimodel-Based Biometric Authentication Supporting Cloud Computing. Studies in Computational Intelligence, 660, 469-485, 2017.
[8] LOVECEK, T., VELAS, A.:Security systems, Alarm systems (in Slovak). EDIS, Zilina, 2015.
[9] Dupe Facial Recognition Software Using Bespoke Glasses. Available: http://www.prodigitalweb.com/ dupe-facial-recognition-software-using-bespoke-glasses/.
[10] Maris, L. Fanfarova, A.: Modern Training Process in Safety and Security Engineering, Key Engineering Materials, 755, 202-211, 2017.
[11] Souleiman, H., O'Riain, S., Curry, E.: Approximate Semantic Matching of Heterogeneous Events. Proceedings of 6th ACM International Conference on Distributed Event-Based Systems (DEBS 2012), Germany, 252-263, 2012.
[12] Zagorecki, A., Ristvej, J., Klupa, K.: Analytics for Protecting Critical Infrastrusture. Communications - Scientific Letters of the University of Zilina, 17(1), 111-115, 2015.
[13] STRELCOVA, S., REHAK, D., JOHNSON, E. A. D.: Influence of Critical Infrastructure on Enterprise Economic Security. Communications - Scientific Letters of the University of Zilina, 17(1), 105-110, 2015.