CYBERSECHUB

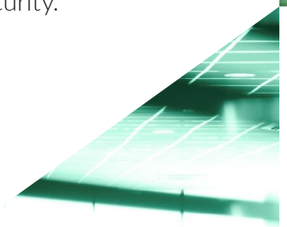
INNOVATION BOOK

KRAKOW

WHAT **WE** DO?

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum - CYBERSEC, one of the main public policy conferences on cybersecurity.



One of the initial projects run by our platform is CYBERSEC Accelerator which helps ICT and cybersecurity startups and SMEs from Małopolska to reach international markets. In the run-up to the project, an expert panel selected 7 of the most innovative businesses amongst the applicants. The Accelerator has been officially launched during the 2nd European Cybersecurity Forum - CYBERSEC 2016. In this Innovation Book you will find unique products and services offered by CYBERSEC Accelerator participants.

THE KOSCIUSZKO INSTITUTE

Do you know that by 2040 artificial intelligence will be as smart as humans?

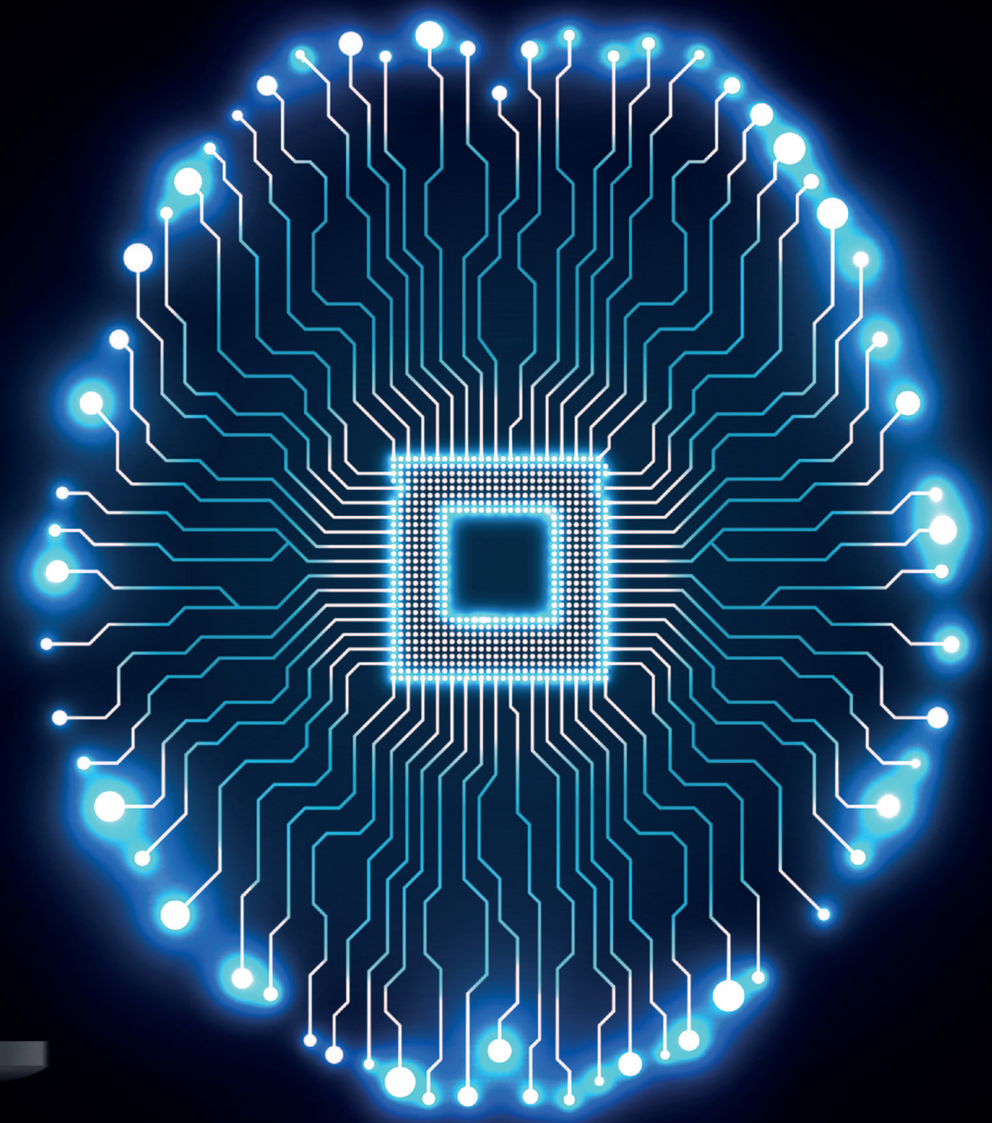
Using technology based on deep learning algorithms we are creating a new category of software.

- It learns from business data using **machine learning**
- Communication with user based on **context**
- Combine real GUI elements with **conversational interface**
- Deliver **push notifications** at the right time

2040.io

ul. Podole 60 Krakow, PL
Contact us at info@2040.io

A.I. for your business



www.2040.io

CS HUB

CYBERUSLABS

FROM SILICON VALLEY TO POLAND

Cyberus Labs, Sp.z.o.o. is a new kind of Polish company that is global in its DNA. Co-founded by Silicon Valley and Polish entrepreneurs, Krakow-based Cyberus Labs is cybersecurity startup that is introducing innovative cybersec products to the Polish and European markets. At Cyberus Labs we have chosen not to “patch a leaking ship” but to bring a new approach to some vexing security problems.

Founded by George Slawek (CEO), Jack Wolosewicz (CTO) and Marek Ostafil (COO), the company has right from the beginning set its own course - to focus on eliminating cyberthreats, and to deliver solutions that will be both secure and easy to use.

PASSWORDS ARE A BROKEN SYSTEM

The use of passwords is a broken system. This has been known for many years, however, we have struggled to find a good alternative to this ubiquitous user authentication system. Companies are vulnerable to data theft of credentials while users struggle to create, remember and input dozens of username/password combinations just to manage daily online life.

To date, alternative user authentication methods such as biometrics have had limited success in the market place for two key reasons:
1. privacy/security concerns (e.g. theft of user biometric data)
2. poor user experience.

The reality is that the username/password login method is still by far the most popular user authentication method. As a result hackers or other bad actors continue to find ways to steal user credentials through ever more sophisticated data breaches. It is estimated that over the last 5 years approximately 1.5 Billion sets of user credentials have been stolen, almost half a billion alone from the 2014 Yahoo data breach announced 2 years later in September 2016.

As Michael Chertoff, former head of US Homeland Security, recently stated, “A closer examination of major breaches reveals a common theme: In every “major headline” breach, the attack vector has been the common password. The reason is simple: **The password is by far the weakest link in cybersecurity today**.”

A DIFFERENT APPROACH

Cyberus Labs has taken a different approach to finding a solution to the user authentication challenge and dilemma – the right balance between the need of the user to have a fast and convenient way to log into their online account and the need of the company to have a secure and effective user authentication system. **At its core is the elimination of the username/password combination as a user authentication methodology**.

The result of our 3 years of research and development in Silicon Valley, CA and in Poland is the CYBERUS KEY password-less logon platform, formerly launched in September 2016 at the Kosciuszko Institute’s CYBERSEC Forum 2016 conference in Krakow, Poland.

CYBERUS KEY is password-less logon and authorization platform that the user accesses their online account by activating the Cyberus Key mobile application on their smartphone and with one-click logs into their banking or e-commerce account on their laptop.

The user is authenticated without any username/password or any “actionable” data being used or transmitted at the time of logging onto their account. In other words, there is nothing for hackers to steal.

A PASSWORD-LESS WORLD

CYBERUS KEY enables a user to securely logon to any web service (for example: banking, e-commerce, e-health, media platform) using a preinstalled application on a mobile device by securely transmitting an audio signal between the device and the web service via a laptop or another mobile device – authenticating that user’s credentials instantly and securely by generating an “unbreakable” short-lived unique onetime password.

The technology of generating and transmitting a one-time-password by the use of the audio signal makes the Cyberus Key system highly secure because:
c) no useful or actionable data for cybercriminals to steal.
d) the characteristics of the audio signal used for user authentication makes it impossible for cybercriminals to compromise.
e) short-lived (few millisecond) one-time password expiration prevents cybercriminals from intercepting or reusing.

The benefits are both on the user side and on the operator’s website side. The user will no longer need to remember and type in user names and passwords - a tedious, inefficient and inherently insecure method of user authentication.

CYBERUS KEY patent pending technology disintermediates the interaction between users and websites, bypassing User ID/Password requirements currently used for authentication.

CYBERUS KEY creates a truly secure log on experience and verifies both sides of an on-line transaction, eliminating the risk phishing, key-logging, “man-in-the-middle” or “man-in-the-app” types of cyberattack.

CYBERUS KEY gives users fast, single touch and secure access to their on-line accounts. There is no more need of costly FOBs, Tokens, SMS’.

CYBERUS KEY offers additional integrated security measures via multi-factor authentication such as biometrics, for high-value, high-risk transactions. The system is fully customizable to meet the specific needs of financial services, government, e-commerce and many other sectors. CYBERUS KEY is also delivering new marketing/sales channels with highly targeted offers to mobile app users in real-time on a 2nd screen.

CYBERUS KEY can be Cloud/SaaS or client-side “on-premise” installation.

THE FUTURE

Automated systems of connected devices in Internet of Things (IoT) e.g. “smart homes” systems -connection of household appliances, air conditioning, heating, power, light, entertainment etc. is a fast growing market. CYBERUS KEY will offer user-to-machine and machine-to-machine authentication solutions ensuring effective authentication and authorization.

CYBERUS KEY proposes a mechanism which will add IoT device identification, authentication and will govern the types of interactions which can be legally performed by devices and to allow only authorized actions to be undertaken by IoT devices.

CS HUB

exnit
experts in information technology

INFORMATION IS IN THE CENTER OF EVERYTHING WE DO.

STORE

Are you aware of the place where your information starts and transforms? Is it in your private or public Cloud, or maybe it is in your employees' mobile devices? Do you control how your data is stored and managed?

First thing about the digital information is the place where it lives. Providing safe and effective space, and tools for managing growing volumes of data is essential when thinking about security.

How can we help?
We plan, design and implement advanced architectures for storing and processing data. We think about information as the process that needs to be protected and managed.

BACKUP

Next step in protecting your data is making a copy but in fact the most important thing in backup and archiving data is restoring it. What is more, effectiveness and ease of use should be the „must have" feature of backup solution. If you look forward backup as a service seems to be the most optimal way to provide effective protection for your data.
Do you have a backup policy? Do you test and verify your backup regularly? Do you spend hours and days on managing and enhancing backup solutions?

We can help you by:
- providing advanced consultancy services helping customer to implement best backup and archiving plans and politics,
- taking care of existing backup environments by enhancing and modernizing backup,
- providing BaaS (backup as a service).

BUSINESS CONTITUITY

When your important information in unavailable your business looses. The consequences may be diverse from company image deprivation, through operational outage, financial loss up to total disaster.

Imagine the possibility to work constantly, recover in fast, simple way to the picked point in time despite of the disaster range.

We think about disaster recovery plan as the insurance for your information. We can help you design a high availability solution that best fits your needs and value of your data. Depending on your company's profile we can implement DR on premise, in a Cloud, or as a Service.

SECURITY

Today's threats forces organizations to protect data in the diverse way. You need to manage and monitor your data from the beginning, defining and controlling the access outside and inside the organization, protecting your data from accidental as well as intentional danger.

Our advanced consultancy services can help you to point the most vulnerable areas and to design the consistent policy in area of data security.

EDUCATION

Continuous learning is the best way to stay up to date with dynamic technology growth as well as threats expansion.

We provide broad portfolio of authorial courses that helps IT Professional to develop their knowledge and competences.

It is obvious that you care about your information.
The case is how you provide this care.
Use our experience to make it sure.

Contact us at www.exnit.com and www.eduexnit.pl

CS HUB

securing

MORE THAN SECURITY TESTING.

WHAT WE DO?

Founded in 2003. Since then we have supported leading banks, insurance companies, telecom providers, government institutions and software houses, providing services such as:

- **Application and infrastructure security testing**
- **Code review**
- **Definition of security requirements**
- **Project review**
- **Education**

KEY FACTS:

- Founded in **2003**
- Over **450 successful** security assessments in **17 countries**
- More than **150 critical vulnerabilities** identified and removed
- Verified systems manage critical infrastructure and process **millions of users' records**
- Our research has been selected for leading security **conferences worldwide**
- **Customers:** Banking, Insurance, Fintech, Software Houses, SaaS Vendors, Telecommunication, IT, Utilities, Industry, Public, Military

WHO WE ARE?

Team of experienced application security consultants. We are focusing on security aspects of applications and IT systems. Our expertise covers different kinds of applications (e.g. electronic banking, electronic payments, FOREX, e-commerce, home/office automation, surveillance, voting, internet of things, etc.) and wide spectrum of technologies (web, mobile, WebServices, embedded, desktop, SaaS, cloud).

We are constantly improving our skills and knowledge in order to stay on the edge of information security issues. This allows us not only to focus on past and current risks but also to look forward into the future. Examples of our research topics include: transaction authorization systems, banking malware, home automation, M2M communication, Bluetooth Low Energy, browser plugins, pull-print systems, proprietary protocols, HTML5 and many more.

KNOWLEDGE:

We are sharing our knowledge on many conferences and meetings. Our research topics has been chosen for leading security conferences worldwide such including: Black Hat USA 2016, OWASP AppSec Europe 2014-2016, Infosecurity Europe Intelligent Defence 2016, CONFidence Krakow 2014-2016, ZeroNights 2015, BSides London 2015, Black Hat Asia 2015, PH Days Moscow 2014, HITB Amsterdam 2014, Internet Banking Security Warsaw 2013, BruCON, Belgium 2012, Black Hat USA 2012 and OWASP, ISACA, ISSA meetings.

OUR APPROACH TO APPLICATION SECURITY TESTING:

The goal is to fix vulnerabilities.

- Our report always includes recommendations on how to fix discovered vulnerabilities.
- Support during fixing phase.
- We communicate with the tested solution vendor to help them understand problem and provide remediation.
- Additional tests after vulnerabilities are fixed.

The main aspect of security assessment is to take real risk impact into account.

- Prior to testing, we perform threat identification and threat modeling.
- We prioritize attack scenarios.
- We take into consideration business impact as well as business logic.

We say no to fire and forget tools.

- Automatic tools can only find small percentage of real vulnerabilities.
- The real threat is live attacker, not automatic tool.
- We prefer manual verification, using specialized "home-grown" tools.
- Understandable, customer-oriented report.
- Realistic and dedicated recommendations.

Deep technical knowledge and audit skills.

- We stay on the edge of new attack techniques and areas (own research, 0-days, worldwide conferences).
- We are certified experts of ITsec management and audit (CISSP, CISM, 27001, PCI DSS, ...)

MORE THAN SECURITY TESTING:

Security testing at very end of the project, just before (or after) deployment are still key component of achieving application security. Nevertheless, doing only security tests as a part of UAT is not effective, because significant costs of fixing bugs at late project stages. That's why besides security testing, we offer support at each stage of development:

- Security training for developers and QA team
- Security requirements definition (functional and non-functional)
- Project reviews
- Code reviews
- Consultations
- Security tests

CONTACT:

info@securing.pl
tel: +48 12 425 25 75
fax:+48 12 425 25 93
www.securing.pl

Sher.ly is a SaaS data smart syncing & collaboration service for business. It delivers a new way of sharing your sensitive files with your co-workers and business partners by creating a secure, invite-only network on demand. It works like a cloud, but all the data stays on your own storage.

ABOUT SHER.LY

Sher.ly is a startup launched in 2013 dedicated to creating innovative software for file sharing among business organisations, on both desktop and mobile devices. The main development centre is based in Krakow, Poland. The company gained traction in June 2014, mainly thanks to a crowdfunding campaign on Kickstarter. The financial target was met in 223% and Sherlybox became a huge success even before hitting the market in August 2015.

We offer you the Sher.ly application, for secure and fast data sharing, as well as the Sherlybox device - the embodiment of a private and secure storage cloud for your files, available 24/7.

HOW THE IDEA WAS BORN?

It all started with two friends who were passionate about new technology – Blazej Marciniak and Marek Ciesla. They met and worked together at Veracomp in Krakow, one of the biggest IT distributors in Poland. Before Sher.ly, they created new technology for safe data transmission over the Internet, called VPN. In further development, the idea has been extended by observing users' behaviour, especially related to storing and downloading files from the Internet.

SHARE & SYNS FILES SECURELY DIRECTLY FROM YOUR DEVICE

Sher.ly delivers a new way of sharing files with your co-workers and business partners, directly from your computer or other devices, by creating a secure, invite-only network on demand.

Sher.ly is a perfect and fully secure alternative to public cloud solutions like Dropbox, OneDrive, Box, Apple Cloud Drive or Google Drive because the data is not uploaded to any external servers. With Sher.ly, you create your own virtual drive, an unlimited cloud using the hard drives in your devices. For this reason, you don't pay for any storage capacity in the cloud.

The application uses the latest secure encryption protocols for file transfer and allows you to track the full history of sharing files with individual users. With this solution, the owner of the file has full control of data confidentiality and can control the identity of the recipients right away.

The files are immediately visible in your Sher.ly app thanks to intelligent metadata synchronisation, which allows you to set preferences for sync and access depending on project you've created, device you've used, file name, file size, modification date or sharing party. There are no bulk uploads and downloads, no data size limits.

When a user device goes offline, e.g. a laptop sleeping to conserve power, it's vital for data availability to have always-on networked storage with Sher.ly software on it. You need a physical storage device to keep your data. That is why we invented the Sherlybox storage device.

SHERLYBOX, YOUR PERSONAL CLOUD, DESIGNED AND BUILDT FOR SHARING FILES

This unique storage device, powered by Sher.ly software, gives you freedom to share files even when your computer is offline. Sherlybox embodies the vision of your own secure cloud for files, available 24 hours a day.

Anyone can install and instantly use Sherlybox. With just a touch of a finger, pairing is done with any device, and three seconds later, you receive secure, unlimited access via Sher.ly app and start a whole new experience of collaboration. Sherlybox is fully compatible with Sher.ly app which mediates and establishes network connections and allows you to work from outside the office in the same secure way like from inside. The data is fully protected, only accessible to authorised users, thereby limiting the data leak risk factor to virtually zero.

Storing data is not enough, Sherlybox's main functionality is to share it, yet separating the data access from device access.

UPGRADE YOUR BUSINESS COLLABORATION TO THE NEXT LEVEL

Sherlybox and Sher.ly Software give organisations the freedom to share any file, with anyone, anytime. Each organisation, each department, each team now has complete control over who, when, and how sharing is done. Sher.ly removes the boundaries of team collaboration.

We are moving far beyond simple file sharing. Our main goal is to create a complete management platform for sensitive data being shared in business, which will facilitate secure & smart workflow across internal teams and external clients.

hello@sher.ly | @sherlyfiles | www.sher.ly | www.sherlybox.com

TECHMO

Techmo is a spinoff of AGH University of Science and Technology in Krakow, Poland. The company implements solutions in the field of audio, speech and language technologies. It was formed by qualified specialists from AGH UST. Techmo focuses on allowing voice control of devices to become more widespread. Currently, it is involved in providing technology for IVR (Interactive Voice Response) solutions for customers such as Energa or Fortum. Techmo cooperates also with Pacific Voice & Speech Foundation from San Francisco in order to build technologies for logopedic applications. Techmo is also conducting project “Integrated system for supporting the teaching process for the purposes of raising the efficiency of operations in KSRG domain” where is responsible for spatial audio simulation and physical effects simulation. The project aims at building a firefighters training simulator using Unity engine and Oculus Rift.

TECHMO - MAKING EVERY VOICE MATTER

Just think about how much easier life would be if we could control everything around us by voice. Talking is the natural way of communicating for most people in the world. Not clicking, not touching - simply speaking. Thanks to Techmo’s solutions, voice can be used for various purposes, including electronic device control, speaker identification (biometrics), 3D sound simulation, and automatic speech recognition. Users no longer have to remember their PIN codes or passwords. It’s enough that they speak in their own voice and they will access their accounts quickly and easily. It’s safer than using fingerprint too! As a university spin-off, Techmo is run by some of the greatest minds in the field of voice technologies. Its technologies have been implemented in a few of the biggest Polish companies and now Techmo is reaching out to global customers. All you need is voice.

VOICE COLOR - SPEAKER VERIFICATION AND IDENTIFICATION

Widely used standard process of identification and verification using password or PIN code is not only uncomfortable for customers, but also expensive for a company. Every call to helpline is connected with necessity of finding or recalling PINs or password and then entering it to the system. It takes time of customers as well as Call Centre consultants.

Biometric voice identity verification with IVR system allows shortening of user identification time more than 4 times and rising the authorization security level at the same time. In contrary to the password, which can be stolen, our voice is our unique property similarly to fingerprints or iris. It is guaranteed that customers’ data are properly secured and access to them is quick and comfortable.

The Voice Color allows remote authorization of access to services and resources offered through teleinformatics channels:

- phone calls (including GSM)
- VoIP internet telephony
- Internet
- mobile applications
- info-booths.

Identity verification does not require memorization of password or PIN - the password is a user’s voice itself!

Registration for verification involves speaking 4 times a short phrase - biometric password, which will be used for verification. All users uses the same phrase, for example “I confirm my identity”. It is possible to adjust the text of biometric password to the needs of particular deployment. In case of identification any content of the recording is allowed but it has to be longer.

SARMATA 2.0 AUTOMATIC POLISH LANGUAGE SPEECH RECOGNITION

Automatic Speech Recognition (ASR) systems are becoming increasingly more popular, even for languages with fewer native speakers (around 60 million worldwide for Polish). Our ASR system aims to work in a difficult environment. It is designed to recognize short phrases or single word commands in Interactive Voice Response (IVR) systems over telephone.
Our system supports context free grammars in form of Speech Recognition Grammar Specification (SRGS). It is a W3C standard, and is widely used in commercial systems. Decoding words with grammar allows the decoder to prune phrases that do not belong to a given formal language.

Fast

Case	#Words	Speedup
Numbers	1000	7,7x / core
Streets	1300	5,5x / core
Towns	265	6,7x / core
Commands	50	26,5x / core

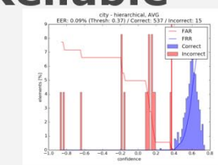
Accurate

Case	Samples	Rate
Numbers	5600	98,4%
Streets	12000	99,1%
Towns	500	99,2%
Commands	4900	98,5%

SARMATA Speech Recognition System

KALDI

Reliable



Easily integratable

- GRPC
- MRCP v2
- Propietary protocol
- C++ / Java clients

Industry standards

- SRGS
- Semantic Interpretation

Biometry is the safest and the most convenient tool of authorization. This is how people recognize each other. Biometric features cannot be lend, stolen or forgotten and their falsification is practically impossible. Until now the barrier to the wider usage of voice biometry technology was high price of implementation and lack of solutions for fields other than telecommunication.

Both in Poland and in the whole world the market of Automatic Speech Recognition (ASR) technology and biometric voice verification (BVV/BVR) is a growing market. Current share of voice verification in the world market is little more than 4% amongst all biometry solutions. Not very high level of market penetration by speaker recognition and verification systems is affected by two basic factors: small number of efficient solutions and high price of licences for BVR/BVV modules. Helplines and voice systems market is a huge one, which is constantly open for new functionalities that increase customer satisfaction, improve security and lower the exploitation costs.

VoicePIN.com is a voice biometrics producer that developed a software for voice authentication for any application. Founded in 2011, Voice PIN replaces traditional passwords and pin numbers with natural voice commands. Its SaaS technology has been used by corporate customers from ING to Alior Bank and made it to the Top 10 at TechCrunch Disrupt competition in San Francisco last year. The Polish company, based in Cracow, is expanding in an emerging market and is focusing on the global development of the business by building a chain of partners on all continents. In 2016, Voice PIN opened a branch in Silicon Valley with plans to open others.

GET TO KNOW VOICEPIN

VoicePIN is the latest tool in biometric technology and speech recognition for data protection. Your clients and users can log on in a convenient way, without the need to remember PINs and passwords. User verification becomes amazingly simple. Natural voice commands are all that is needed. VoicePIN minimizes the risk of frauds and personal data theft. The human voice is as unique as a fingerprint. VoicePIN saves you money by shortening client service time as well as enhancing the service and clients experience.
Thanks to our API, connecting VoicePIN to any mobile application, website, Call Center system, or an IVR is as simple as can be. VoicePIN can also be applied wherever there is no keyboard – in the dynamically developing Internet of Things.

The innovative technology enables voice recognition to be used for verification, access control, fraud detection and other security protection. It can be implemented on mobile apps and at call centers, helplines, websites and anywhere password-protected information exists. No automatic speech recognition software or hardware is needed therefore installation is fast and it's easy to use.

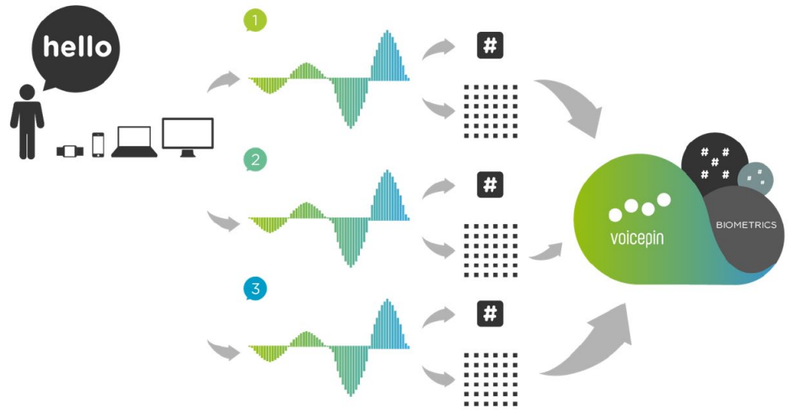
VoicePIN can be used to login, authorize transactions, reset passwords and perform many other security functions.

As the latest tool in biometric technology and speech recognition for data protection, users can log on conveniently without needing to remember pins and passwords. Natural voice commands minimize the risk of cyberattacks and personal data theft because the human voice is as unique as a fingerprint which is carefully analysed and detected through Voice PIN's cutting-edge technology. Upon initial installation, a user registers a "voiceprint" which is stored in the form of mathematical models. Each time the user attempts to access protected information, the command is compared to registered voiceprints and the software verifies whether the voiceprint belongs to the user who registered it. Since individuals are identified by analysis of the voice, Voice PIN is a safer and less complicated alternative to traditional methods of authentication.

Voice PIN can be used to login, authorize transactions, reset passwords and perform many other security functions which is why the tool is currently being used in the financial sector, insurance industry and telecommunications. Businesses can subscribe to Voice PIN as-a-service and enhance their customers' user experience by providing hands-free authentication without logins or passwords. API integration is simple and does not require an installation process and can be used on multiple channels. This solution is the most cost-effective while providing high-level security.

While no biometrics tool can provide 100 percent safety, according to the company, Voice PIN is 98-99 percent effective. Passwords, pins, security answers can be obtained by unauthorized users but voice biometrics is good at detecting attempted fraud and provides a higher level of security than even more methods such SMS authorization.

Even though VoicePIN, in order to guarantee top-level security, uses complex, advanced technology, registration process takes about 15 seconds and the verification just 3 seconds!



A software producer invented a tool that enables users to login and verify their identity using only the sound of their voice.

WANT TO KNOW MORE?

Feel free to contact us:
VoicePIN.com
Krakusa 11 St.,
30-535 Cracow
+48 12 378 98 21
info@voicepin.com
TT: @VoicePINcom

CYBERSEC 2017

The 3rd Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

STAY TUNED!

WWW.CYBERSECFORUM.EU

ONE MARKET
ONE JOURNAL
MANY POSSIBILITIES

WWW.CYBERSECHUB.EU

KRAKOW

YOUR PLACE TO INVEST IN CYBER

CYBERSECHUB.EU
CYBERSECHUB@IK.ORG.PL
THE KOSCIUSZKO INSTITUTE
UL. FELDMANA 4/9-10 31-130
KRAKOW, POLAND
+48.12.632.97.24