The Challenge of Licensing Artificial Intelligence Technology for Cybersecurity Applications

Michał Rotnicki†
Technology Transfer Department
NASK – national research institute
Warsaw, Poland
michal.rotnicki@nask.pl

ABSTRACT

The central question of this article is whether the transfer of cyber security technology based on neural networks into a production environment poses significant challenges due to the complexity and time variation of the technical environment, constantly evolving threats, and regulatory requirements.

The article uses observational research techniques for cybercrime activities, and experimental research for product management since 2011.

The article presents an application case study of behavioural biometrics and artificial intelligence (AI) techniques to detect remote desktop attacks, and technology transfer adaptations to changing conditions.

The added value of the paper is to draw conclusions from a real business case observed in internal business activities.

KEYWORDS

Cybersecurity, Artificial Intelligence, software licensing, software development, low compliance, behavioral biometric, AI licensing.

1 INTRODUCTION

NASK activities are focused on issues of security in cyberspace.

One of the areas of influence on cyberspace [6] is the provision of new technologies for counteract cybercrime and transfer them to commercial IT products. The goal is to increase resilience of the banking services and key services supplier [1].

The banking sector is particularly vulnerable to the activities of commercially motivated criminals [7], who are believed to be personally motivated in their criminal activities. These are criminals who directly seek to make a profit by seizing the funds of electronic banking users.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
Information Society 2024, 7–11 October 2024, Ljubljana, Slovenia
© 2024 Copyright held by the owner/author(s).

It's difficult to quantify the impact of cybercrime on the banking sector, but public data from the US[17] and the EU [16] suggest it is around €4 billion each. The criminals are highly effective in the search for the optimal strategy of action in order to steal money from Internet users, while at the same time minimizing the legal risk and the resources (effort) involved **Error! Reference source not found.**

The criminal'ss resources involved are the use of a technical method, a socio-technical method, or both, leading to a successful theft [5].

2 METHODOLOGY

Since 2007, cybercrime data has been based on natural observations. NASK provides Computer Emergency Response Team (CERT) services at the national level and commercial threat intelligence services to the main financial institutions in Poland.

The case study is an original commercialisation case provided as part of the BotSense product offered by NASK.

3 THE BANKS, THE THIEVES AND EVEN THE SCIENTISTS

Poland has a population of about 38 million and in the first quarter of 2024, the Polish banking sector operates approximately 43,5 million accounts retail accounts with contracts allowing access to internet banking. About 23 million accounts are actively accessed via internet banking and about 22 million users access via mobile applications [15]. Since 2007, NASK has been working with the Polish banking sector to identify and counteract theft from Internet banking users. Over the years, with the improvement of technical methods of protecting electronic banking, both on the side of the banks and on the side of the end user, attacks based on vulnerabilities of IT systems, have been significantly reduced [2] [3]. They required sophisticated technical knowledge, considerable technical resources and centralised malware management, making such criminal infrastructure vulnerable to law enforcement.

Socio-technical attacks , on the other hand, have experienced a renaissance, using voice communication techniques to persuade the victim to provide the criminal with login and authentication credentials for banking transactions and, crucially,

to give the criminal access to their device's desktop via a legal remote access application.

As a result, the attack scenario does not require any specialist IT knowledge [9], which has made this method of criminal activity accessible to a wider group of criminals, resulting in a sharp increase in the number of remote desktop attacks.

At the same time, in a social engineering and remote desktop attack scenario, there is virtually no event that can be classified as technically incorrect. The user voluntarily provides his or her credentials to the criminal, voluntarily agrees to open a remote desktop connection, and is often persuaded by the criminal to deliver the final blow by turning off the monitor. This means that no cybersecurity incident occurs in the data transmission channel between the endpoint and the bank's server.

Analyzing the above, it can be said that a dynamic market model is emerging in which criminals are effectively and efficiently adapting to the limitation of increasing the resistance of information systems to cyber-attacks. Criminals are creatively and rationally searching for new effective techniques and crime scenarios to carry out successful theft. The specific type of attacks mentioned above are those carried out with the unwitting participation of the victim.

However, banking institutions in particular, burdened by legislation [11], are forced to search for ever new technical solutions to identify electronic banking sessions compromised by criminals.

From a technology transfer perspective, this raises the non-obvious problem of how to organize the process of technology transfer to combat criminals.

4 Case Study - Behavioral biometrics and artificial intelligence techniques to detect a access via Remote Desktop

NASK set up an internal research project to work on an AI model capable of analysing how an end user uses a keyboard to identify themselves. In a laboratory environment, this is a task that requires a certain number of experiments, the construction of relevant data sets and the application of technical expertise, but in principle the level of scientific risk is limited. However, when it comes to transferring the developed technology to a production application that is expected to operate at a certain minimum level of effectiveness for the entire population using e-banking, the issue becomes much more complicated.

Even if the expected level of efficacy is auxiliary, e.g. 70%, and unrepresentative individuals are discarded from the user population.

4.1 The cybersecurity technology ecosystem

Cybersecurity technologies require deep and precise technical integration with the environment to be protected. For example, tracking the use of a keyboard via a web browser, as a function of the time can be disrupted by the security mechanism embedded in that web browser. One of the security mechanism implemented by vendors is randomization of selected user behavior data and disrupt the time line data.

If we take the oversimplification of identifying the main layers of the environment in which cybersecurity technology must operate, we can distinguish between technical layers: device category, hardware, operating system, components of operating system, web browser.

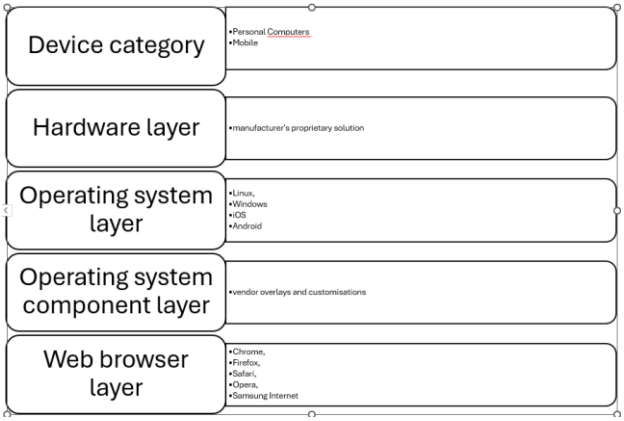

Figure 1: Technical layers

However, overcoming the additional complications posed by the diversity of devices, operating systems and web browsers does not guarantee the achievement of a stable, transferable technology. The whole technical environment described above is evolving. For example, the major web browsers, Chrome [13] and Firefox [14], are released on a monthly basis. This means that, the technical conditions under which cybersecurity technology should operate are constantly changing.

It should also be noted that changes affecting the security of the operating system and web browser may be made between the scheduled release dates of new versions and may involve unpredictable technical changes.

In addition, there are other elements in the formal-legal field [11] that we should consider, such as: international and national legislation, technical legislation, standards, norms, recommendations and internal company regulations.

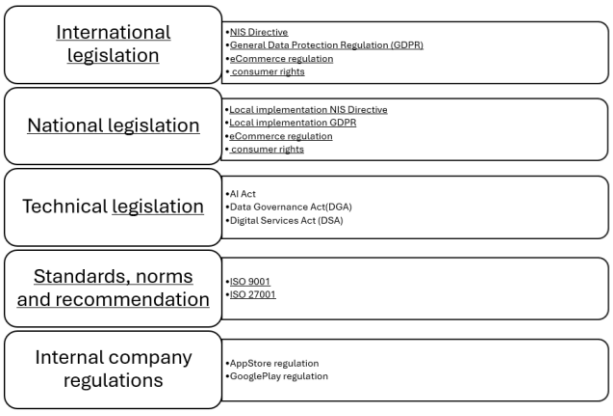

Figure 2: Formal layers

We are also seeing dynamic changes in the way criminals operate: variability of attack scenario and variability of tools.

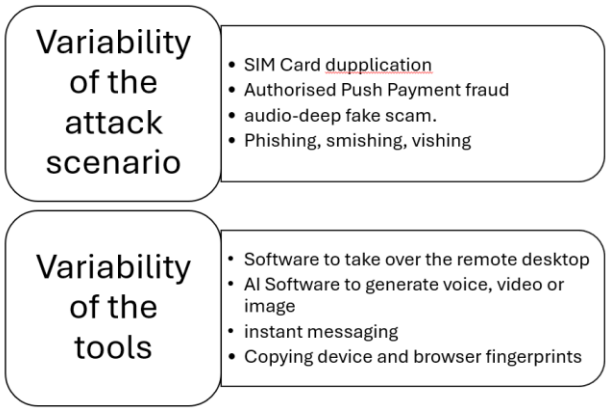

Figure 3: Criminal activity

And, of course, criminals are constantly identifying banking security techniques and bypassing or neutralising them [10].

We can think of cyber technology as a black box influenced by the forces of many independent parameters.

As in physics, the degrees of freedom (DOF) of a mechanical system is the number of independent parameters that define its configuration or state.

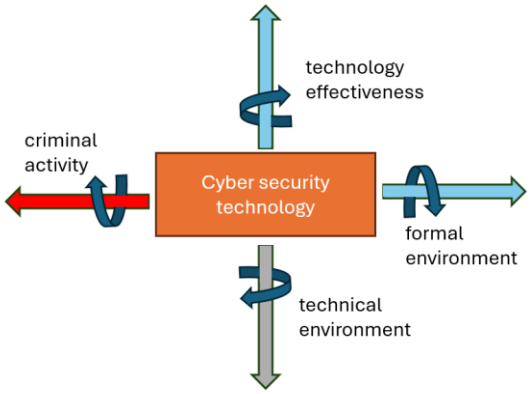

Figure 4: Forces affecting cyber security technology

A useful technology should be in balance between these parameters. If one vector increases, it means there's a need for action.

A multi-layered dynamic model of the variability of the environment is thus created, which seeks an equilibrium that includes the success rate of attacks. The stimulating (agonistic) factor is the activity of criminals and the antagonistic (inhibitory) factor is the development of security technologies. Another two parameters, which can be both agonistic and inhibitory, are changes in the technical or formal domain. Both can improve or reduce the effectiveness of cybersecurity technology. What is certain, however, is that all of these parameters create a need for constant review and adaptation of the technology.

4.2 The challenge of licensing

As a result, a solution developed in the laboratory will either start to fail immediately when deployed on the entire population, or it will start to fail over a finite period of time (as a function of time). This phenomenon has no risk characteristics, but is an inherent feature of the cybersecurity technology ecosystem.

The question is how to structure the process of technology transfer and licensing in this dynamic ecosystem?

In the process of technology transfer, we can distinguish:

1. Stage I - licensing the results of the R&D team and transferring them to the product development team (in this case software),
2. Stage II - advising the product development team on how to incorporate the innovation into the manufacturing environment.

Such an approach is not rational and will fail if we apply it to the transfer of cybersecurity technology.

This is because there is a high probability that the transferred technology will need to be modified before it is fully implemented in the product.

This will make the whole process infeasible and banks will start looking for non-IT methods to fight crime.

4.3 Practices applied

For technology transfer in the cyber domain, the NASK has adopted its own specific operating procedures.

First, the cybersecurity technologies developed in the NASK R&D teams are transferred to internal development teams.

By technology, we mean the form of a method, algorithm or learned AI model. The development team then builds a finished software component on top of it.

After that, the R&D team still, support and develop technology. The R&D teams are prepared for long-term development of the technology for detection of specific types of attacks, including its modification in the event of a change in the conditions of the technical environment in which the technology is to operate (e.g. loss of access to data relevant for detection).

Such organisation of technology production and preparation for transfer enables the temporary licensing of the finished software component, which allows the use of the cybersecurity technology for implementation in software. The license contains a number of specific conditions tailored to the cybersecurity ecosystem, the main ones are:

1. an assurance that the licensee will adapt the technology to changes in the technological environment,
2. an obligation on the licensee to improve the technology in the event of a decline in the effectiveness of attack detection,
3. an limitation of the licensor's liability for failure to adapt the technology to changes in the technological environment or to changes in the activity patterns of the perpetrators.

These points are almost impossible to define precisely. They are declarative in nature, with no strict guarantees from either party. The technology provider cannot reliably guarantee the effectiveness, cost or time it will take to modify its technology, and the recipient cannot guarantee the conditions under which it expects the technology to be effective.

In other words, the factor that determines the balance between the technology provider and the technology recipient is a common rational economic interest. And the basis for deciding on such a cooperation model should not be so much an assessment of the effectiveness of the technology at the time of its production, but rather the ability of the technology provider to modify and develop the technology to keep pace with changes in the application environment within a reasonable period of time.

5 Conclusion

The transfer of ICT technologies for cybersecurity may force a different way of thinking about building a collaborative model with business [12]. Thinking of collaboration with business as a one-off design phenomenon may prove to be a dead end. To ensure a steady flow of solutions for business in a rapidly changing environment, it is worth considering a process model of collaboration [4].

The example case study analyses the behavioral biometrics project and the AI technology used. However, the issue seems relevant to any application of technology or methodology in an unstable cyberspace environment.

The fundamental value of collaboration is to ensure the ability to solve a class of research problems within a reasonable time and cost. The process for sharing further technologies developed on the basis of the first project should be proposed in advance. The initial project or technology licensing is therefore only a starting point for long-term collaboration. It's also necessary to rethink the organisation of technology transfer agreements. Towards a collaborative framework and the definition of a dynamic research process.

For future work, it is possible to approach techniques to assist in predicting the effects of the changing environment.

REFERENCES

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[2] *Raport Roczny z Działalności Cert Polska 2023*, NASK 2023

[3] *Annual Report From The Actions Of Cert Polska 2022*, NASK 2023

[4] *Successful Technology Licensing*, World Intellectual Property Organization (2015), ISBN 978-92-805-2633-2,

[5] Lella I., Tsekmezoglou E., Theocharidou M., Magonara E., Malatras A., Svetozarov Naydenov R., Ciobanu C. *Enisa Threat Landscape 2023*, October 2023, ISBN: 978-92-9204-645-3

[6] Hogan M., Newton E, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, NISTIR 8074 Volume 2, 2015

[7] Troy E. S., *A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime*, August 2013

[8] Gargir Sarkar, Sandeep K. Shukla, *Behavioral analysis of cybercrime: Paving the way for effective policing strategies*, Journal of Economic Criminology, Volume 2, December 2023

[9] Phiri. J., Lavhengwa, T., Segooa M.A., *Onlinebanking fraud detection: Acomparative study of casesfrom South Africa and Spain*, South African Journal of Information Management 26(1), a1763., 2024

[10] Tapiwa Mazikana A., *Development of a Predictive Model for Online fraud Detection in the Banking Sector. Case Study of First Capital Bank*, Journal of Machine Learning Research, May 2024,

[11] Harnay S., Scialom L., *The influence of the economic approaches to regulation on banking regulations: A short history of banking regulations*, Cambridge Journal of Economics 40(2), April 2015

[12] Larsson B, Rolandsson B., Ilsøe A., Masso J., *Digital disruption diversified-FinTechs and the emergence of a coopetitive market ecosystem*, Socio-Economic Review, July 2023

[13] Chrome RoadMap, https://chromestatus.com/roadmap , 10.08.2024

[14] Firefox Release Calendar https://wiki.mozilla.org/index.php?title=Release_Management/Calendar&redirect=no, 10.08.2024

[15] Barbrich P., Nocoń B., *NetB@nk bankowość internetowa i mobilna, płatności bezgotówkowe*, Polish Bank Association Raport I Kwartał, 2024

[16] *2024 Report On Payment Fraud*, European Central Bank 2024

[17] Global Banking Fraud Index 2023, https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html , 18.09.2024