Streszczenie

W niniejszej pracy przedstawiono zagadnienia wykorzystania kilku rodzajów biometrii w zastosowaniach systemów autoryzacji i ochrony użytkowników. Szczególny nacisk został położony na biometrię sposobu pisania na klawiaturze - *keystroking* oraz wizualną biometrię twarzy. Przedyskutowano i zaproponowano mechanizmy ochrony tożsamości biometrycznej - algorytmy zamazujące prawdziwą tożsamość, algorytmy personalizujące dane biometryczne na rzecz ich odbiorcy, schematy osadzające nadmiarowe informacje w przekazywanym medium (*steganografia*) mówiące o pochodzeniu tych danych. Przedstawiono w rozprawie również systemy zapewniające prywatność użytkowników i silnie chroniące dane biometryczne. Zaprojektowano w tym zakresie także generyczny system do bezpiecznego weryfikowania danych biometrycznych oparty o operacje na zbiorach prywatnych i wykorzystujący protokół *Oblivious Polynomial Evaluation*. System ten zachowuje prywatność jego użytkowników oraz zapewnia ochronę danych osobowych *by design*. Bezpośrednio nadaje się do wdrożenia w rozwiązaniach kontroli dostępu - np. biometryczne zamki do drzwi.

Wszystkie rozważane zagadnienia analizowane były pod kątem wykorzystania ich na urządzeniach o ograniczonych zasobach obliczeniowych, pamięciowych i komunikacyjnych, takich jak karty elektroniczne *smartcards*, czy urządzenia mikroprocesorowe. Prowadzone badania były motywowane chęcią aplikacji uzyskanych wyników w rozwiązaniach przemysłowych, stąd duży nacisk położony był na kwestie implementacyjne i techniczne wykonalności projektowanych technologii. W ramach prac udało się przygotować zgłoszenie patentowe nr P.406507 jednej z opracowanych technologii pt. *Urządzenie do ochrony tożsamości biometrycznej, sposób jego działania i zastosowanie urządzenia do ochrony tożsamości biometrycznej użytkownika* złożone w Urzędzie Patentowym Rzeczypospolitej Polskiej w dniu 16.12.2013 r. Opracowano również i zgłoszono do ochrony w UP RP znak towarowy - *biometric KEYPRESS* pod numerem Z.440509 w dniu 23.03.2015 r.

Z przeprowadzonych badań i eksperymentów wynika bezpośrednio, że cechy biometryczne, które z pozoru mogą się wydawać niewystarczające do zastosowania w samodzielnych systemach rozróżniających poszczególne tożsamości, stają się bardzo wartościowe w połączeniu z innymi mechanizmami weryfikacji tożsamości. Zastosowanie biometrii jako drugiej linii obrony w systemach bezpieczeństwa komputerowego zdaje się być rozwiązaniem bardzo korzystnym z uwagi na znaczne podniesienie poziomu ochrony użytkowników i automatyzację procesu weryfikacji (przynajmniej wstępnego) przy jednoczesnym zachowaniu niskiego kosztu implementacyjnego. Istotnie, (właściwie każde urządzenie komputerowe posiada obecnie wbudowaną kamerę, mikrofon i interfejs klawiaturowy, zapewniające możliwość pobierania próbek i weryfikacji trzech biometryk: wizualnej - biometria twarzy, głosowej - biometria głosu i sposobu pisania na klawiaturze - keystroking. Przeprowadzone badania skuteczności systemów bezpieczeństwa korzystających z cech biometrycznych potwierdzają ich obiecujące – ponad 95% – wyniki prawidłowego funkcjonowania.

Przeprowadzone obserwacje rynku wykazują bardzo szybki wzrost rozwiązań

opartych o karty elektroniczne i związane z nimi elektroniczne dokumenty tożsamości. Wiąże się to z nowymi protokołami uwierzytelniania stron, ale również z zagrożeniami dotyczącymi kradzieży, klonowania i podszywania się pod użytkowników. Zapewnienie integralności danych warstwy fizycznej i warstwy elektronicznej samej karty oraz warstwy biometrycznej użytkownika karty pozwoliło na podnisienie poziomu bezpieczeństwa systemu kontroli dostępu opracowanego w ramach ninijeszej pracy.

Konieczność ochrony danych biometrycznych, jako danych szczególnie wrażliwych i posiadających własność rozróżnialności ich posiadaczy wydaje się bardzo istotna. Analiza literatury, istniejących rozwiązań technicznych oraz badania przeprowadzone w ramach niniejszej pracy zdecydowanie pokazują, że ochrona danych biometrycznych jest fundamentalna dla systemów bezpieczeństwa.

Niezabezpieczone dane biometryczne mogą stanowić poważne zagrożenie prywatności użytkowników i dawać możliwość podszywania się nieupoważnionych osób pod prawowitych klientów. Ochrona danych biometrycznych powinna być zapewniona już w procesie projektowania danego rozwiązania technologicznego, co wpisuje się w podejście *privacy by design* [6], *Doktrynę Cyberbezpieczeństwa Rzeczypospolitej Polskiej*[11] z 22 stycznia 2015 roku oraz stosowne dyrektywy Unii Europejskiej - *European Data Protection Directive 95/46* oraz *European Directive on Privacy and Electronic Communications Directive 2002/58/EC*. Wkrótce (2016/2017) wchodzi w życie nowe rozporządzenie Parlamentu Europejskiego dotyczące ochrony danych osobowych, wprowadzające ujednolicone przepisy na terenie wszystkich państw członkowskich. Zdefiniowano w nim explicite *dane biometryczne*, a także zaostrzono kryteria użycia danych osobowych, wprowadzono również wysokie sankcje karne za niedostosowanie się do procedur i przepisów. Wymagania te są nieco na wyrost, bowiem obecna praktyka w przetwarzaniu danych osobowych daleka jest od postulowanych zasad, zaś oferta rynkowa niezadawalająca pod kątem potrzeb.

Najnowsze trendy rynkowe wskazują, że rozwiązania oparte o mobilne urządzenia elektroniczne wypierają z rynku tradycyjne systemy teleinformatyczne. Na ich miejsce wchodzą urządzenia o ograniczonych zasobach, takie jak tagi NFC, beacony czy po prostu smartfony i tablety. Rynek wywiera na producentach konieczność dostarczania usług na miejscu i natychmiastowo, często zapominając o kwestiach bezpieczeństwa lub odkładając je na drugi plan. Za sprawą takiej przemiany technologicznej, to właśnie cyberprzestępcy stają się najbardziej niebezpieczną grupą i przed nimi należy się chronić. Biometria daje nam nowe możliwości obrony.

[11] www.bbn.gov.pl/ftp/dok/01/DCB.pdf, dostęp 05.04.2015 r.

Abstract

This work has considered questions of usage of several types of biometrics in authorization and user's security systems. Particular emphasis has been put on keystroking biometrics and visual face biometrics. Mechanisms of biometric identity security have been discussed, taking into consideration algorithms blurring true identity, algorithms personalizing biometric data in favor of the recipient, schemes placing excessive information in the given medium *(steganography)* providing information of the rightful owner or the source of the data. The work has also described systems which ensure privacy of the user and strongly protect biometric data. It was designed generic system for verification biometric data based on private sets calculations and *Oblivious Polynomial Evaluation* protocol. This solution is privacy preserving system and provides data protection *by design*. It is ready to deploy in access control area - for instance biometric door locks.

All of the considered questions have been analyzed for their usage in devices with limited processing power, memory and communication, such as electronic smartcards or microprocessor devices. Since the conducted research was driven by the desire to utilize the acquired results in industrial solutions, particular emphasis has been put on questions of implementation and technical issues of feasibility of the designed technologies. In the process, the patent application P.406507 was prepared for one of developed technologies under the name *Device for biometric identity protection, its mode of action and use to protect the biometric identity of the user* and submitted at the Patent Office of the Republic of Poland on December 12th, 2013. A trademark application - *biometric KEYPRESS* - was also designed and submitted at the Patent Office of the Republic of Poland on March 23rd, 2015 with number Z.440509.

The conducted research and experiments show that biometric features, which on the surface can appear insufficient to be used in independent systems of distinction of particular identities, can prove very useful while utilized with other mechanisms of identity verification. Using biometrics as the second line of defense in computer security systems appears to be a very advantageous solution in view of significant improvement of the user's security level and automation of the verification process (at least the initial one) with simultaneously ensured low implementation cost (virtually all computer devices nowadays have built-in cameras, microphones and keyboard interfaces which enable sampling and verification of the three following biometrics: visual - face biometric feature, audio - voice biometric and the individual's way of using the keyboard - keystroking). The conducted research of effectivity of security systems utilizing biometric features has proven their promising results of correct functioning - over 95%.

The carried out analyses have shown a very quick increase in solutions based on electronic cards and electronic IDs connected with them, which in turn is connected with new protocols of website authorization, but also with danger of theft, cloning and identity theft. Therefore, a very significant conclusion drawn from this work is the need to ensure the integrity of physical layer data

and electronic layer data of the card itself, as well as the integrity of biometric layer data of the card user. It has been also proposed a system supporting realization of the demand for checking access permissions for particular resources with the use of electronic cards - access control of e.g. a building entrance. The need to secure biometric data as particularly sensitive data distinctive for every individual user seems to be very vital. Analysis of literature, available solutions and the research conducted in this work shows that such a protection is fundamental for security systems.

Unsecured biometric data can pose a serious threat to users' privacy and enable unauthorized individuals to pose as legitimate customers. Biometric data protection should be ensured as early as in the process of designing a particular technological solution, which fits in the *privacy by design* approach [6], as well as in the *National Cyber Security Strategy* [12] and appropriate *European Union directives: European Data Protection Directive 95/46* and *European Directive on Privacy and Electronic Communications Directive 2002/58/EC*. Soon (2016/2017), a new European Parliament regulation concerning personal data protection, unified for all member countries, shall enter into force. It defines biometric data and tightens the criteria of personal data usage, simultaneously proposing criminal penalties for failing to adjust to the procedures and regulations. These requirements are little bit exaggerated, because current practice in personal data processing is far from proposed rules, and market offers definitely too less in terms of needs.

The latest market trends show that solutions based on mobile electronic devices are displacing traditional communication and information systems. Instead, there appear devices with limited resources, such as NFC tags, beacons or simply smartphones and tablets. The market urges producers to provide services right here, right now, often neglecting or completely ignoring security measures. Owing to this technological change, it is cybercriminals who pose the most serious threat, and users should be protected against them. Biometrics provides new ways of ensuring this security, so it is advisable to make use of them.

[12] www.bbn.gov.pl/ftp/dok/01/DCB.pdf, access 05.04.2015 r.