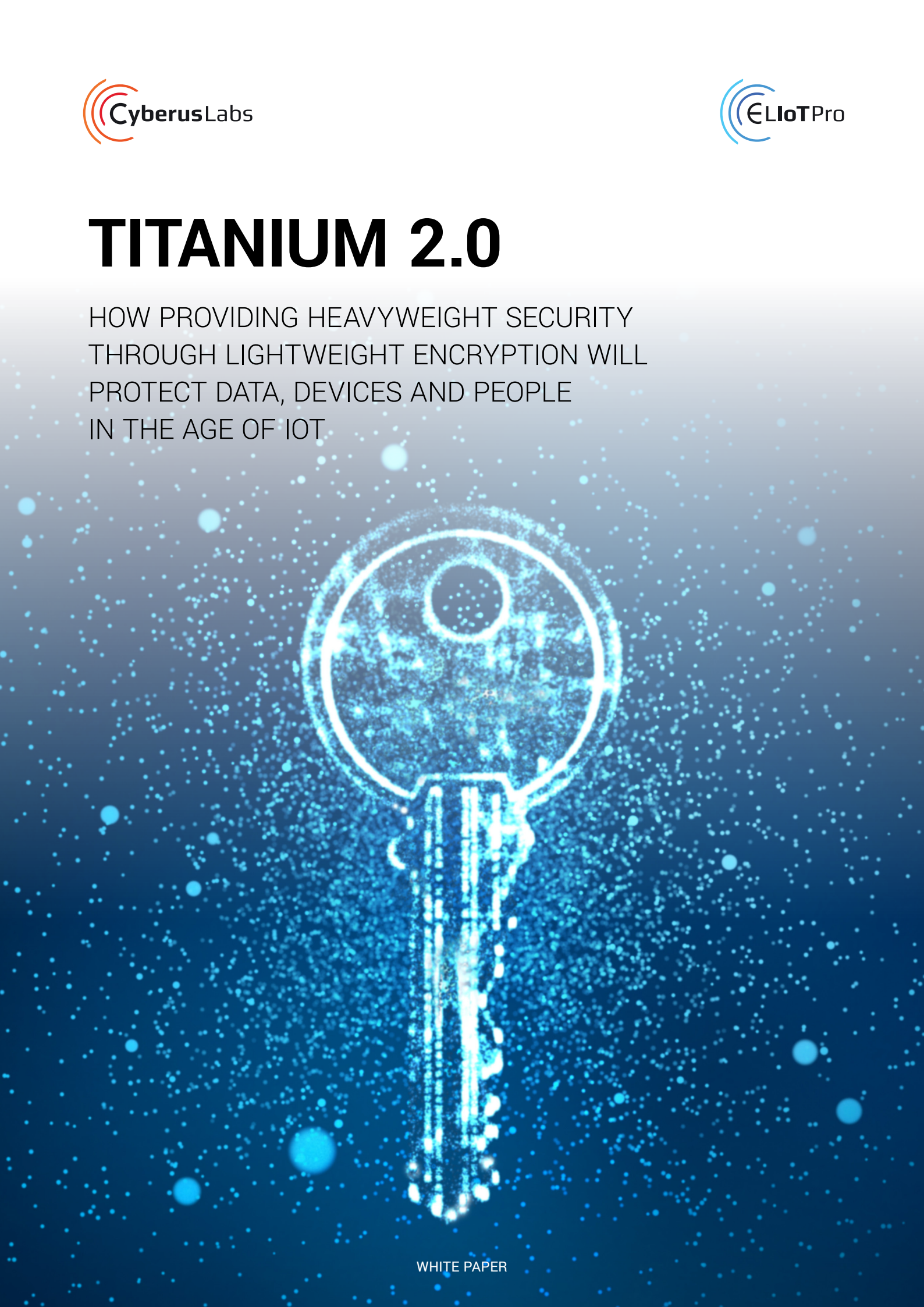
CyberusLabs

ELIoTPro

TITANIUM 2.0

HOW PROVIDING HEAVYWEIGHT SECURITY THROUGH LIGHTWEIGHT ENCRYPTION WILL PROTECT DATA, DEVICES AND PEOPLE IN THE AGE OF IOT



WHITE PAPER

CONTENTS

Executive Summary

Connectivity shapes every part of our daily lives and the ease with which we move through everyday chores and tasks thanks to our hyper-connected digital and physical world, would have been hard to imagine only 20 years ago.

Alexa invokes AWS Lambda synchronously. The effect of this is that a Lambda function invoked directly by Alexa will not return a response to Alexa until all calls it makes complete. For ELIoT Pro authentication this means that the login/status API request can't be made from this function. Instead it is made in a second Lambda function invoked by the service endpoint function using the InvocationType "Event" in the Lambda invoke call.

This Internet-of-Things (IoT) brings with it major advantages and enormous potential. Its exceptionally fast growth has unintentionally prioritised speed and connectivity over security and unfortunately, IoT networks are prone to infiltration and cyber attacks in the form of identity theft, phishing, DDOS attacks, and more. So many connected devices are designed to complete simple, singular tasks and giving them the battery power, computational ability and processor speeds that traditional computers and laptops enjoy was previously thought unnecessary.

Simple endpoint devices in IoT networks are vulnerable to hacking attacks. Their low power, low memory and low processing capabilities means that most of today's encryption methodologies are not capable of protecting these devices. As a result, both the devices and data are vulnerable to cyber attacks.

A MAJOR CYBERSECURITY THREAT

These very capabilities would enable IoT devices to run crucial encryption programmes. And inadvertently, across all IoT networks from Smart Cities and Smart Buildings to Smart Factories and Smart Cars, an army of connected devices that cannot adequately protect themselves has been built. These gaping security holes are already delivering consequences to many aspects of business and society.

Millions of new devices potentially mean millions of opportunities for hackers and cyber-thieves. Theft and hijacking is already a feature for the automotive sector while in the wider consumer world, reputational damage to major brands will continue and both device manufacturers and IoT network owners are on high alert.

These security breaches can all be traced back to one core principle which is that although their lower specs and slimmed-down capacity allow IoT devices play the part they're designed for, it means they are now the weakest point of entry in cyber security terms. The only way forward was to develop an encryption standard that enables devices of all levels to run a form of encryption but to make this so light and secure that it does not impact on performance.

INTRODUCING LIGHTWEIGHT ENCRYPTION

This standard has now been developed by Cyberus Labs and is known as Lightweight Encryption (LE). It is designed with simple devices in mind, retains unique entanglement technology and as it's based on the symmetric cryptography key, it is well positioned to handle future concerns like the advent of quantum computing and its anticipated impact on IoT security.

The team at Cyberus Labs have taken this standard and combined it with their existing one-time password authentication protocols to create the first end-to-end IoT cyber security solution on the market, ELIoT Pro, protecting human users, IoT devices and data. LE adds the titanium-esque qualities of strength, lightness, and flexibility to offer all IoT devices the protection they need, regardless of their computational power, or capacity.

Biggest single threat to IoT security

By the year 2020, it is expected there will be more than 20 billion devices[1] connected to the Internet. That is a level of connectivity we never thought possible but it's here and it delivers wonderful advantages to all aspects of life.

A NEW ERA OF ENDLESS POSSIBILITIES

In today's IoT world, fridges tell us what foods we need to stock up on and central heating systems await our instructions as we make our way home after a hard day's work. And even waste bins can report back to municipal services to help optimise collection routes and frequency!

Communication between such devices, in the shape of Machine-to-Machine (M2M) protocols means they can stay connected, and this enables the flow of information that help us make better decisions on everything from the weekly shop to inventory control.

With no humans interrupting communications, machines connect faster and centralisation leads to higher levels of automation and control, resulting in better service, more consistency, and transparency. This perfect marriage of monitoring and automation saves time, money, and hassle for consumers, companies, and organisations.

NO REAL DEFENCE

And with the advent of enhanced communication protocols like 5G, opportunities seem endless, and it all feels a bit like the early days of the Internet.

Even with all the advantages IoT can offer, analysts now believe we have created an army of devices and units that do not have the armour to defend both themselves and us too from the threat of hackers. These devices carry crucial, valuable information and as they grow in number, it means many more attack routes for hackers and other malevolent groups determined to break into IoT networks, take control of devices, steal data, identities, and more.

[1] https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

PCs, Laptops, Smartphones, and other more complex machines with high processing speeds and bigger memory capacity are much less likely to be hacked as they can run and maintain in-built security and software to handle cyber security threats. For many years, IT security specialists saw these conventional machines as the major risk areas and worked hard to develop solutions to tackle this head on.

OPEN TO ATTACK

Today's connected devices do not enjoy the same level of protection mainly because they are primarily designed for the role they are carrying out, and simply do not require high levels of computational power. Inadvertently, we have built a network of machines with low computing power, and low memory that use very little energy. They are well able to complete their main function but much less capable of a whole lot else.

For example, a smart baby monitor was designed to give parents peace-of-mind that their child's sleeping patterns and night-time conditions are optimal so being able to relay images and report real time temperatures and similar data is enough. Similarly, a smart fridge can run internal cameras for monitoring, create temperature zones and even run a TV, and has the only computational power and processor speed required to carry out these tasks.

VULNERABLE NETWORKS

So while we know them the world over as smart devices, they have also been described as 'dumb robots' in many ways – as they lack the memory, electrical, and computational power to handle demanding algorithms like AES 128 or AES 256. And keep in mind that these are the encryption specifications for electronic data that have been adopted worldwide for nearly 20 years.

Even though they are known as the weakest element of IT security, we use passwords every day to access information, and machines and devices in the IoT world also talk to each other through passwords. It's this lack of secure device-to-device authentication that is leaving networks vulnerable and open to attack. The infamous Mirai[2] attack brought this precise issue into the global security spotlight. Every system is only as strong as its weakest link and this gaping weakness that exists right across our IoT ecosystem has consequences for companies and organizations of all sizes.

[2] https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Impact of sub-standard cybersecurity

The consequences of connected devices with inadequate levels of security are wide-ranging and far-reaching. For data and devices within both industry and society, cyber security breaches have come in many forms and unsecure IoT networks create an unstable present and an uncertain future.

THEFT

Stolen personal information has unfortunately been an aspect of life since the online revolution began, through techniques like phishing. What makes the connected IoT world more susceptible to theft is that the potential is now there to intercept strategic or sensitive information that is 'in flight' between devices.

A recent US survey found that 15.4 million consumers were victims of identity theft or fraud in 2017 with thieves stealing $16 billion[3] in total, making identity theft a very lucrative illegal business. Separate research reports that 84 percent of businesses[4] say they have already experienced an IoT-related security breach.

Physical theft of devices is also an issue and there have been several examples of cars that have been hijacked or others that could be stolen and possibly remotely controlled through wi-fi and cellular connections.

[3] https://www.javelinstrategy.com/coverage-area/2017-identity-fraud
[4] https://www.arubanetworks.com/solutions/internet-of-things/

REPUTATION

A recent Gemalto report found that 90 percent of companies believe IoT security is a big consideration for consumers[5]. And companies that run less secure devices are feeding this fear and damaging their brand. In turn, the original manufacturers will be held to account by their own customers for making devices that are cyber security risks.

With growing levels of awareness and concern over data breaches and vulnerability, consumers are understandably highly sensitive and place real value on manufacturers and service providers who take security as seriously as they do. The trust between manufacturer and vendor is the foundation of any supply chain and a manufacturer that develops a less-than perfect reputation when it comes to developing IoT devices is one that will never be taken seriously in a hyper-connected world.

In 2018, Under Armor reported that its "My Fitness Pal" was hacked, affecting 150 million users[6] and no doubt suffered damage to its brand. The consequence here is a loss in trust in a brand or local or national authority which can be very difficult to restore.

SOCIETY

The targeting of IoT systems is another serious security concern for society overall. In communications terms, IoT devices that form parts of VoIP systems and routers can be very vulnerable and loss of service or damage to these networks has major ramifications for all aspects of daily life. Our built environment also depends on IoT-driven elements that control access security, power, environmental controls, and leaving these systems unsecure makes for an uneasy general public.

EU Research puts the number of IoT smart city units at 17.3 million in 2017, and it is expected to reach 47.1 million units by 2025[7]. For municipalities, local councils, and authorities, traffic systems and CCTV networks are all part of IoT networks and this 'smart-city' infrastructure, in worst-case scenarios, is open to infiltration causing terror attacks. Similarly, nuclear power plants and electrical grids hold enormous power which in the wrong hands could prove devastating.

[5] https://www.gemalto.com/press/Pages/Almost-half-of-companies-still-can-t-detect-IoT-device-breaches-reveals-Gemalto-study.aspx
[6] https://www.news.com.au/lifestyle/fitness/150-million-myfitnesspal-accounts-hacked-in-huge-data-breach/news-story/2cc6955e47b853cb6a0eb0369a9fbf91
[7] https://www.statista.com/statistics/691843/smart-city-iot-units-in-the-eu/

INDUSTRY

Industrial IoT is a fast growing ecosystem and Juniper Research expects that by 2023, there will be close to 46 billion active industrial connections[8]. This means many daily workplaces like construction sites, labs, factories, and particularly those using switches, valves, CNC, and production environment controls are at risk. Were any of these to be infiltrated, it could lead to production downtime, technical malfunction, damage, and serious health and safety concerns for employees.

As the numbers of connected devices grow and technology develops, new routes emerge for hackers. For example, voice is quickly becoming an integral part of the IoT world and nearly 50 million consumers in the US already own smart speakers[9]. And it is devices just like these that are most in need of protection.

NEXT STEPS

With the scale of this issue now in context, it became clear that a new approach was required. A cyber security standard that offers real protection to IoT units and devices of all specifications has now been developed and is well positioned to play a crucial role in cyber security for many years to come. This standard is known as Lightweight Encryption.

[8] https://www.businesswire.com/news/home/20180612005154/en/Juniper-Research-IoT-Connections-Grow-140-Hit
[9] https://voicebot.ai/2018/06/28/smart-speaker-users-pass-50-million-in-u-s-for-the-first-time/

Introducing Lightweight Encryption

ANATOMY OF AN IOT CYBER SECURITY STANDARD

Now that we understand the consequences, it's clear that IoT devices need to benefit from the security of encrypted communication. And the only way forward was to develop a standard that matches the limited computational power while delivering the highest levels of protection possible. Lightweight Encryption (LE) is that standard as it is purpose-built, while incorporating uniquely strong authentication technology, and these titanium-like properties can help tackle one of the key cyber security concerns of the next decade.

PURPOSE-BUILT FOR IoT DEVICES

While all IoT devices are not equal, they do need to be afforded an equal level of protection in the context of growing connectivity meaning no one device can become the single point of entry that hackers need. Without the capacity to handle complex or demanding encryption methodologies and the fact that device battery life is affected by computing activities and memory usage, these devices are wide-open. LE recognises this core issue head-on and it is fair to say that technology best-practice-standard-development usually begins with deploying technology to solve business or organisational problems.

ENTANGLEMENT AUTHENTICATION PROTOCOLS

Traffic and data being sent between devices require encryption and LE incorporates the concept of 'entanglement', its unique characteristic that sets it apart from other developments in the cyber security world. This is where authentication that deploys encryption creates a degree of entanglement and as a result, substantially stronger security delivering mutual authentication. In simple terms, the better devices 'know' or recognise each other, the stronger the authentication is.

PREPARING FOR Y2Q[10]

Quantum computing is coming and brings with it huge benefits but inadvertently, major security risks too. The mathematical calculations required to break asymmetric cryptography, on which PKI (Public Key Infrastructure) relies are beyond the abilities of today's computers but would pose no problem to a quantum computer. These are the perfect conditions for a classic brute-force attack where hackers simply try every possible variant of a password in order to gain access. LE is based on the symmetric key, using the same key for both encryption and the decryption, making it ideally positioned for what has become known as Y2Q, the arrival of wide-scale quantum computing.

Working alongside supporting technology in one architectural framework, LE can become the standard base technology for cyber security in the IoT world. Cyberus Labs have done precisely that and have fused Lightweight Encryption with their own one-time-password-protocol to produce the world's first end-t0-end cyber security solution for IoT – ELIoT Pro.

[10] https://www.innopay.com/en/publications/quantum-computers-will-revolutionize-cryptography-and-cybersecurity-heres-why

How ELIoT Pro deploys LE

ELIoT Pro runs on LE to provide end-to-end security for IoT networks

Here at Cyberus labs, we are proud to present ELIoT Pro, taking our own carefully developed LE standard and by supporting it with an authentication module, a cyber security solution is now available that is dedicated to protecting devices that would usually not have the internal armour to defend themselves. Automotive, Industrial IoT, Smart Cities, and Smart Homes specialists can now protect their customers against IoT cyber security threats including DDoS, cloning, Man-in-the- Middle attacks, and more.

ELIoT Pro takes a dual-module approach to cyber security for IoT devices. By combining secure Human to Machine (H2M), and Machine to Machine (M2M) authentication and communication with LE, IoT networks can become safer than ever.

DUAL APPROACH TO ULTRA-SECURE IoT NETWORKS

1 Replace passwords with superior authentication protocols

As a first step, passwords must be eliminated for machine to machine authentication, wiping out the possibility of unauthorised access. Our authentication protocol uses one-time audio token technology or one-time passwords transmitted by an ultra-sonic signal.

2 'Lighten' encryption to ensure readability on devices of all specifications

ELIoT Pro provides equally ultra-high level of security to all types of IoT devices regardless of their memory/computational power limits. ELIoT Pro introduces an entirely new "language" of communication through LE with all IoT devices which is understandable even for the simplest units on the market.

What makes ELIoT Pro different?

TIGHTER SECURITY

It is commonly accepted that the weakest link in IT security today is the password. And because machines, as well as people, use passwords to communicate with each other, it's a wider issue in an IoT context. ELIoT Pro enables us to eliminate passwords on all connected devices, ensuring there is nothing for hackers to steal and no way to gain access.

PROTECTING ALL DEVICES EQUALLY

In recent years, security analysts have anxiously watched the IoT ecosystem develop and now see many simple devices like heat sensors, vibration sensors, and more leaving entire networks wide open simply because they are not equipped with the capability to run their own encryption modules. With ELIoT Pro, now even the simplest devices can enjoy the protection that up to now was only for conventional computers like laptops and Smartphones.

FULL FUNCTIONALITY

ELIoT Pro maintains all the characteristics of a custom-built software platform. It is easy to install and implementation options are available for cloud-based, on-premise, and hybrid set-ups too. It uses API functionality and a Software Development Kit can be accessed on demand. Built-in Artificial Intelligence creates and fosters a self-healing capability that can detect unusual or suspect behaviour and predict device failure.

VOICE CAPABILITY

In such a dynamic, fast-moving technical field like cyber security, it is important that research and development work is carried out with one eye firmly on the future. Voice-controlling technology has entered the mass market within the last decade but it is anticipated that the IoT landscape will only accelerate its growth with almost limitless use-cases now possible. ELIoT Pro's Smartphone-based user login with sound technology means a fully secure user authentication mechanism for voice-controlled environments like Alexa, Google Home, or Siri is now possible.

Conclusion

Lightweight Encryption has the potential to transform best-practice cyber security standards in the IoT world. Application of this technology ensures that weak links can be eradicated in IoT networks. And that despite the low computational power and relatively unsophisticated make-up of everyday IoT units, LE can be the means by which they can securely connect with other devices in their network and keep out hackers, cyber-thieves and other similar threats.

Working as a core element of the Cyberus Labs end-to-end cyber security solution, ELIoT Pro, it means all devices can be protected to the same level. This can give genuine peace-of-mind to manufacturers, IoT network owners and consumers as they continue to grapple with cyber security in an increasingly connected world.

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 who 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 using one-time transaction codes.

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.

Contact us

Marek Ostafil, COO

+48 692 437 857

marek.ostafil@cyberuslabs.com

Cyberus Labs Sp z o.o.

ul. Warszawska 6/309

40-006 Katowice, Poland

00 12345 56789

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