CyberusLabs

ELIoT Pro White Paper Series: Part 2

Titanium 2.0

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

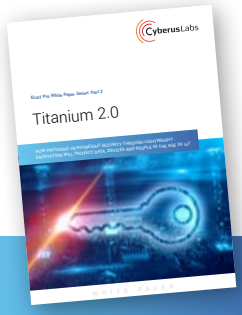
WHITE PAPER

A note on the ELIoT Pro White Paper Series

The ELIoT Pro four-part white paper series details how Cyberus Labs has identified the key issues that need to be addressed in order to develop the industry's first end-to-end cyber security solution for IoT.

Part 1

considers the issues associated with using passwords for Human-to-Machine (H2M) authentication and the move into the post-credentials era.



For Part 2 and this paper

we'll explore 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 3

Biggest single threat to IoT security 5

Impact of sub-standard cybersecurity 7

- Theft 7
- Reputation 7
- Society 8
- Industry 8

Introducing Lightweight Encryption 9

- Anatomy of an IoT cyber security technology 9

How ELIoT Pro deploys LE 11

- What makes ELIoT Pro different? 12

Conclusion 13

About Cyberus Labs 14

- Role of Horizon 2020 15

Executive Summary

Connectivity now shapes every part of our daily lives. 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.

This Internet-of-Things (IoT) brings with it major advantages and enormous potential. Its exceptionally fast growth, however, 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, data theft and more. Many connected devices are only required to complete simple, singular tasks and so they are often designed with low battery power, computational ability and processor speeds.

Most of today's encryption methodologies are not capable of protecting these simple devices. As a result, both the devices and data in the IoT network are vulnerable to cyber attacks.

A MAJOR CYBERSECURITY THREAT

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 to play the part they're designed for, it means they are now the weakest point of entry in cyber security terms. Cyberus Labs saw a clear need to develop an encryption technology that enables devices at all levels to run a form of encryption but to make this so light and secure that it does not impact performance.

INTRODUCING LIGHTWEIGHT ENCRYPTION

This technology has now been developed by Cyberus Labs and is known as Lightweight Encryption (LE) which is a unique synthesis of secure device-to-device authentication with data encryption to protect both devices and data.

Designed with simple devices in mind, using specific entanglement technology, the LE approach avoids the need for complex encryption calculations. In turn, this eliminates brute-force attack vulnerabilities making it well positioned to prepare for future concerns like the advent of quantum computing and its anticipated impact on IoT security.

The team at Cyberus Labs have taken this technology and combined it with their existing one-time password user authentication protocols and other key components to create the first end-to-end IoT cyber security solution on the market, ELIoT Pro. 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.

Biggest single threat to IoT security

Today there are 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 weekly shopping 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, the opportunities for IoT 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 vectors for hackers and other malevolent groups who are 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 devices with high processing speeds and bigger memory capacity seem less likely to be hacked as they can run and maintain in-built security and software to handle cyber security threats. Yet they still remain vulnerable even though they enjoy a level of protection - something simpler IoT devices just do not have.

OPEN TO ATTACK

Today's connected end-point devices such as sensors and actuators do not have adequate levels of protection mainly because they are primarily designed for the specific role they are carrying out, and simply do not require higher levels of computational power, memory and energy.. Inadvertently, we have built a network of machines that are vulnerable to cyber attacks as they cannot be protected using today's widely used encryption algorithms and security frameworks..

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 data like that is enough. Similarly, a smart fridge can run internal cameras for monitoring, create temperature zones and even run a TV, so has only the computational power and processor speed required to carry out these tasks.

Find out more about...

User Credentials

"Why tackling the credentials culture is the first step in delivering safe authentication in an era of rising cybercrime"

in Part 1 of our whitepaper series which you can read here

Download or read the paper right here

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.

Generally speaking, passwords are the weakest element of IT security and today. Authentication largely depends on password usage and user credentials that have countless weaknesses and vulnerabilities. And unfortunately, while we, as human users, use passwords to authenticate and access information every day, machines and devices in the IoT world do the same thing again using passwords.

It is 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 wider society, cyber security breaches have come in many forms and unsecured 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 situ” or ‘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 were stolen and remotely controlled through wi-fi and cellular connections.

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, 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 lack-of-trust for the brand which can be very difficult to restore.

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

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 can make 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.

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.

NEXT STEPS

With the scale of this issue now in context, it became clear that a new approach was required. A cyber security algorithm 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 technology is known as Lightweight Encryption.

[7] https://www.statista.com/statistics/691843/smart-city-iot-units-in-the-eu/
[8] https://www.businesswire.com/news/home/20180612005154/en/Juniper-Research-IoT-Connections-Grow-140-Hit

Introducing Lightweight Encryption

Anatomy of an IoT cyber security technology

Now that we understand the consequences, it is clear that IoT devices need to benefit from the security of encrypted communication. And the only way forward was to develop a methodology that matches the limited computational power while delivering the highest levels of protection possible. Lightweight Encryption (LE) 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 - as the old saying goes “a system is only as strong as its weakest link.” 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 to attack. LE recognises this core issue head-on and it is fair to say that technology best-practice-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 Y_2Q[9] AND THE ARRIVAL OF QUANTUM COMPUTING

Most encryption modules as we know them are based on PKI (Public Key Infrastructure) which works by generating a pair of encryption keys: one public and one private. In practice, 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.

However, quantum computers will be significantly faster than today's hardware, and it is expected that by the time it's developed, this technology will 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 in real danger when quantum computing becomes accessible sometime within the next ten years.

PROBLEM OF CREDENTIALS

It is the presence of credentials or passwords that 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.

Working alongside supporting technology in one architectural framework, LE can become the base technology for cyber security in the IoT world. Cyberus Labs have done precisely that and have fused Lightweight Encryption with other key components including ground-breaking user authentication protocols, and robust analytics to produce the world's first end-t0-end cyber security solution for IoT – **ELIoT Pro**.

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

How ELIoT Pro deploys LE

ELIOT PRO DEPENDS ON LE TO HELP PROVIDE END-TO-END SECURITY FOR IOT NETWORKS

Here at Cyberus labs, we are proud to present ELIoT Pro. By taking our own carefully developed LE algorithm and supporting it with an authentication module and robust analytics, a cyber security solution is now available that is dedicated to protecting IoT 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, data theft, DDoS, cloning, Man-in-the- Middle attacks, and more.

ELIoT Pro takes a three-layered approach to cyber security for IoT devices. By combining secure Human to Machine **(H2M)** authentication, Machine to Machine **(M2M)** authentication with LE, alongside our custom-built data analytics and intelligent control centre, **EP Cortex**, IoT networks can become safer than ever.

THREE STEPS TO ULTRA-SECURE IoT NETWORKS WITH ELIoT PRO

1. H2M: **Replace passwords with superior authentication protocols**

   ELIoT Pro is based on the theory that 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. M2M: **'Lighten' encryption to ensure readability on devices of all specifications**

   ELIoT Pro provides equally ultra-high levels 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 for all IoT devices which is understandable even for the simplest units on the market.

3. EP Cortex: **Deploy data analytics in the form of our customized rules engine, artificial intelligence and real-time portal to maintain and monitor**

   ELIoT Pro benefits from an in-built Rules Engine and Flight Envelope parameters to determine safe operating ranges for devices. Artificial Intelligence and predictive analytics can predict IoT device failure in the system while an intuitive device portal enables system owners and device vendors to interact and keep IoT systems operational.

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 ultra-secure device to device communication by eliminating the need for 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 it is now clear that many simple devices like heat sensors, vibration sensors, and more, are leaving entire networks wide-open to attack simply because they are not equipped with the capability to run their own encryption modules. With ELIoT Pro, 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 also 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.

Conclusion

Having successfully tackled the ‘password problem’ in the context of H2M interaction, turning our attention to the issues associated with M2M in the IoT world was the next logical step. It is now clear that our Lightweight Encryption technology has the potential to transform best-practice cyber security standards in the IoT world too.

Application of this innovation 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, LE ensures 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.

In Part Three of our Four-Part white paper series, we’ll explore the emerging role of data analytics and in particular the need to set rules in order to monitor the behaviour of IoT devices, track performance, and detect malfunctions.

Download or read the paper right here

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.

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.
- An in-built AI engine, which we call the EP Cortex, creates an adaptive, self-healing IoT environment that can anticipate system failures, identify attacks, and automatically react so users receive Just in Time device upgrades and replacements to keep IoT systems fully operational.

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 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