CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE
OF TECHNOLOGY

CAIS – CYBER ATTACK INFORMATION SYSTEM

Cyber Security Intelligence Solutions for Industry Control System Protection

THE TIMES THEY ARE CHANGING

Foreword by Helmut Leopold, Head of Center for Digital Safety & Security,
AIT Austrian Institute of Technology.

In our modern, globally networked and digitally determined society, the rules for controlling digital technology have fundamentally changed, with positive consequences for our social and economic development. As the result of comprehensive networking in all areas of our lives, we are building complex systems which no longer display deterministic behaviour. System of Systems, the Internet of Things (IoT), and Cyber Physical Systems (CPS) all indicate the increasing complexity of our technological platforms, making it ever more difficult to understand the systems thoroughly and in detail, and to define fixed rules for describing correct system behaviour.

For economic reasons, as well as a lack of awareness amongst customers, economic stakeholders and society at large, we have failed to develop a culture of security in a global context. From the perspective of technology use, we are all very casual in dealing with passwords and electronic access security. Manufacturers of technological equipment for all sectors of industry, whether modern vehicles, industrial control systems, power networks, or smart homes, etc., are still not making security mechanisms an integral part of their development processes.

This ongoing process of digitalization is leading both to ever greater dependency on technical systems, and to a constantly growing risk from using them. At the same time, the scale and professionalism of the threats themselves have changed significantly in recent years. In the beginning interest focused on the technology itself, and the first viruses were developed without any commercial interest. In recent years, however, political and economic interests have become key motivating factors. As a result, the threat is no longer single hackers working in isolation, but organised structures making substantial investments into dedicated attacks.

It is only in recent years that this massive development has reached its current dimensions, presenting not only industry, but also society, with new challenges in dealing with the cyber domain. In order to master these challenges, every decision-maker and every customer must be thoroughly aware that secure systems are not only a cost factor, but also an absolute necessity if we are to create a common secure, global infrastructure for our digital society, and to comprehensively protect our private spheres.

CYBER SECURITY INTELLIGENCE SOLUTIONS MADE IN AUSTRIA

Seen in this light, it is necessary to adopt comprehensive, joint research efforts to make our technological systems more resilient to failures and hostile attacks. We must learn to understand much more clearly how our social processes depend on individual technological systems if we are to put appropriate measures in place within an economic and social context.

Austria has leading researchers in a variety of fields as well as world-class expertise. In the field of cyber security, technology development here at AIT concentrates in particular on protecting critical infrastructures and industrial control systems, with the following focuses: special system designs for resilient industrial control systems and critical infrastructures (security by design); novel smart encryption processes for the Internet of Things (IoT) and cloud systems to ensure the highest possible levels of data security and the protection of the private sphere; a revolutionary immune system for technical systems in the form of intelligent and adaptive software (machine learning) which detects even the most sophisticated cyber attacks; and finally, suitable cyber-testing and training platforms (cyber range) to help IT system developers and operators acquire special skills.

EUROPEAN CYBER SECURITY FRONT-RUNNER

Thanks to the special expertise at AIT, Austria is regarded as a high-tech location for cyber security in the international arena. Based on its rich experience in digital safety and security, AIT has positioned itself as a reliable partner to national authorities engaged with the topic on a nation-wide scale, and is a well-respected expert institution for cyber security within the European scientific community. Experts at AIT are creating leading-edge technologies and solutions based on machine-learning technology appropriate for the future cyber defence ecosystem, to tackle the cyber threats arising from the emergence of comprehensive ICT networks with their increasing interconnectedness and unclear attack surfaces. These special IT security solutions will set new standards and help to ensure that Austrian products remain competitive in the global market as a result of Austrian research expertise.

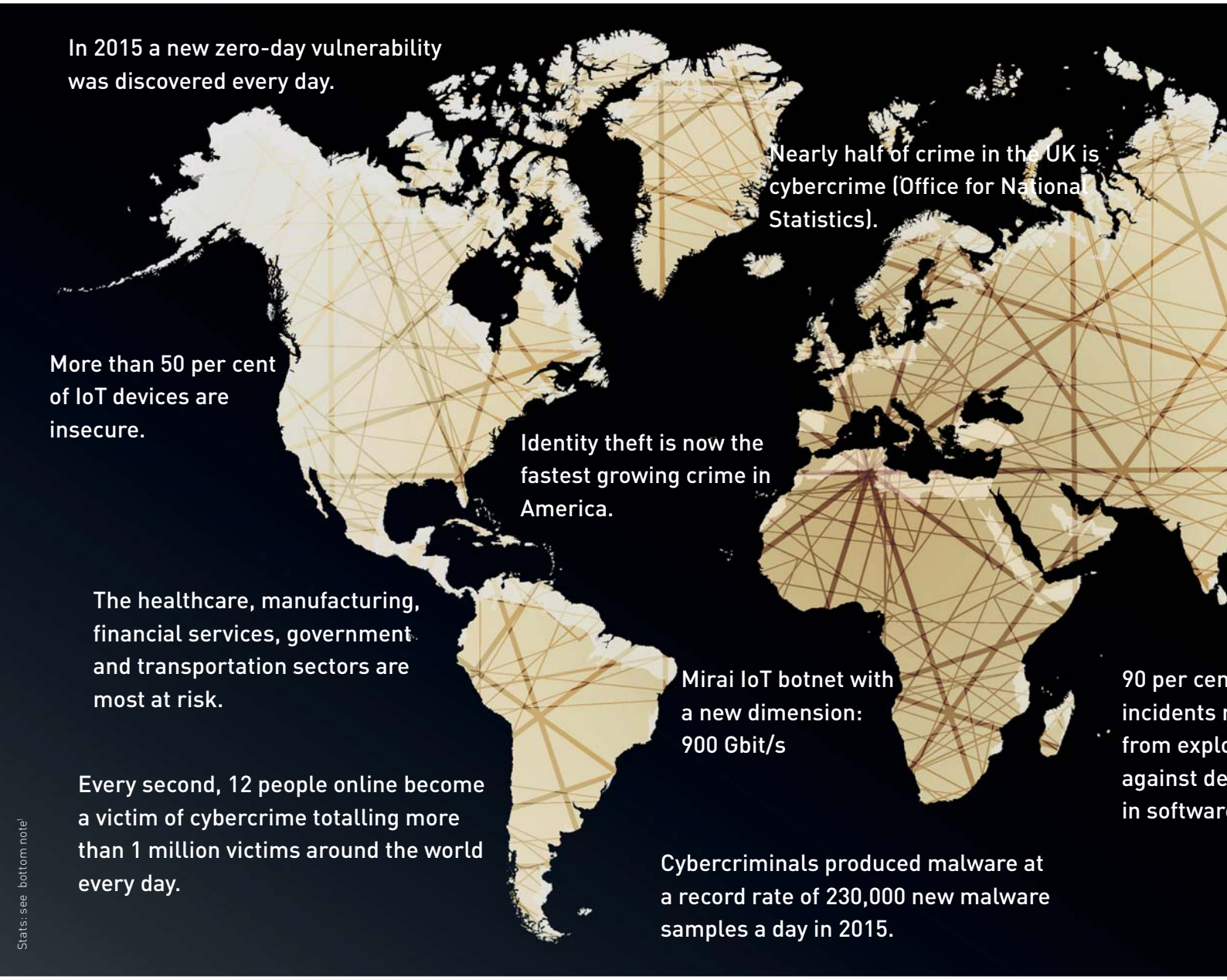
A NEW RESILIENCE THROUGH MACHINE LEARNING FOR OUR COMPLEX DIGITAL SYSTEMS

The growing complexity of our IT systems demands new mechanisms to protect them from advanced cyber attacks, to detect operational anomalies caused by complex system behaviour, and even to identify failures in operational processes made by IT system users. Three elements are crucial to building tomorrow's resilient digital IT systems: novel risk management solutions based on well-defined threat catalogues, the harmonization of safety methodology with security methodology (safety & security co-design), and real-time monitoring of IT systems for anomaly detection based on novel machine-learning concepts.

Helmut Leopold, Head of Center for Digital Safety & Security, AIT

We are starting to build artificial intelligence into our digital systems in order to create resilience to any influence which could destabilize our IT systems.

CONTENTS



THE GLOBAL CYBER THREAT MARKET

A status quo of today's worldwide cybercrime marketplace.

For a more precise picture of cyber threats we first need to look at the phenomenon from two different angles. Firstly, in terms of global spending on cyber security products and services, in 2016 Cybersecurity Ventures estimated that the figure will eclipse $1 trillion cumulatively for the five-year period from 2017 to 2021. However, current IT forecasts appear unable to keep pace with the dramatic rise in cybercrime, the speed of the ransom epidemic and the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices and the legions of hackers-for-hire, as well as the more sophisticated cyber attacks launched at businesses, governments, educational institutions, and consumers globally.

Secondly, it is estimated that the annual cost of global cybercrime will grow from $3 trillion in 2015 to $6 trillion by 2021. This includes factors such as damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigations, restoration and deletion of hacked data and systems, through to reputational harm, to name a few. Our interconnected world will also cause an unprecedented rise in data volumes, offering a larger target area for cybercrime activities. International experts expect that in 5 years' time we will need to defend 50 times the volume of data that we defend today. Added to that, in the years to come the Internet of Things (IoT), with new electronic devices used in consumer electronics, wearables, medical applications, Industry 4.0, automotive, public safety and the environment, will open up new entry routes for criminal intruders.[1]

The underground black market is steadily on the rise. Today's cybercrime forums have become highly professional domains populated by well-organized criminal enterprises and even some nation states. Inside knowledge on how to commit profitable attacks has multiplied greatly since the early days of sporadically organized ad-hoc gangs whose main motivation was notoriety and ego.

Today the black and grey markets are cyber-extensions of organized crime and they have matured significantly in recent times. In other words, 20% of professional criminals have adopted sophisticated and specialized skills, and they operate their destructive tasks using smart and highly advanced technologies. With their capacity for stealing intelligent IT tools, the service offerings have become more extensive, ranging from the sale of stolen credit cards, bank accounts, IP and email addresses, to phishing and spam attacks, on-demand DDoS takedowns and easy-to-use botnets.

Today anyone with criminal energy can rent the necessary weaponry at low prices from agents in the darknet in order to execute variable attacks. And the most dangerous face of the new cybercrime world order is that the perpetrators themselves don't even need to be skilled in their field. Where there is a lack of cybercriminal talent, others are available who can be hired for these tasks. Only money matters.

Additionally, criminal greenhorns can themselves easily become victims of more expert criminals who can rip them off, for example, by giving away 10 good credit cards for free before going on to sell them thousands of cards which are out of date and no longer valid, as a RAND study[2] reports.

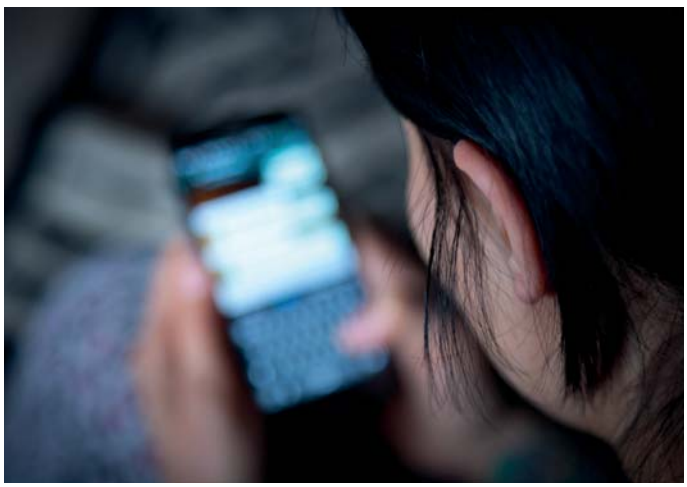
Expert predictions for future cybercrime developments are therefore pessimistic:

- Growing activity in darknets, more vetting of participants, more use of cryptocurrencies, greater anonymity capabilities in malware and more attention to encrypting and protecting communications and transactions
- Supported by such markets, the capacity to attack is likely to outpace the ability to defend
- Hyperconnectivity will create more points of presence for attack and exploitation, so that crime will increasingly have a networked or cyber component, creating a wider range of opportunities for black markets
- Exploitation of social networks and mobile devices will continue to grow
- There will be more hacking for hire, as-a-service offerings, and brokers[2]

The whole cyber threat defence industry urgently needs to bring its most powerful counterattack applications to the cybercrime scene, and to strengthen its technological maturity and intelligence in the years to come.

[1] "Hackerpocalypse: A Cybercrime Revelation", Steve Morgan, Editor-in-Chief, Cybersecurity Ventures; A 2016 report from Cybersecurity Ventures sponsored by Herjavec Group, Q3 2016; http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, page 6

[2] RAND, National Security Research Division; Lillian Ablon, Martin C. Libicki, Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar", Sponsored by Juniper Networks, 2014)



ADVANCED PERSISTENT THREATS (APT)

A definition of advanced persistent threats and how they are enacted.

Over the recent years the "black hat" community has developed many profitable identity theft schemes with massive quantities of personal data harvested from corporate and government sectors. Disruptive changes in IT infrastructure, and usage models such as mobility, cloud computing and virtualization, have dissolved traditional enterprise security perimeters and paved the way for "target-rich" environments which are now being attacked by enduring international espionage and sabotage campaigns in order to conduct IP (Intellectual Property) theft with actors originating from organized cybercrime.

Targeted attacks such as these are sometimes known as APTs (Advanced Persistent Threats). Advanced means that the criminal operators utilize the full spectrum of computer intrusion technologies such as drive-by downloads, SQL injection, malware, spyware, phishing and spam, to name but a few, in combination with social engineering techniques. If necessary, they improve their access tools to levels far beyond the commonly available DIY construction kits and off-the-shelf products. Using multiple "kill chains", such as zero-day vulnerability exploits, viruses, worms and rootkits, the offenders try to navigate through the penetrated network and successfully circumvent defence areas to abuse and compromise "trusted connections" by cracking encryption, thus pretending to be regular network traffic.

Persistent implies that the attackers give clear priority to a specific task and goal, and in most cases the criminals are guided by external entities. APTs follow a customized "low-and-slow" approach and are conducted through continuous monitoring and interaction to achieve defined objectives and stay undetected over a longer period.

In a next step APTs carefully gather confidential data and sensitive information such as trade or military secrets. They are commonly high aspiration cybercrimes focusing on full remote control of the targeted information infrastructure.

Therefore the organizations most at risk at becoming a victim of a serious and extensively prepared, advanced persistent threats are government agencies, manufacturers of highly competitive products on the global market, and critical infrastructure providers such as energy operators, power plants, governmental institutions, or data warehouses.

WHAT IS MACHINE LEARNING?

In the broader sense, machine learning refers to a series of techniques designed to train a machine to solve a problem. The starting point in the machine-learning process is feeding the machine with the right information on manifestations or typical patterns of some aspect central to the purpose of an information processing routine. After the machine has learned its lessons, by constantly repeating the trained recognition schemes (machine learning model) based on data analysis algorithms, it can improve its effectiveness through ever more accurate predictions of the future.

The emergence of data science, what we usually call Big Data, and the availability of cheap and plentiful computational power to store and transport datasets and give them meaning through interpretation, has spurred the machine-learning movement in recent years. There are two trends in the cyber security industry that will further enhance the performance of machine learning technologies in this field. Firstly, the collection of large amounts of raw data on an everyday basis is well underway, and a plethora of tools designed to sort, slice and mine data in a somewhat automated fashion are already available on the IT market. Secondly, the lack of qualified and experienced individuals to successfully defend vital infrastructure and systems will push demand for the adoption of machine-learning technologies in support of human cyber defence interventions.

There are many time-consuming cyber defence procedures which humans cannot exercise in the short timeframe necessary in the event of a serious attack. This makes machine learning a valuable tool for carrying out highly automated tasks such as determining stolen data, reviewing access logs or network traffic, screening unusual amounts of sensitive data flowing out of the network and tracking malware samples for data exfiltration. Machine learning will prove especially valuable for incident response teams in a 24/7 SOC (Security Operation Centre) as an early warning mechanism for real-time identification of dangers before any damage occurs. With the aid of timely insights offered by well-trained machines, human experts in the defence loop can focus instead on taking the final decision.

In a sense, the machine-learning approach for cyber threat defence is a special playing field related to cognitive network security, built on intelligent systems that can analyse incoming information and identify patterns as quickly as an initial attack itself. This gives IT security engineers the technological tools to defend attacks using human intelligence, but at machine scale in terms of the amount of supervised data flows and the speed of intervention.

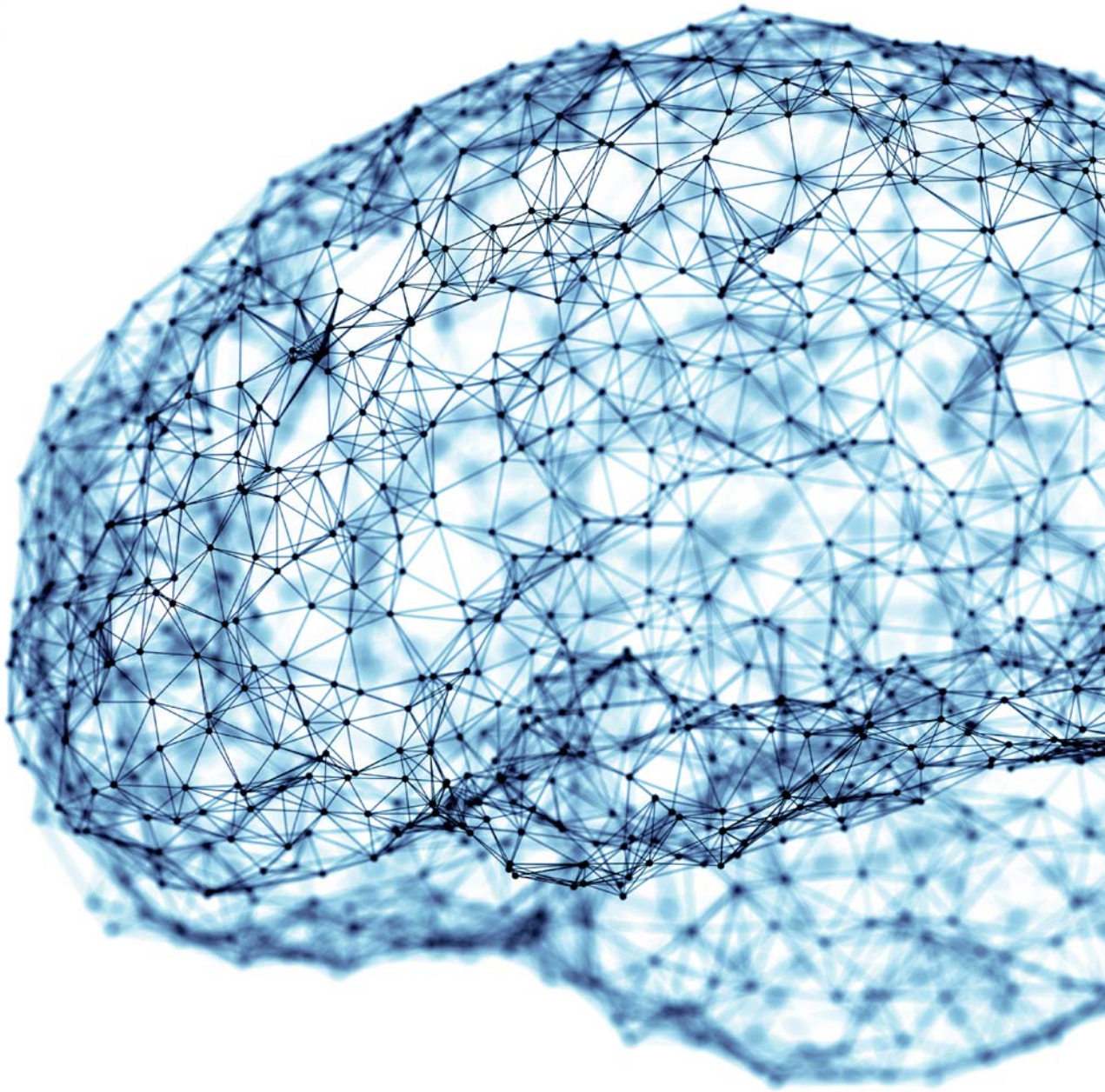
CYBER SECURITY RESEARCH AT AIT

Here at the AIT Center for Digital Safety & Security, we are aware that in this diverse world of countless emerging new cyber threats, 100% cyber security is an impossibility. But we can help businesses and administrations alike to enhance the resilience of their critical networks and IT infrastructures, and to protect their assets to the highest extent possible.

That's why our scientists are working on leading-edge machine-learning technologies and solutions appropriate to serve the future cyber defence ecosystem in order to tackle cyber threats arising from the emergence of comprehensive ICT networks with their increasing interconnectedness and unclear attack surfaces. For example, AIT has developed Automatic Event Correlation for Incident Detection technology (AECID), a patented solution inspired by approaches from the domain of bio-informatics, to build up system behaviour models to understand relevant events and their interrelationships. Our self-learning solution for adaptive network log stream processing can help to detect, classify and cluster frequently occurring patterns in log files and events, and to eventually distinguish the known good from unknown malicious activities in the IT infrastructures of enterprises.

The application is capable of understanding event correlations across systems, protocols and layers of varying abstraction levels, using multiple mining instances for increased scalability. AECID is applicable for legacy systems and proprietary systems with low market penetration. Users do not need to replace existing security solutions as AECID runs in parallel and can be connected to existing SIEM (Security Information and Event Management) tools.

AECID is part of the AIT Cyber Security Intelligence Solutions Portfolio which is described on the following pages.



THE AIT CYBER SECURITY INTELLIGENCE SOLUTIONS PORTFOLIO

A short overview of intelligent security technologies to counteract modern cyber threats.

The ever-growing complexity of cyber threats means it is simply a matter of time before cyber security businesses will have to adopt self-learning approaches if they wish to survive. Thus experts at AIT's Center for Digital Safety & Security, working closely with organizations from industry, science and the public sector, are developing modern information and communication technologies and systems in order to build and establish highly resilient ICT infrastructures for the future. The main focus areas include the essential pillars of modern next-generation cyber security protection: risk management, security by design and next-generation encryption for virtual IoT and cloud environments, post-quantum computer encryption, highly reliable and secure communication technologies, systems for anomaly and incident detection using machine learning methods, communication tools for intra-organizational information exchange on cyber incidents, as well as cyber range activities for capacity building in dedicated industries such as industrial control systems (ICS), automotive and Industry 4.0.

AIT´s digital safety & security experts offer specific cyber security intelligence solutions, comprehensive and long-term expertise in this complex field, and know-how in terms of capabilities for nationally and internationally-funded partnerships. On the next page you will find a selection of our research and development services.

CYBER DEFENCE THROUGH MACHINE LEARNING

The growing complexity of our IT systems demands new mechanisms to protect them from advanced cyber attacks, to detect operational anomalies caused by complex system behaviour, and even to identify failures in operational processes made by IT system users. AIT experts are working on leading-edge technologies and solutions based on novel machine-learning concepts appropriate to serve the future cyber defence ecosystem, in order to tackle the cyber threats arising from the emergence of comprehensive ICT networks, with their increasing interconnectedness and unclear attack surfaces.

In the field of blockchain technologies, experts are working on algorithmic solutions which can provide insight into functionality and transaction flows for the real-time analysis of virtual currency transactions. A particular focus lies in the detection of „anomalies", i.e. the identification of transactions and transaction patterns that deviate from the usual structures. The aim is to leverage the advantages of technology and prevent potential abuse.

SMART ENCRYPTION FOR IoT AND CLOUD SYSTEMS

When it comes to storage and processing, big companies and public authorities are reluctant to entrust their most sensitive data to external parties. AIT experts are working on concepts to better protect data in the cloud by means of novel agile cryptography. They are designing secure cloud services which support collaborative work on cryptographically-protected data, i.e., with support for selective fine grained access control and built-in resiliency. Furthermore, they are developing privacy-enhancing technologies which are used to build trustworthy identity management systems and privacy-friendly smart applications for cloud computing and the Internet of Things (IoT).

SECURITY BY DESIGN FOR CRITICAL INFRASTRUCTURES

In the context of smart grid technologies, integrating previously isolated components comes with two main challenges: the interoperability of components from different system levels and/or manufacturers, and high levels of resilience against cyber attacks. As part of the Austrian initiative for defining a reference architecture for secure smart grids (RASSA), together with all the relevant stakeholders including network operators, equipment manufacturers, energy suppliers, regulators and public authorities, AIT experts have developed methodologies and tools to model a reference architecture for secure future smart grid solutions.

AIT CAPACITY BUILDING AND TECHNOLOGY VALIDATION

Security is not just a technology issue – it encompasses processes, usability, operational skills and understanding system complexity. Together with the International Atomic Energy Agency (IAEA), AIT has established a "cyber range" training centre to share AIT´s extensive knowledge and to train and raise all stakeholders from industry, science and the public sector to a common level of knowledge. A cyber range is a virtual environment for the flexible simulation of large and complex networks with different system components, networks and users. It offers a safe and realistic environment to test, investigate and analyse incidents in various, scalable scenarios without using the actual production systems. With its flexible architecture, a cyber range can be used for diverse applications such as training, evaluation of incident response processes, and software testing. This allows researchers and stakeholders from industry and government to work together within realistic environments on the design, implementation and validation of methods, technologies and processes for establishing an increased level of defence against cyber attacks.

INTERNATIONAL SECURITY PROTECTION MECHANISMS AT THE COMPANY LEVEL

Cyber attacks, whether with criminal, espionage, terrorist or even warlike intent, are becoming extremely professional and sophisticated. Resilience to these threats has become a key factor in the success of modern enterprises.

INTERNATIONAL CYBER SECURITY INITIATIVES

Several measures have been initiated at EU as well as national level to establish a system of European cyber protection. The EU has defined a cyber security strategy[3], as well as a recommendation[4] for prevention and response to disruptions and attacks affecting European critical infrastructures. Dedicated structures for cyber security management at a state level, minimum security protection mechanisms at company level, and mandatory reports on serious cyber incidents are all measures being discussed by certain companies and organizations in order to increase the resilience of our digitally controlled infrastructures. Furthermore, the EU's NIS Directive[5] requiring the implementation of national cyber security laws entered into force in August 2016.

In Austria, a national law elaborated by the Austrian Federal Chancellery (BKA), the Ministry of the Interior (BMI), and the Ministry for Defence and Sport (BMLVS), will come into effect in 2018[6]. A European-wide EU data protection law will also enter into force on 25 May, 2018, requiring companies to prove to the authorities that they are sufficiently protecting personal data. Protective measures include risk analysis and implementing cyber security systems.

INDUSTRIAL COUNTERMEASURES

However, in order to manage these far-reaching security issues, industry must focus on five essential issues:

- Creating fundamental understanding of digitalisation technologies and the security aspects vital for every company
- Redefining priorities: new skills and new processes are required in order to adopt a holistic view of systems
- Establishing a modern risk management strategy enabling suitable protective measures to be implemented in an effective and targeted manner
- Security and privacy by design approaches to integrate security concepts into system solutions right from the start
- Deployment and use of modern intrusion detection and defence tools in a coordinated approach to combat threats emanating from the internet, and a joint defence strategy

[3] http://www.consilium.europa.eu/de/policies/cyber-security/
[4] http://www.spiegel.de/netzwelt/netzpolitik/cyber-gesetz-eu-kommission-einigt-sich-auf-nis-richtlinie-a-1066642.html
[5] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[6] http://www.bmi.gv.at/cms/cs03documentsbmi/1326.pdf

A STATE-OF-THE-ART SECURITY SHIELD

DEFAULT SECURITY INFRASTRUCTURE ASPECTS OF A MODERN ENTERPRISE

When establishing and maintaining an enterprise-wide state-of-the-art security infrastructure the following security categories and aspects must be considered.

CYBER SECURITY TEAM

Firstly, an enterprise needs a dedicated cyber security team which deals with security aspects on a daily basis. This team needs to organize the network, operate the network entities, and continuously adapt all network elements (firewalls etc.) to the current workflow and working behaviour. And last but not least, this team has to deal with all anomalous behaviour in the network, interpret log files of firewalls and servers, and fight recognized attacks.

RISK MANAGEMENT

Critical infrastructures increasingly depend on information and communication technologies with the consequence that cyber security risks are becoming a threat in all types of industry sectors, including energy, automotive, healthcare or production. Every infrastructure provider needs to find answers to critical questions such as:

- What if data is stolen or disclosed? The system is down, out of control, or modified?
- How can I detect misconduct? Or a modification? Or a deletion?
- How can I recover the system from an uncontrollable state?

In response, AIT is offering technologies and tools to strengthen the resilience of critical infrastructures, such as smart grids, to cyber attacks. AIT´s portfolio includes specific risk management approaches for utility providers, processes and guidelines for implementing security in infrastructure environments, as well as security assessment and monitoring solutions.

SECURITY BY DESIGN

Modern ICT systems need to be engineered with security "built in" from the start. Therefore methodologies, techniques, and tools to facilitate secure and efficient system design and implementation are highly in demand. The methodologies leverage existing technologies such as cryptography and federated identity management, and take innovative approaches such as model-driven security for ensuring the confidentiality, integrity, and availability of large-scale distributed systems. Furthermore, a system is only as secure as its weakest link. Security engineering tools must therefore make it easier for system engineers to adhere to security requirements in different stages of the software development lifecycle, including design, implementation and testing. AIT offers the development of "security by design" architectures and supporting tools for secure software development lifecycles.

ENCRYPTION

Internet banking, secure payment systems, digital signatures – all would be unthinkable without the use of modern encryption technologies. Designing next generation secure and intelligent communication systems raises many new challenges which also call for new approaches in cryptography. Therefore AIT offers new cryptographic methods and investigates how these can be used to make tomorrow's ICT systems safer. Methods, concepts and prototypes are developed to help protect user data and enhance privacy in the interaction with ICT in the context of cloud computing and the Internet of Things (IoT).

CLOUD SECURITY

Cloud computing is one of the most important IT trends in recent years and has led major companies to invest heavily in cloud infrastructures. The cloud computing paradigm shares many aspects of current IT enterprise infrastructures (e.g. security management in organizations, facility management, regulatory frameworks), but with increasing concerns about security, reliability and information security. Therefore AIT offers state-of-the-art concepts, methods and technologies for implementing protected, reliable and highly secure cloud computing environments for critical IT infrastructures.

SAFETY & SECURITY CO-DESIGN

Interconnected embedded systems integrated into the physical surroundings are known as cyber physical systems (CPS). These are the driving force behind many technological innovations designed to improve efficiency, functionality, and the reliability of products, services and infrastructures. In turn, our society is becoming dependent on these 'intelligent' or 'smart' systems which are used in everything from smart home appliances to industrial controls, smart cities, and intelligent transport.

Owing to the scale, complexity, and connectivity of these systems, ensuring their safety, security, and resilience is a very challenging task. Faults and malfunctions as well as malicious attacks can cripple a system and lead to devastating consequences in the physical world, eliminating all the advantages technology brings. Since system features increasingly depend on computation, network, and information processing, safety and security become tightly coupled in CPS. Safety cannot be guaranteed without security.

An integrated process for cyber security and safety has the advantage of a common resource set, thus requiring fewer additional resources. AIT is actively involved in standardisation activities to foster safety and security co-engineering and to promote joint approaches.

SECURITY CHECKLIST

The basic measures to be taken in any organization can be divided into three categories: network, data and people. Use this checklist to identify the general status quo of your security infrastructure level.

NETWORK MANAGEMENT

1. Network sections according to security plan
Separate critical areas from the normal network (also physically). Allow only a few interconnection points. Avoid empty access points where someone can plug in a computer.

2. Effective domain management
If users do not need access to a particular network or computer, don't give it to them. Not all workstations need to be connected to other workstations. Where users need access to particular networks only on an irregular basis (e.g. for maintenance purposes) then they should use different accounts.

3. Least-privilege access control
Access control should be granted by application to the data owner, and all control should be audited periodically. Avoid "grant-to-all" possibilities, especially in cloud environments.

4. Role-based access control (RBAC)
RBAC provides least-privilege control determined by authorized actions and the role of the user. In RBAC systems, least-privileged permissions are granted to role-based groups instead of user accounts or departmental groups.

DATA MANAGEMENT

1. Data leak prevention
Effective monitoring systems can help prevent access to, or transfer of, unauthorized data. However, they must be configured to identify unauthorized data and finely tuned to avoid a large number of false positives. More importantly, somebody needs to be accountable for monitoring and acting on the information identified by these systems.

2. Encryption
Implement encryption in order to protect sensitive data both in transit and at rest, including on storage media such as portable hard drives and USB keys.

3. Design security into your system from the outset
Poor default security or misconfigurations cause many security incidents. It is important to ensure all computers have been configured using industry-accepted best practices.

PEOPLE

1. Basic background checks
Many internal attacks are committed by repeat offenders. Organizations are advised to perform background checks on employees, including at former employers where suspicion is high.

2. Acceptable use policy
Acceptable use policies are helpful to establish the behaviour expected from employees. They should sign an agreement that clearly states that accessing unauthorized data is a serious offence, and which educates them about good password practices and physical security protections. External drive handling should be explained as a critical action.

3. Effective HR termination procedures
Every company should have a standardized termination process for when an employee leaves the company. This should include the prompt termination of the person's access to company buildings and digital networks.

4. Access rights associated with role / function
As an employee changes roles within an organization, companies should formally reassess their access rights in order to ensure that permissions and access do not simply accumulate. Passwords that were previously known to the transferred employee should be changed. In general avoid passwords for teams – always use individual passwords.

5. Supply chain & third-party agreements
A significant number of data breaches are performed by trusted third parties. All third parties should sign an acceptable use policy, and all programs they use should observe good security hygiene procedures, such as having up-to-date anti-virus protection and firewalls, etc.

6. Separation of role and functions
Policy controls should be put in place to prevent a single employee from abusing their power and significantly damaging the company. For example, highly-privileged accounts should be separated from the user's regular account. That means different accounts for different tasks.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Markus Kommenda
Business Development
Center for Digital Safety & Security
Phone +43 50550 4180
Donau-City-Straße 1, 1220 Vienna, Austria
markus.kommenda@ait.ac.at
www.ait.ac.at

Production manager: Michael Mürling; images: iStock.com, AIT