CyberusLabs

ELIoT Pro White Paper Series: Part 3

The Brain behind the IoT security

WHY IoT SYSTEM MONITORING AND DEVICE PROFILING WILL BECOME AN INTEGRAL ELEMENT IN THE FIGHT AGAINST CYBERCRIMINALS

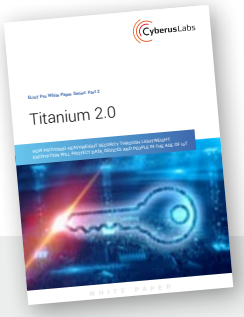
WHITE PAPER

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.

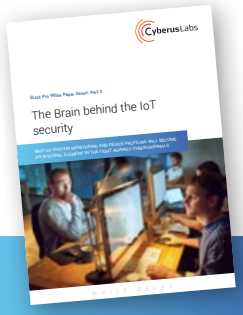
Part 1

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



Part 2

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



In this publication, Part 3,

we examine the need to set rules to monitor the behaviour of an IoT device, track its performance and 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

Our IoT eco-system continues to grow at speed, and as with any major shift in technology, rules and best-practices often lag behind in the early days.

A distinct lack of monitoring and real-time network visibility is presenting hackers with real opportunities in our relatively young IoT eco-system. System owners (SOs) need to be made aware if component devices are being stressed or operating outside their pre-programmed parameters.

This suboptimal approach to IoT device monitoring and management could potentially have devastating consequences across all sectors. Wherever operating parameters can be breached or tampered with, havoc may well ensue. From temperature settings in manufacturing environments to pollution metrics in metropolitan authorities, if devices are allowed operate outside of their optimum range undetected, there will be serious safety, commercial, and compliance consequences for many.

Only by moving to some form of monitoring and built-in 'light surveillance' will this problem be tackled. If SOs are alerted when a dangerous or otherwise anomalous condition has developed, they can respond and adjust. Monitoring functionality has been successfully deployed in other IT security and engineering applications and can also play a crucial role in IoT security too.

INTRODUCING EP CORTEX

In response to this need, Cyberus Labs have developed an IoT-specific data analytics module known as EP Cortex. An integral part of the world's first end-to-end cyber security solution ELIoT Pro, EP Cortex is home to a unique IoT device profiling and rules management system.

SOs will have access to dashboards that show device performance and display operational limits that the device should not exceed. This ensures the SO stays fully informed and can detect anomalous or suspect behaviour.

Also containing diagnostics and self-healing properties, EP Cortex enables data analytics to provide a new level of visibility and management for system owners. It works in tandem with ELIoT Pro's core elements including H2M password-free user authentication and M2M password-free encryption and machine authentication.

Minimalist monitoring is weakening our IoT

With the number of devices forecast to grow to 41.6 billion by 2025[1], the IoT eco-system is becoming an integral part of our daily digital lives. While the role of IoT was to increase automation and make life easier, smoother, and less disruptive, a lack of proactive measures and monitoring is potentially putting this entire system at risk.

DANGER

Device outputs or inputs are typically not being monitored to determine if they are in a safe operating range. If component devices are being stressed, misdirected or operating outside chosen parameters, it spells danger. It also means SOs are currently not being alerted that dangerous or otherwise anomalous conditions have developed. As a result, the system is unable to respond and adjust.

While many IoT devices are quite limited in functionality and capacity, they often carry out very important, high-value tasks including everything from temperature regulation to traffic monitoring, and so much more. A lack of monitoring and system awareness will have major consequences for the systems, owners, and anyone with a device connected to the hacked system or overtaken unit. It is only by moving to some form of monitoring and built-in 'light surveillance' will this problem be tackled.

DATA

Data plays a crucial role in ensuring the devices operate as they are intended within specific parameters, and keep SOs informed when they do not. These parameters will ensure that even if devices are hacked, certain limits can never be extended or increased.

Without monitoring, we do not know if these settings are being reached or breached. This lack of data is hampering development, reducing peace-of-mind, and significantly diminishing security too. Right now we are leaving the IoT door wide open for bad actors to hack in and take control.

IoT security is ready to evolve and the next phase will need to focus on delivering more insight about what's actually happening on devices, detecting anomalies, and equipping SOs with the insight to react and respond quickly and effectively.

[1] https://futureiot.tech/idc-forecasts-connected-iot-devices-to-generate-79-4zb-of-data-in-2025

INACTION MAY PROVE COSTLY

It is feared that this lack of monitoring and awareness of network activity could result in major impacts for companies and people across all sectors. From safety issues right through to reputational damage, the consequences of this suboptimal approach to IoT device monitoring and administration are far-reaching.

Smart Home – as the number of IoT devices grows within our homes, the risk grows with it. For example, if temperatures in a given home are tampered with and set too high or too low, this can become more than an irritant to a house owner or resident. Similarly, connected lights can be hacked to stay on too long while doors and windows might have different operating patterns depending on the seasons. If they are not working as intended, risks to the home include increased energy bills, physical security breaches, and more.

Smart Cities – the benefits of an IoT smart city infrastructure are numerous. Once again, many metrics are measured to assess all types of issues like pollution indicators and traffic management. If these tools are compromised, they immediately represent a threat to the city in terms of citizen health and compliance. Overheating power grids, polluted water treatment plants, and more can also cause major resource and safety issues for metropolitan areas. Unfortunately, in our modern world, the threat of terrorism is never far away and there is also potential for major disruption in the event of misinformation being sent by sensors intentionally to paralyze smart-city systems.

Industrial IoT – in any production environment, a manufacturing unit must operate to strict schedules, systems, and protocols to ensure maximum productivity. In the age of IoT, automation has seen the introduction of many networked sensors, machines, and infrastructure. Their connected status means they represent a cyber security risk. Hackers can potentially purposefully overheat devices, increase pressure or adjust any one of thousands of IoT settings. Without full knowledge of what devices are doing, the SO is risking potential downtime, staff safety, and reputational damage.

Automotive – connectivity has been a part of automotive engineering for quite some time and with the adoption of IoT technology, this has accelerated substantially. And with that comes an extra degree of risk since more devices are connected. From engine overheating to brake failure, there are so many opportunities for bad actors to seriously tamper with a car's digital connectivity. SOs need greater awareness and must ensure devices are operating within desired metrics like interior temperature ranges, battery levels, and power grid parameters. Driver safety, reputational damage, and compliance are among the many risks for automotive providers in the digital age.

Aviation – airplanes are now managed by highly complex on-board computer systems. Sensors throughout the plane are programmed to complete certain tasks which all play a role in ensuring safe, successful flights. With computers controlling everything from cabin temperature and structural components to in-flight entertainment, monitoring must play a crucial role. Simply put, lives are at risk whenever aviation IoT is compromised and were any of these metrics to be adjusted or tampered with through a cyber attack, it could have major safety implications.

Medical devices – smart medical devices today are tasked with carrying out many very important procedures and treatments. From dispensing medicines through infusion pumps to monitoring vital organs like pacemakers, if anomalous behavior is not picked up in these scenarios, the consequences could well be fatal for the patient and catastrophic for the device manufacturer or IoT system owner.

It's clear to see the time has come to put rules in place and monitor IoT devices with greater vigilance. As cybercriminals become more creative, we too must change and put the focus on monitoring and surveillance as much as security itself.

Next, we will describe how elements of existing technology partly hold the key to cracking this specific cyber security nut.

Technology can build device management tools and provide transparency

For many years now, rules engines have been written into software programs, and elsewhere, while device-profiling technologies have prowled networks to address security concerns. Deployed individually, they have played an important role in the pre-IoT world.

RULES ENGINES

From email scanners to anti-virus software, rules engines have been active in IT security for many years. Rules engines work best in situations where parameters are in place to secure the consistent and accurate deployment of technology in order to deliver intended results or benefits.

For example, antivirus software uses rules engines to determine if a program is malware, while firewalls deploy a rules engine to identify whether a connection is malicious or not. Essentially, these products typically have a rules engine which tests if a program or connection matches a particular signature. These signatures or indicators might include connecting to a known-to-be-suspicious IP address, or creating a file with a name that was once associated with malware.

If a well-written rule has been developed to address a piece of malware or for an attack, owners are assured that they will get the notification they need and be alerted to an attack.

Rules engines have also been part of industrial infrastructure for many years, well before the arrival of IoT. Rules were often written to handle general structural or fixed asset damage. For example, when parameters or metrics are not met due to incapacitation or if other measures indicate the potential for future damage, machinery can be programmed to automatically be shut down.

DEVICE PROFILING

Device profiling typically allows you to gather device type and operating system information by inspecting data that is sent by these devices in the network. Accurate deployment of device profiling in any networked environment can detect, track and report back any device that connects to the network down to its specific make and model.

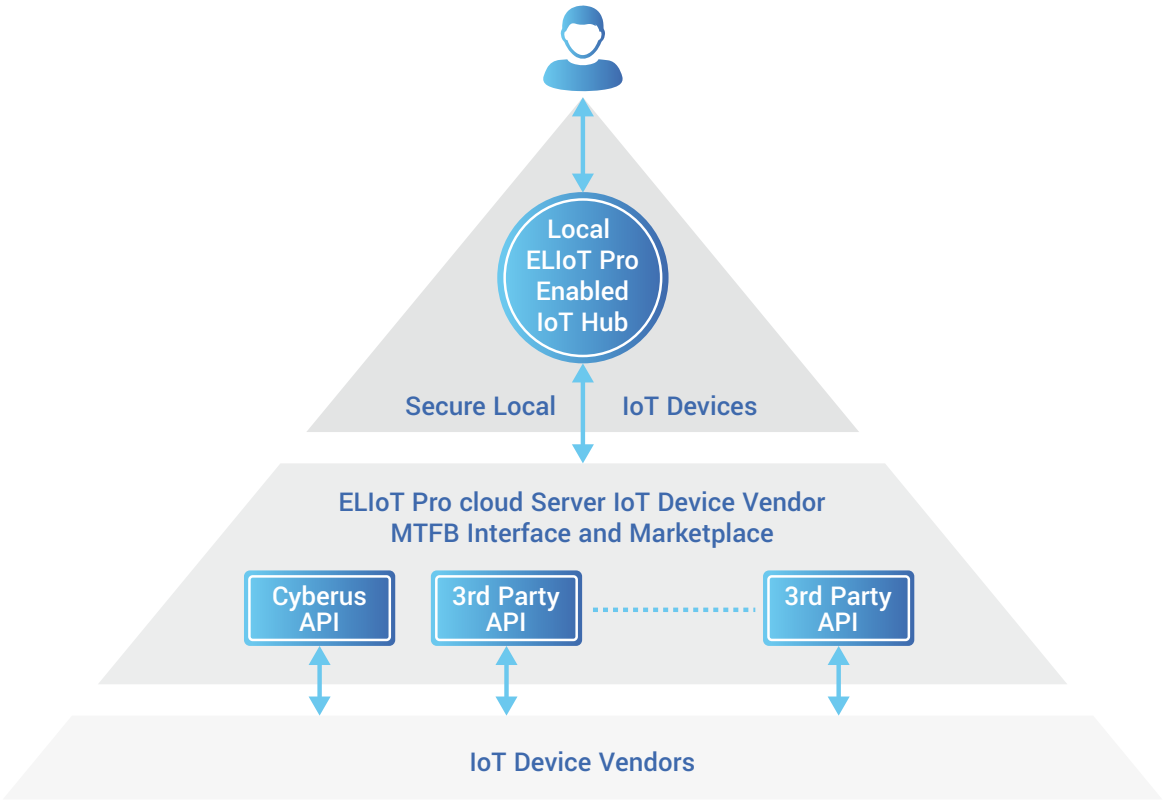
From ensuring devices have the latest software updates to detecting unusual behaviour and performance, device profiling offers a level of assurance for SOs.

At Cyberus Labs, we have fused these twin technologies with other key components to create a robust analytics capability which we call EP Cortex.

INTRODUCING EP CORTEX

At Cyberus Labs, we are proud to present our purpose-built EP Cortex technology, home to our unique ELIoT Pro IoT device profiling and rules management system.

Made up of several key components, including monitoring, diagnostics, and self-healing, it is the third layer in ELIoT Pro, the world's first end-to-end cyber security solution for IoT.



EP Cortex recognizes that an IoT system must be made aware if its component devices are being stressed or operating outside their pre-programmed parameters. Acting as a type of command centre, EP Cortex allows the system to alert its owners that a dangerous or otherwise anomalous condition has developed so that the system can respond and adjust.

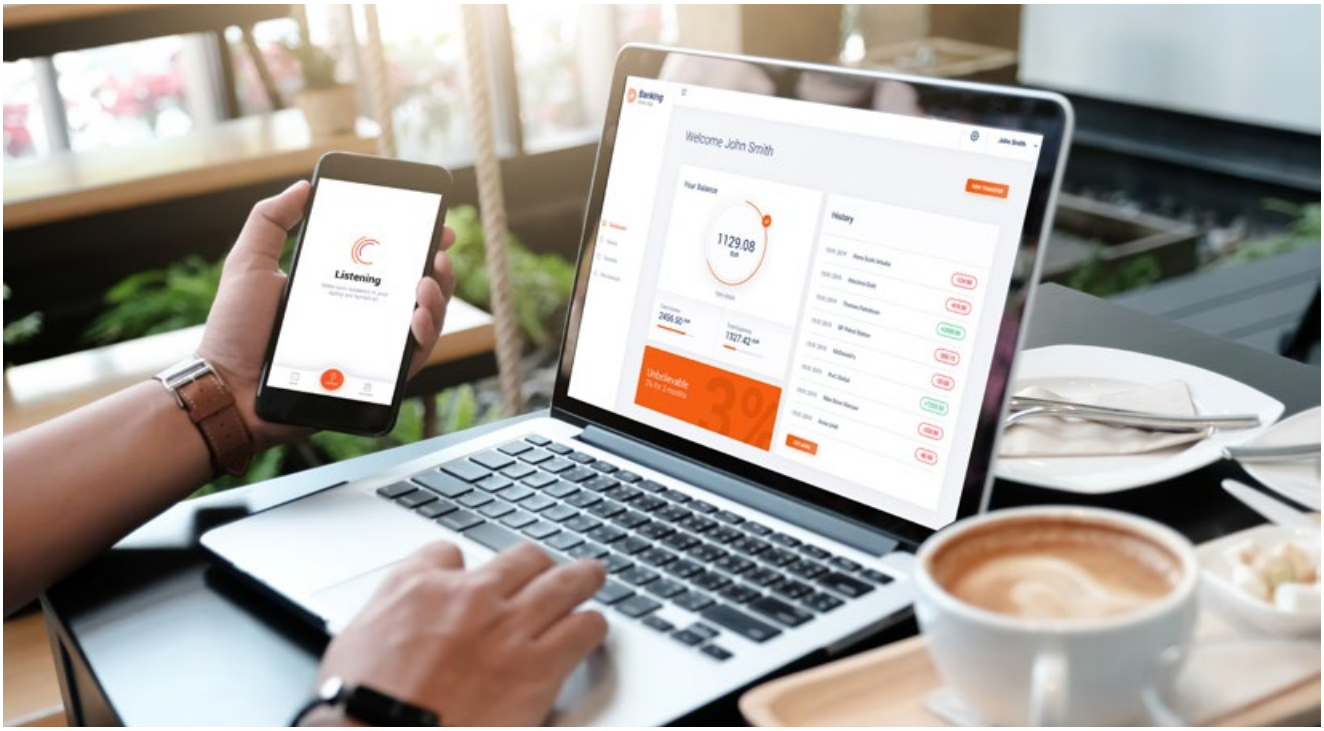
THREE KEY FEATURES OF EP CORTEX

Rules engine - at the heart of the EP Cortex, a rules engine receives data from all connected devices and runs it against the IoT device operating limits. It then applies rules specified by the SO or user to control the IoT system and to evaluate system state and health. The rules engine can also shut down devices which are behaving erroneously.

Flight Envelope – the rules engine is based on a flight-envelope-limit or operational parameters. In aviation, the term flight envelope refers collectively to the operating parameters and capabilities of a specific model or type of aircraft. The various parameters that make up a flight envelope include the aircraft's maximum altitude, maximum and minimum speed, the maximum amount of g-forces the craft can withstand, climb rate, glide ratio and other factors that define the aircraft's flight characteristics.

Just like aircraft, IoT ecosystems and devices also need flight envelopes – pre defined operating and performance parameters. Any device performing outside of these is an indication that the device is either 1. failing/has failed or 2. the device has been hacked. The device should stay within this range for everything to be operating normally. Our flight envelope database holds this SO-defined IoT device operating limits information, and all necessary IoT device data.

Dashboard - through a set of intuitive screens, the SO User can interact with the IoT Hub using a web browser and this is known as the System Owner IoT Hub Dashboards. It allows the SO User to monitor current IoT network state and manage rules in the Flight Envelope. This has a dashboard showing device performance and it also displays operational limits that the device should not go over including one provided by the device manufacturer which if exceeded, will damage the device.



CASE STUDIES – IN BRIEF

BOSMAL

ELIoT Pro is already up and running at Bosmal, a state-of-the-art automotive testing and R&D facility in Central Europe, which provides comprehensive services in the area of engine and fuel technology, as well as other automotive technologies.

Bosmal now deploys ELIoT Pro's password-free, multifactor, one-touch secure login to enable authorized users to login, manage, and control the production processes in the IoT environment.

In the coming months, Cyberus Labs will integrate other ELIoT Pro components in Bosmal's smart production plant system. As well as our M2M credentials-free authentication between computers, ELIoT Pro's EP Cortex will provide additional security to the manufacturer's system.

KATOWICE

The southern Polish city of Katowice is a pioneer when it comes to introducing Smart City components in Poland. And in partnership with the Katowice City Office, Cyberus Labs is running a pilot implementation of ELIoT Pro's multi-layered security components.

System users now access their smart city programs and platform through our password-free, one-touch secure login dashboard, where they can monitor data that is being sent from various sensors, including CCTV cameras. Our Lightweight Encryption technology enables credentials-free authentication between devices all over the city while EP Cortex runs its rules engine to handle performance monitoring.

Three layers of cyber security working together as one

ELIoT Pro takes a step-by-step approach to achieving genuine end-to-end security for IoT devices that is firmly built on three mutually dependent pillars. And with each step taken, our level of security intensifies.

1. Beginning with **H2M authentication**, the first layer eliminates the password through the use of one-time transaction codes conveyed via a sonic transmission. Users can simply open an app on their phone and place it near their computer in order to escape the friction and hassle so many of us associate with the login process.

   Read the whitepaper

2. Building on this initial platform and with the wide expanses of the IoT ecosystem firmly in mind, the next layer brings us a level deeper again. By implementing a strong variant of **lightweight encryption**, ELIoT Pro can provide a high level of security to IoT devices with even the most minimal computational ability.

   These two defensive layers work in tandem to provide a new level of protection in our increasingly connected world.

   Read the whitepaper

3. The third and final layer brings IoT cyber security to its deepest level yet. Putting in place a data analytics element we call **EP Cortex** which acts as an IoT immune system, a complete end-to-end solution has now arrived. Through deployment of rules engines, device profiling functionality, predictive analytics, artificial intelligence, and just-in-time device replacement, **EP Cortex** provides a self-healing capability to any IoT system.

Conclusion

As our IoT ecosystem has grown larger, it has become more difficult for SOs to manage networks and identify cyber security threats in today's IoT world. At Cyberus Labs, we believe that robust analytics has a key role to play in helping SOs increase visibility and vigilance across their IoT networks.

In an IoT context, SOs must be made aware of component device activity and need to be clear if a given device is being deployed incorrectly or operating outside either intended or optimum parameters. This level of knowledge will enable them to act and respond as the situation demands it.

NEXT STEPS

Greater vigilance achieved through functionality like automated rules engines and device profiling can give SOs the insight they need to run their networks with increased efficiency and peace-of-mind.

With ELIoT Pro's data analytics layer EP Cortex already successfully implemented across many use-cases and industries, it's clear that monitoring and profiling can play a crucial role in the next phase of IoT security.

In part IV (entitled Stay Ahead of the Hack) of our four-part white paper series, we'll explore artificial intelligence in IoT cyber security. We'll also examine how predictive analytics and just-in-time device-replacement play a key role in creating a self-healing capability which is key to maintaining a solid level of security for IoT networks today.

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, 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 SOs 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.

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