CyberusLabs

ELIoT Pro White Paper Series: Part 1

The “broken system” and the dawn of the New Era

WHY TACKLING THE CREDENTIALS CULTURE IS THE FIRST STEP IN DELIVERING SAFE AUTHENTICATION IN AN ERA OF RISING CYBERCRIME

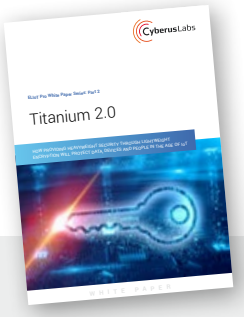
WHITE PAPER

A note on the ELIoT Pro White Paper Series

The ELIoT Pro four-part white paper series identifies the four key elements of a true and pioneering end-to-end cyber security solution for the fast-growing world of IoT.

In Part 1,

we consider the issues associated with using password-based credentials for Human-to-Machine (H2M) authentication and the move into the post-credentials era.



Part 2

explores Machine-to-Machine (M2M) authentication, including the problems associated with designing cyber security for IoT devices.

Part 3

examines the need to set rules to monitor the behaviour of an IoT device, track its performance and to detect malfunctions.

Part 4

discusses the importance of Just in Time device upgrades and replacements to keep IoT systems fully operational.

Table of Contents

Executive Summary

For too long, we have put up with the password as our solution to authentication and how we confirm our identity in order to gain access to services, information or functionality. By depending on static user credentials like passwords, PIN codes, and even fingerprints, we are leaving a trail for cybercriminals to follow and this approach has seen technology after technology fail to keep identities secret and users secure.

EXISTING AUTHENTICATION TECHNOLOGIES ARE NOT SECURE

From passwords and biometrics to smart tokens and password mangers, these technologies are simply not secure, and often cumbersome to use. Additionally, this dependence on credentials has resulted in major adverse impacts on businesses, brands and people, the world over.

Today, through cyber security techniques like phishing, man-in-the-middle attacks, and regular data theft, the consequences of poor security are there for all to see.

Tomorrow, with the advent of quantum computing, Public Key Infrastructure (PKI) the most widely used framework for secure and trusted authentication, will be under threat because of quantum-based computational power will break Public Key encryption.

Any new approach must be developed with current and future challenges in mind.

INTRODUCING PASSWORD-FREE USER AUTHENTICATION

What can best be described as the 'post credentials era' in cyber security is fast approaching. Cyberus Labs has recognised this and developed a password-free user authentication platform. This layered cybersecurity solution is based on the use of highly secure symmetric encryption, short-lived one-time-codes, out-of-band and ultra-sonic communication, eliminating the risk of stolen credentials and makes systems more secure than ever before.

Already being used by people in banking, finance, ecommerce, and other high risk/high value use cases to authenticate their identity with service providers, this new approach has the potential to revolutionise how we as human users authenticate our identities with machines.

As IoT becomes firmly established, this technology can be the first building block in a holistic solution dedicated to taking on the IoT security challenges that lie ahead: a core platform tackling both Human-to-Machine and Machine-to--Machine authentication.

It’s high time to authenticate users securely and easily

As we enter a new phase of even greater connectivity with the growth of IoT, associated security risks are growing exponentially.

For decades, when it came to User Authentication (UA), we have applied short-term fixes like passwords to protect information, systems and devices. In our popular culture, from early playground games to spy movies, the password was considered a safe and easy way to authenticate people. But times have changed.

Technologists worldwide are slowly but surely recognising the password for what it is – an outdated, cumbersome and unsafe approach belonging to the dark ages of computing.

THE CURSE OF CREDENTIALS

Credentials and more specifically, how we check credentials are at the core of user authentication. Our information systems and infrastructure are jam–packed with valuable passwords, user names and other identifiers that have all proven to be too tempting and accessible for even the average cyber-criminal.

In any situation where credentials are static or where they can be remembered, accessed or intercepted, they can also be stolen and reused. In today’s world, we login several times a day to read newspapers, access banking services, drive cars, and so much more. With more and more of our lives moving behind digital walls and fences and with greater connectivity thanks to the arrival of IoT, a new approach to user authentication is now more important than ever.

From the humble password itself to updated variations on it, there have been many attempts to optimise user authentication, making it truly fit-for-purpose. Unfortunately, these methods are prone to security flaws and poor user experience, simply compounding the overall UA problem.

CURRENT AUTHENTICATION METHODS ARE NO LONGER FIT-FOR-PURPOSE

Passwords - the fact that most of us use passwords that are easy to remember means that by their very nature, passwords are often relatively easy to guess. Research tells us an alarming amount of people still use incredibly simplistic passwords and codes ranging from '1234567' to 'qwerty', and even 'password'[1].

It must also be considered that many people use the same or simply make up other passwords using a simple variation of their old password across multiple online accounts. This makes users extremely vulnerable when hackers steal credentials from one company and are able to use the same credentials across multiple sites.

In user experience terms, tedious password recovery processes add to the frustration of users and cost to the company and the circle continues as we are encouraged to develop passwords so complex they are impossible to remember by mere mortals.

Biometrics – for centuries, people have authenticated each other based on knowing what they look like and how they sound. In later years, the uniqueness of fingerprints has enabled a more enhanced version. The use of biometrics can provide powerful security as a single authentication factor in a multi-factor authentication system , but it has significant flaws.

Biometics can be stolen: Even though biometrics depends on a unique aspect of our physiology like a fingerprint, facial image, or voice print, biometric data is still stored as a file that can be stolen. Once a fingerprint or other biometric profile has been stolen the user has lost that option for ever. Additionally, technology is developing at an incredible rate in fields like 3D image modelling and voice modelling, making biometrics easier to falsify and work around.

Biometic technology is still early: Biometric solutions are highly sensitive and are prone to report false negatives – creating frustrated users or false positives – creating major security risks.

[1] https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

SMS and Software Tokens – Often used as second-factor authentication (also known as 2FA) they are methods of confirming users' identities through a combination of two different factors. SMS and software tokens are among the most commonly used forms of 2FA. But they are a poor user experience and can be digitally threatened by computer viruses and software attacks. SMS 2FA has proven so insecure that the EU and EU banking regulators have recommended not using it[2].

Hardware tokens – These cryptographic tokens are physical devices which authorized users are given to authenticate themselves. They are used in addition to, or in place of, a password to prove that the user is who they claim to be. Think of it like an electronic key that's used to gain access.

These solutions require that users have a second device (the hardware token itself) to be able to authenticate themselves. If you forget to bring your token, you cannot login. Additionally, in many implementations, the user must activate the token which generates a number that then must be typed into the website or mobile app to log in. Unfortunately, tokens are often small devices that can easily be lost or stolen and even though they are seen as very secure devices, they are not immune to hacking.

Password Managers - these software applications are online services which assist in generating and retrieving complex passwords, often storing such passwords in an encrypted database or calculating them on demand. As we gather more devices and logins, Password Managers have certainly gained in popularity.

Unfortunately, this has now snow-balled the key risk into one big exposure. People still depend on one master password to access the rest of their passwords. This makes the use of these tools particularly dangerous and still leaves the user at the mercy of recovery procedures should they lose or forget that all-important master password.

For many years now, user authentication has meandered along an uncertain road, developing short-term patches and quick fixes to major security issues. This credentials-first era of IT security has seen breach after breach with personal details and company information being exposed to great risk - resulting in serious consequences for businesses, their customers and society overall.

[2] https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication

Unintended Consequences of a credentials culture

IN THE LAST DECADE, SOME OF THE WORLD'S BIGGEST BRANDS HAVE HAD MILLIONS OF USER NAMES AND PASSWORDS STOLEN

- **LinkedIn** - 117 million
- **Dropbox** - 80 million
- **Sony Playstation** - 77 million
- **Marriott Hotels** - 500 million
- **Ebay** - 145 million

..and many more

Table 1.0

Poor UA technology and methods like those referred to earlier have very serious consequences for us all. Theft of data, including logins, passwords and credentials is hitting epic proportions. In 2016, it was reported that around 95 passwords were stolen every second[3] . Not a month goes by without a new data breach being reported. Recent research show that 63% of data breaches[4] were from weak, stolen, or compromised passwords.

FINANCIAL LOSS AND REPUTATIONAL DAMAGE

Companies can suffer substantial financial cost and reputational damage as a result of a security breach. The average data breach incident costs nearly $ 4 million[5] and can have far-reaching consequences for a company's financial health - not to mention the internal upheaval and stress on executives and business leaders within the organisation.

For their customers, individual losses can be even more hard-hitting with many suffering heavy financial losses, credit card fraud, and more. Once an identity is stolen or compromised, the details can be shared among criminal networks far and wide and it can take some time for consumers to finally escape the disruption such a breach causes to their life.

[3] https://thycotic.com/resources/cybersecurity-ventures-protect-300-billion-passwords-worldwide-2020/
[4] https://enterprise.verizon.com/resources/reports/dbir/
[5] https://globaldatareview.com/article/1195534/ibm-average-data-breach-costs-nearly-usd4-million

HOW CYBERCRIMINALS EXPLOIT THE VULNERABILITIES OF CREDENTIALS

For a moment, consider the life of a cybercriminal. Their ultimate goal is to access your information and identity usually for some financial gain. In today's world, a focus on credentials-based authentication means there are many ways the cybercriminal can steal the email IDs, passwords, and even biometrics required to carefully construct a version of your identity and do real damage (see Table 1.0 above).

An initial crime might start with a cybercriminal using screen scraper software which can gather freely available email addresses from all over the Internet and collate them in one list.

That list might then be spammed with a malware programme that will infect computers and help them harvest information like passwords used on a device or website.

Phishing is another technique where unsuspecting people are contacted by email, telephone or text message by someone posing as a legitimate authority like a bank or credit card company. People are then duped into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords, all the time assuming they are dealing with a supplier or partner they trust.

Man-in-the-middle attacks happen when a cybercriminal puts themselves in a conversation between a user and an application, intending to either eavesdrop or impersonate one of the parties. The goal of an attack is to steal personal information, like login credentials, account details and credit card numbers. It would be like a rogue postman opening your credit card statement, writing down the number and then resealing the envelope and dropping it in your letterbox.

LARGER CRIMINAL NETWORKS

Now that the criminal has used some of these techniques to steal large amounts of valuable personal details and credentials, if they do not use them themselves, they find a buyer on 'the dark web', the hidden internet used by cybercriminals.

Here, other spammers and what are known as 'credential stuffers' will buy the information in volume and often very cheaply. The 'stuffers' will take usernames and passwords leaked from one site to log into accounts on other websites where people might have used the same credentials.

So, for example, someone buying a big database of stolen credentials could decode the weaker passwords in the list, and then try to use the email address and cracked password combinations to log into Gmail or Facebook accounts, where the email address and passwords have been reused.

Now that we understand the consequences, it's clear to see why the urgency exists to develop a solution capable of tackling these cyber crimes on a larger scale. Standard encryption has played a role in protecting many users and their data over the years but the potential emergence of newer, more sophisticated technologies confirm that as long as any authentication method depends on static credentials, the risk of identity theft remains.

Existing encryption offers some protection – but for how long?

Developing any new UA platform must be considered in the context of the rapidly developing pace of technology. In particular, the anticipated ability of quantum computing looms large on the horizon as it has the potential to brutally expose the limitations of the current credentials-based approach, particularly so the Public Key Infrastructure (PKI) which we have used for so long to authenticate users and devices.

Standard encryption modules as we know them are based on PKI which works by generating a pair of encryption keys: one public and one private. As the name suggests, the public key can be accessed by all, but only the individual that has the private key can decode the message intended for them.

Essentially, once you keep the private key safe, the encrypted message stays secret until the person with the private key wants to decrypt it. The public key is related to the private key mathematically, so it is possible, in theory, to get the private key from the public key. Using a process called Prime Number Factorization, deploying a form of trial and error, it would take today's computers months or years to crack such a code.

ARRIVAL OF QUANTUM COMPUTING

Exponentially faster than today's hardware, quantum machines have the ability to try or guess thousands of different private key passwords in seconds. This means it's highly probable that our PKI system will be broken when quantum computing becomes accessible sometime within the next ten years.

And once more, the presence of credentials or passwords is creating this challenge. In order to tackle modern cyber security threats, any solution to user-authentication must avoid the need to use any form of credentials.

Password-free authentication is now a reality

With an accelerated increase in cybercrime and data breaches, it became obvious that the market was ready to take a new approach and the scene was set for what we call the post-credentials era.

For some time now at Cyberus Labs, we have been working on developing secure and simple UA technology that would facilitate secure Human-to-Machine interaction.

By replacing user credentials with an alternative that was fluid and temporary but still secure, it became apparent that we could eliminate the biggest risk in UA, namely leaving something static that that could be stolen or hacked.

DEVELOPING TECHNOLOGY FOR THE POST-CREDENTIALS ERA

For Cyberus Labs, the primary goal was to eliminate the use of credentials and create a platform where there was nothing for hackers to steal like passwords or even fingerprints. This would mean phishing and man-in-the-middle attacks are simply not possible using this platform. Research shows that the latter accounts for over 90% of data breaches[6].

In a development context for such a technology, security is the first consideration but user experience must come a close second. In other words, if any new approach is not easy to use, it may not matter how secure it is because people could be less likely to use it. By focusing on usability, we developed a one-click user logon to online accounts, prioritizing the user experience, which is particularly crucial for new technologies.

When it came to implementation, we chose a cloud-based approach, making it quick and easy to install using an API for web applications while we also made sure to provide a software-development-kit for integration with mobile applications.

For scenarios or service providers that demand it, multi-factor authentication was made available that can incorporate supporting functionality like biometrics, PINs, device geo-location, and more.

Now developed, this technology forms the core of our Human-to-Machine authentication platform Cyberus Key, a next generation UA system designed for the post-credentials era. With one eye on the current IoT explosion, this technology is also perfectly positioned to form a core element of a ground-breaking Machine-to-Machine authentication system in the coming years.

[6] https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

Presenting the first password-free User Authentication platform

Cyberus Labs spent 3 years developing a unique password-free user authentication platform which was designed to be ultra-secure and at the same time simple and fast to use. Our system enables users to log on to websites, mobile applications, and complete transactions and exchange information with fully authenticated service providers without the need for any credentials like user IDs or passwords.

HOW IT WORKS

Imagine for a moment you wish to log in to your existing bank account on your laptop.

1. Once registered, our system generates a highly secure, unique one-time token (truly random number) for each log-in session. This code is sent from our system server to the browser that's being used to login.
2. The browser then sends the one time code to your Smartphone via a sonic wave on a chosen frequency.
3. Along with a carefully developed formula, the Smartphone sends the code back to the system server and you are now authenticated in less than one second.

No credentials left means there's nothing for hackers to steal and a seamless user experience means no lost passwords or extra security tokens required. As a user, you benefit from fast, password-free authentication while eliminating fraud through direct authentication using one-time transaction tokens.

And as both sides are authenticated using out-of-band channels, security threats such as identity theft, phishing, and man-in-the-middle attacks are eliminated.

INSPIRED BY HISTORY

In 1917, in the closing years of the second industrial revolution, Gilbert Vernam, a telecoms engineer from the USA made a dicovery that would change cryptography forever in what became known as the Vernam cipher or One Time Pad Encryption. It would also provide our team at Cyberus Labs with the technical inspiration to develop a user authentication platform for the information age, some 100 years later.

Our Cyberus Key UA system generates a highly secure, unique one-time token (truly random number) for each log in session, utilizing a variant of One Time Pad Encryption. This has been mathematically proven to be unbreakable in 1947 and is widely accepted to be the most secure encryption methodology available.

Already available in the form of our product Cyberus Key, this technology can be deployed across a number of applications and industries, thanks to its ability to provide cast-iron Human-to-Machine authentication in many key sectors.

CYBERUS LABS UA PLATFORM IN ACTION

Banking & Finance - this password-free UA platform is tailor-made for online and mobile banking, insurance and fin-tech companies of all sizes. For these service providers, security is vital but customers must also enjoy a seamless login experience. The easier the login process is, the more often users will return and use the services offered, ultimately increasing revenue for the service provider.

E-commerce - through a simple, secure login, consumers can register and sign into sites without passwords. It also ties the login to a Smartphone, something the majority of users have with them at all times. This means no extra hardware is required and the login experience becomes as simple as opening an app and holding the Smartphone near the computer.

Telecoms - providers can deploy the password-free UA platform to offer customers a much easier user login to WLANs. Their customers will have no need to type in a Password or PIN to be authenticated and gain access to the network as they just need to activate the app. These service providers will benefit from using a one-click log-in into public or semi-public Wi-Fi networks.

Developing robust User Authentication with IoT on the horizon

While we often think of passwords as a way that humans can authenticate themselves on machines, computers or the Internet, the reality is that machines use passwords too on a daily basis to communicate with each other - and we see this on a huge scale within our rapidly developing IoT world already.

Like humans, the fact that IoT devices are still using static credentials is a big problem too. And although machines cannot 'forget' their passwords or suffer a poor user experience, the use of passwords on a machine-to-machine basis is a genuine cyber security challenge.

IoT DEVICES DEPEND ON PASSWORDS TOO

What amplifies the problem is that often, these credentials belong to innocuous devices like smart fridges, TVs and other devices that are not viewed as important as say, online banking portals or laptops. It often means that these IoT devices are left protected only by the default, simple passwords set by the manufacturer like 1-2-3-4 or even 0-0-0-0. Because of this, it makes the devices easier to hack than one that has a password developed by a human.

Within the last five years or so, the number of connected devices has surpassed the number of humans worldwide[7]. And while humans have so far not been able to protect themselves through static credentials like passwords, it is clear we are now expecting this growing population of machines to be left to fend for themselves in the IoT wilderness.

There is no doubt that the IoT represents our greatest cyber security challenge. In that context, the development and adoption of a safe, secure user authentication platform has never been more important for both Human-to-Machine and Machine-to-Machine purposes.

[7] https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

Conclusion

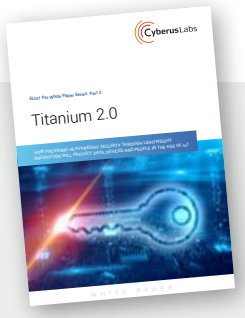
The password system as we know it is well and truly broken. At Cyberus Labs, we believe our password-free user authentication platform can deliver a new level of security for both Human-to-Machine and Machine-to-Machine authentication.

From biometrics and passwords through to hardware tokens, the failure of existing authentication approaches typically stem from one core shortcoming. The existence of credentials and particularly static credentials simply represents an invitation to hackers. If there is nothing to steal, intercept or replicate, the opportunity disappears. And when you include a poor user experience and what can only be described as 'password fatigue', it's easy to see why the appetite is there for a new direction on the part of users and companies alike.

MOVING ON

By moving to the post-credentials era and leaving behind passwords, many practices like data theft, phishing, and man-in-the-middle attacks can ultimately be eliminated.

With the Cyberus Labs UA platform already successfully authenticating across many use-cases and industries, it's clear the first crucial part of the bigger IoT security picture is now in place.



In part II (entitled Titanium 2.0) of our four-part white paper series, we'll explore Machine-to-Machine (M2M) authentication, analyze the problems associated with designing cyber security for IoT devices and outline how these challenges can be overcome.

Download or read the paper right here

More about Cyberus Labs

Based in Poland, with proven Silicon Valley experience, Cyberus Labs is a team of cyber security specialists that fully understand the new cyber threats faced by your business or organisation, whatever your size.

From traditional sectors, which have fully embraced the digital age like banking and e-commerce to the fast-growing world of IoT, your consumers are under threat from hacking attacks in the form of phishing, identity and data theft, and much more. Working closely with the European Union's Horizon 2020 research and innovation programme, we continue to focus on eliminating the risk of stolen passwords or credentials for both your users and devices - with our unique password-free authentication.

A NOTE ON ELIoT PRO

IoT devices and networks currently suffer from a lack of security leaving them vulnerable to a wide range of cyber-attacks. Whether it's rogue nations, thieves or terrorists attacking vulnerable networks, cybercrime is a multi-trillion dollar global threat. When IoT devices are hacked by cybercriminals, it can create devastating financial and reputational damage, and may even endanger human lives.

With ELIoT Pro, the world's first end-to-end cyber security solution for IoT networks developed by Cyberus Labs, you will no longer have to worry about cybercrime, knowing that your IoT users, devices and data are ultra-secure.

- No more passwords or old-fashioned logins means your users' credentials can never be stolen. And by eliminating passwords on your connected devices and machines too, there is nothing for hackers to steal and no way to gain access.
- Your IoT devices have different levels of computing power. And our lightweight encryption requires lower computing power and memory than any encryption system today – making it work on even the simplest IoT devices.
- Whether you prefer cloud-based, on-premise or a hybrid model, it's easy to set up and install with API functionality, an SDK, and a white-label option also available.
- Its AI engine, known as EP Cortex, creates an adaptive, self-healing IoT environment that can anticipate system failures, identify attacks, and automatically react so System Owners (SO) receive Just in Time device upgrades and replacements to keep IoT systems fully operational. SOs will also be made aware of any breach in progress and provide remedial reaction to safeguard the IoT system.

ROLE OF HORIZON 2020

„Horizon 2020 funds high-potential innovation developed by SMEs through the SME instrument. The SME instrument offers Europe's brightest and boldest entrepreneurs the chance to step forward and request funding for breakthrough ideas with the potential to create entirely new markets or revolutionise existing ones."

https://ec.europa.eu/easme/en

Contact Cyberus Labs

Cyberus Labs sp. z o.o.
ul. Warszawska 6 pok. 309
40-006 Katowice
Poland

office@cyberuslabs.com

www.cyberuslabs.com

The project ELIoT Pro has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 822641