ISSN 2599-8293

European Commission

CORDIS Results Pack on cybersecurity

A thematic collection of EU-funded research innovation results

October 2018

Securing cyberspace: Concrete results through EU research and innovation

Research and Innovation

SECOND EDITION

Contents

Editorial

The steady increase in cyber-attacks on ICT devices, systems and networks, along with the lack of guarantees and control over data privacy, are major concerns for citizens, industry and decision-makers alike. The European Union has the ambition of being a global leader in cybersecurity, ensuring trust, confidence and protection of citizens and enterprises.

This is why the Commission's proposals for the next multiannual EU budget starting in 2021 will include a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres. The purpose is to support industry and the public sector in adopting state-of-the-art security solutions made and pioneered in Europe.

Cybersecurity: Policy challenges and EU action

Through the Seventh Framework Programme (FP7) and Horizon 2020 projects, the Union is focusing on areas such as cryptography, digital authentication and privacy-enhancing technologies.

In two years from now, the EU will have invested close to EUR 1 billion in cybersecurity and online privacy projects, be it under FP7 or Horizon 2020. Close to half of this will have been within the framework of the contractual public-private partnership on cybersecurity for the period 2017-2020.

Highlighting innovative EU research efforts

This CORDIS Results Pack showcases some of the most promising and successful of these EU-backed projects. It covers the likes of novel security frameworks and recommendations for businesses, technologies tackling issues related to increased device interdependence and networking, authentication, cryptography, innovative solutions for developers and privacy-control tools.

These projects, of course, provide just a glance of what EU researchers are currently working on. The EU sees cybersecurity as a key enabler for its digital economy, and many new projects will continue to be funded over the coming years.

An advanced approach to security accountability for cloud service providers

As business and personal data increasingly move to the cloud, protecting the information – and tracing responsibility for privacy leaks and breaches – has become paramount. To address this, the A4CLOUD project developed guidelines for security accountability.

Portable heart-rate monitoring devices, which are for example very popular among joggers, are just one of the many devices that nowadays collect sensitive personal information. When combined with Wi-Fi or GPS-enabled technologies, they create instant online records for the user, as well as for hospitals, insurance companies and other intermediaries along the information value-chain who process personal data via the cloud.

The cloud raises a lot of questions about the accountability of the handling of personal data: How is it handled? How do we trace who is responsible if things go wrong? Indeed, because the cloud is relatively new, there are no established rules of accountability and transparency that apply to it.

"It's all about data privacy – as an individual and an organisation," says Julie Grady, a researcher at Hewlett Packard Enterprise in the UK. "Companies have to be accountable for the security of their data and the remedies, and take responsibility for how they do that."

Framing the accountability guidelines for cloud service providers was the goal of A4CLOUD (Accountability for Cloud and Other Future Internet Services), a recently completed cybersecurity research project co-funded by the EU and coordinated by Grady's company.

A4CLOUD's main objective was to frame an 'advance' approach to accountability for cloud service provision ecosystems ahead

of the EU's General Data Protection Regulation (GDPR), which entered into force in 2018. This was done through a survey of current and best practices across the Member States and by coming up with detailed check-lists of tasks that cloud service providers and their customers should do to ensure transparency and accountability regarding data protection.

Our biggest challenge was trying to reconcile the technical with the legal, making sure that these work together.

"Our biggest challenge was trying to reconcile the technical with the legal, making sure that these work together. Implementation of this by cloud-based business will be very challenging," said Grady. "All players, whether small or large, will be subject to the GDPR. On one level, it will be easier for the large ones since they have the means and have been accustomed to doing the due diligence anyway. Our checklists are really there for the SMEs."

Asked if accountability varies significantly from one Member State to the next, she gave a nuanced answer.

"Each Member State's interpretation has been slightly different. However, there have not been any big fines concerning data processing and the cloud so far: no one has been punished at the customer level. But that will change after 2019, so getting the good-practice guidelines in place is important. Most companies won't worry about this until the regulatory 'stick' comes into the picture. So in that sense, we were ahead of the curve with A4CLOUD," said Grady.

PROJECT
A4CLOUD – Accountability for Cloud and Other Future Internet Services

COORDINATED BY
Hewlett-Packard Limited in the United Kingdom

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
a4cloud.eu

Protecting personal data in a secure online environment

An EU-funded project has developed a secure means of accessing online services that requires users to provide minimal personal information. This privacy-enhancing technology could have significant applications in large institutions such as schools, universities and organisations with high levels of customer contact.

When you log into social media, access a restricted site or perform any number of online activities, the identification and authentication procedures that you have to follow help to keep your transactions safe. There are growing concerns however that the amount of personal information you are required to share could represent an unnecessary breach of your privacy. This is why the EU-funded ABC4Trust (Attribute-based Credentials for Trust) project has developed a new approach that aims to keep systems secure while protecting users' identities.

When less is more

"Many websites require 'over-identification', which means that they ask for knowledge about you that is simply not needed," explains project coordinator Prof. Dr Kai Rannenberg from Goethe University in Frankfurt, Germany. "Collecting lots of information in order to identify and authenticate people could backfire if this information gets into the wrong hands."

Through a series of groundbreaking trials, Rannenberg and his team demonstrated that users can be authenticated and authorised using minimal personal information, and enabled to choose 'what' information they are willing to share. This was accomplished using privacy-enhancing Attribute-based Credentials (Privacy ABCs). The technology has huge potential in institutions where data on individuals must be protected, such as in education, but also commercial scenarios in general.

"Privacy-ABCs allow users to log into a service by proving that only certain parts of a larger certificate are valid, such as belonging to a specific school class," explains Rannenberg. "While minimal data is necessary to access certain services, the integrity of the user is maintained."

Young digital pioneers

The ABC4Trust team showed in real life situations exactly how the new technology can benefit both users and institutions. At Norrtullskolan secondary school in Söderhamn, Sweden for example, pupils wishing to access online counselling services could not – until recently – use a pseudonym; they had to identify themselves by name so the school could check whether they were allowed to use them.

In order to maintain anonymity while guaranteeing security, the ABC4Trust pilot scheme issued each child with a 'deck' of digital certificates that validate information like their enrolment status, their date of birth and so on. Pupils, able to remain unidentified, appeared to be more willing to talk about their problems.

"Schools have to react to ongoing digitalisation, e.g. by introducing 'internet competence' into the curriculum," says Rannenberg. "Implementing Privacy-ABCs into school networks could be part of this. Active negotiations are now underway to integrate the pilots into larger systems, so in the not so far future we expect more European public services and other organisations to switch to Privacy-ABCs."

Another pilot trialled at the University of Patras, Greece provided students with a smart card that was used to obtain Privacy-ABCs, issued by the university. Students could use the card to anonymously collect proof of attendance by swiping it in front of a device set up in the lecture room. The card also allowed students to give anonymous feedback on their courses and lecturers, while ensuring that only students who attended classes often enough could take part in the polls.

In the not so far future we expect more European public services and other organisations to switch to Privacy-ABCs.

"While Privacy-ABC technology has been shown to be usable, improvements now need to be made, such as adapting it for smartphone applications," says Rannenberg. "Here the challenge is not so much the Privacy-ABC technology itself, but rather the insecurity of current smartphones compared to the smart cards used in trials."

The current version of the ABC4Trust Engine source code can be obtained from the ABC4Trust resource page. "It was a decision by the consortium to make the architecture implementation available to all, in order to improve applications," says Rannenberg. "App developers and eID providers have shown great interest in our work."

PROJECT
ABC4Trust – Attribute-based Credentials for Trust

COORDINATED BY
Goethe University Frankfurt in Germany

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
abc4trust.eu

Combined protections for greater security in mobile apps

As advanced as they have become from a purely technological point of view, smartphones still represent a step backwards from desktops in terms of security. Mobile apps and software are still largely vulnerable to attacks, and current software protections are often limited. The ASPIRE project has developed a turnkey solution for software vendors and developers to overcome these problems.

Mobile security statistics show little improvement since the first smartphone reached the market. According to Arxan, a market leader in mobile software protection, 90 % of apps contain critical security vulnerabilities and 46 % of app-making companies expect their products to be hacked within six months. And while protections are available on the market, they do not offer adequate protection, and are expensive or difficult to use.

"It is almost impossible for developers to determine the value they get for their money, or to assess the benefits and risks of investing in protection," Bjorn De Sutter says, coordinator of ASPIRE (Advanced Software Protection: Integration, Research and Exploitation) and Professor at the University of Ghent's Computer Systems Lab. Knowing that most organisations have limited budget to invest in the security of their apps, the market seems to be caught in a vicious circle.

This is where ASPIRE technology comes into play: "We tried to push the state-of-the-art by presenting concrete improvements," Prof. De Sutter explains. "For example, we have developed anti-debugging techniques that are really hard to circumvent. We pushed the boundary of combining a lot of protections, covering a wide range of features and challenges (such as source-level and binary-level deployment) while still meeting industrial requirements like cooperation with standard code compilers in which code generation cannot be controlled."

The consortium managed to demonstrate the feasibility of these academic solutions on complex, real-world use cases, and developed a decision support system with an in-built evaluation methodology for underlying software protection strength. "It is the first of its kind, as far as we know, to assist users in selecting good combinations of protections in light of their software, assets, and security requirements," Prof. De Sutter says.

© Vadim Ermak, Shutterstock

Combining strengths

One of ASPIRE's main strengths is the combination of various protection techniques. The point is of course to make the hackers' job more difficult, but also to account for the requirements of the multiple assets included in a single app. Last but not least, this approach enables the system to protect even the protection techniques themselves. As Prof. De Sutter points, such a combination of forces makes possible attacks so time- and effort-consuming that they are no longer seen as worthwhile.

Technically speaking, ASPIRE combines five lines of defence: data value hiding, code obfuscation, anti-tampering techniques, remote attestation, and renewability techniques. "Renewable techniques allow us to distribute different versions of the same program and to update programs frequently, so that successful attack paths, once they are identified by attackers, can only be exploited on a limited number of software instances and during a limited window of opportunity," Prof. De Sutter explains. The goal is to reduce the potential for an attack to become profitable, in the hope that the attackers will give up on attacking altogether.

To verify the reliability of their system, Prof. De Sutter and his team have opened a public challenge where hackers are provided with seven programs to defeat. Successful attackers are provided with a reward if they share their attack method with the consortium.

Looking ahead

The use cases run over its course have brought valuable knowledge that the consortium intends to exploit in the near future. There were some positive outcomes, notably the fact that the ASPIRE system can effectively be deployed on complex libraries embedded in Android apps, and the consortium also identified room for improvement in the effectiveness of some protections.

We pushed the boundary of combining a lot of protections, covering a wide range of features and challenges.

Most code generated under the project will be made publicly available after the project ends in October 2016, so that researchers can deploy, research and extend existing protections. "The industrial partners of ASPIRE are working on their exploitation plans, as for my group it will continue to build on these tools both for internal research purposes and for collaboration with industry," Prof. De Sutter concludes.

PROJECT
ASPIRE – Advanced Software Protection: Integration, Research and Exploitation

COORDINATED BY
University of Ghent in Belgium

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
aspire-fp7.eu

A cyber-secure communication platform for smart energy grid applications

The way we produce and consume energy is constantly changing, with new uses and applications coming up on a regular basis. However, all these applications continue to work in silos – making observation and control of the whole energy grid complex, inefficient and expensive. A flexible and secure communication platform supporting diverse applications at the same time could soon be brought to the market thanks to the C-DAX project.

Smart grids are typically defined by the multitude of applications, actors and communicating devices they bring together, along with their limited use of human intervention. Different, isolated software is used for the likes of metering, monitoring and fault detection, which inevitably results in unnecessary burden when it comes to configuring and managing the energy grid.

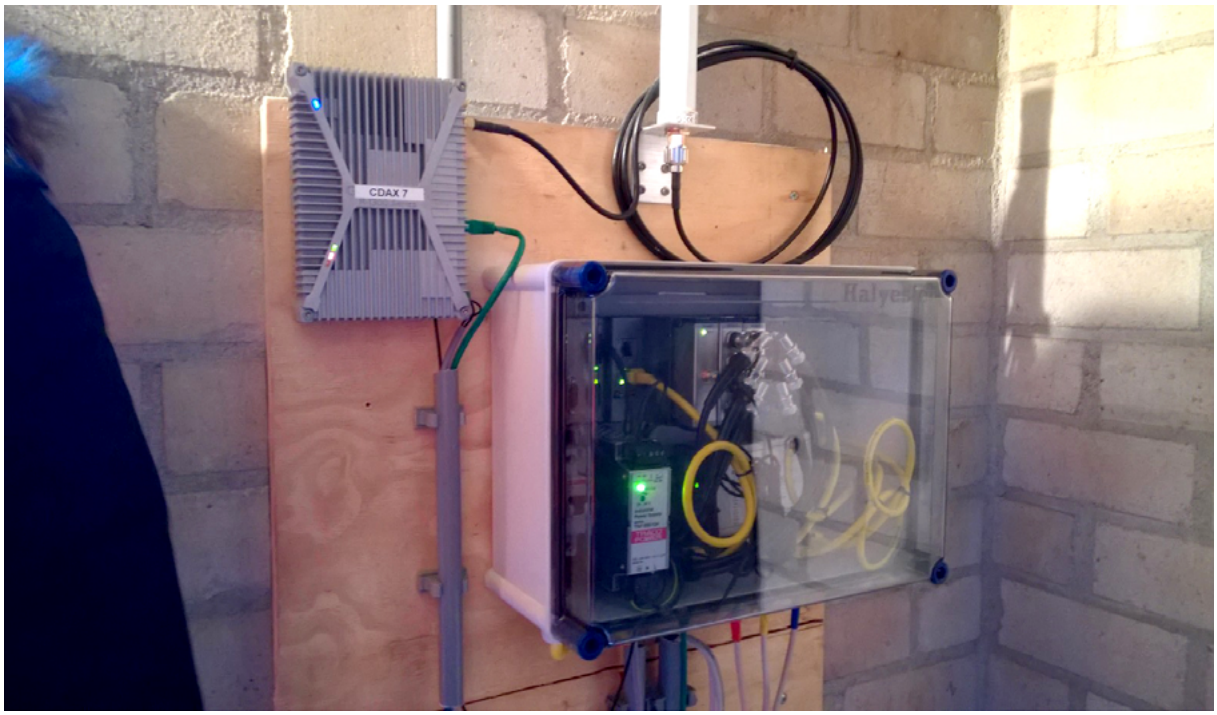
C-DAX (Cyber-secure Data and Control Cloud for Power Grids) technology solves this problem by building upon the concept of information-centric networking (ICN). This concept enables smart grid applications – for example electric vehicle charging, smart metering or grid monitoring – to exchange information in a secure, scalable, flexible and reliable manner.

To achieve this, C-DAX developed a cloud-based middleware that uses a topic-based publish-subscribe engine: While today's grids use individual silos to manage separate types of demands for electricity, the C-DAX approach virtualises these silos into topics which can be reconfigured and adapted based on current demand and constraints. To avoid security issues, the system decouples communicating end hosts. This simplifies the configuration of the system and provides inherent security protection to obscured target hosts.

The C-DAX platform can support applications with diverse requirements, ranging from retail energy transactions between large numbers of different actors to real-time grid monitoring applications.

"We support different communication modes (broker-based, query-based, point-to-point communication) and we use the adapter concept to encapsulate existing smart grid protocols. This makes our solution stand out when compared to other ICN-based communication systems currently used on the Internet, especially with respect to the integrated security functions," says Dr Matthias Strobbe, coordinator of C-DAX and project manager at iMinds. "Additionally, the C-DAX platform can support applications with diverse requirements, ranging from retail energy transactions between large numbers of different actors to real-time grid monitoring applications."

In addition to state-of-the-art security functionalities that grant only the strict minimal trust to intermediary communication nodes, the C-DAX architecture allows energy



© metamorworks, Shutterstock

distribution system operators (DSOs) to personalise their security parameters to the requirements of the deployed application.

"Aspects for each application can be selected, like the used cryptography function or key distribution mechanisms. For instance, latency-sensitive applications like Real-Time State Estimation of distribution grids (RTSE) can use fast symmetric cryptography, while smart metering can select stronger asymmetric cryptography for privacy-sensitive applications," says Dr Strobbe.

Real-time state estimation

One C-DAX application that particularly stands out is the RTSE of distribution grids using Phasor Measurements Units (PMUs). Concretely, this application provides operators with a perfect view of the status of their grids at any time. It supports all kinds of applications, from voltage control to congestion management, optimal dispatching of distributed energy resources (DERs) and fault location.

"We performed one major field trial on the distribution grid of Alliander (Dutch DSO), near Arnhem in the Netherlands, to demonstrate that the combination of the C-DAX platform and RTSE application can help operators to better manage their grids," Dr Strobbe explains. Ten PMU devices were deployed along with a power quality meter, and Vodafone's local LTE network was used as the underlying telecom infrastructure – a first for the exploitation of PMU data for RTSE.

"The results show that a real-time view of a distribution grid can be achieved via a public, wireless LTE network, that the added latency from C-DAX is negligible, and that the C-DAX resilience mechanism was both fast and reliable in the face of node and link failures," says Dr Strobbe. The use of PMU technology also showed higher refresh rates and lower measurement latencies compared to standard monitoring devices.

Whilst the project was completed in February 2016, project partners have remained active. Alliander and National Instruments are drafting plans to assess the potential of C-DAX for different uses and are planning to develop its code base. EPFL, the main developer of the RTSE application, is also exploring the possibility of creating a spin-off company to commercialise the project's PMU-based monitoring infrastructure. "We strongly believe that the combination of PMUs with RTSE can constitute the backbone of future smart grids," Dr Strobbe concludes.

PROJECT
C-DAX – Cyber-secure Data and Control Cloud for Power Grids

COORDINATED BY
iMinds

FUNDED UNDER
FP7-ICT

Novel security architecture for embedded systems soon to hit the road

Modern computing heavily relies on embedded systems built to solve very specific problems. At the same time, the advent of the Internet of Things means that these systems will be increasingly connected with each other, and the weakest link in terms of security can quickly take down whole networks and physical systems with it in case of hacking. The EURO-MILS project has developed a high-assurance security architecture to prevent such disasters from happening, which is currently being tested in automotive systems.

EURO MILS (Secure European Virtualisation for Trustworthy Applications in Critical Domains) is riding the wave of 'security by design' – in a world where many computing systems are built with security as an after-thought rather than a core functionality. This means that instead of producing devices that constantly need to be patched to ensure security – which is inefficient, time-consuming and costly – the four-year project has come up with a small virtualisation platform that offers the secure decomposition of complex embedded systems into independent components.

© Chesky, Shutterstock

"Networked systems need to be aware of surrounding systems and correspondently receive, handle, verify, process and send information. With embedded systems this problem is brought to a whole new level: interconnections create extremely complex systems and it becomes very difficult to guarantee security in systems combining components from various vendors," says Sergey Tverdyshev, coordinator of EURO-MILS and director R&T at SYSGO.

"In this context, what we bring to the table is a methodology that enables the system developer to generate security assurance evidence coherently with design decisions. There is no gap between what the system shall do, does, and why it does it correctly."

The MILS approach

As its name suggests, EURO-MILS relies on the Multiple Independent Levels of Security (MILS) approach – a high-assurance security architecture based on the concepts of separation and controlled information flow.

"The MILS approach provides a way to execute mixed-critical applications on one system and still to have that system certified to the highest security and safety assurance levels. This is extremely interesting for the likes of car infotainment systems: Android applications can run on the same platform as the AUTOSAR applications communicating with the engine," says Tverdyshev.

Thanks to a separation kernel that has already undergone avionic certification and is deployed in commercial aircrafts, the MILS approach separates system parts into independent security domains that can only exchange data via explicitly defined channels. System resources such as CPUs, CPU time, memory, IO devices or files are assigned to compartments, and the communication channels between these compartments are defined with respect of the required security policies and API.

A separation kernel brings separation by default, and any interaction has to be configured explicitly. This keeps the attack surface small and supports well secure development that emphasizes threat modelling at an early stage.

The MILS approach provides a way to execute mixed-critical applications on one system and still to have that system certified to the highest security and safety assurance levels.

A cross-domain approach

Over the duration of the project, the team developed use cases for the automotive and avionics industries – respectively a mixed-critical system able to prevent issues such as the recent hack of Jeep's electronic control unit and infotainment systems, and a gateway between two aircraft domains to control information flow exchanges according to pre-defined security policies and standards. Now, the partners are keeping busy by developing products for various other sectors.

"For example we are deploying our system in the subway of a European capital," says Tverdyshev. "Exploiting this cross-domain capability is of course very challenging, as we need to smoothly integrate and support existing practices and strong certification requirements for safety-critical systems in each of these sectors." This challenge is being tackled by the 'MILS community' established in 2014, which will take part in the biggest embedded systems trade-show 'Embedded World' in March 2017.

"Many results have already been translated into commercial products despite the fact that EURO-MILS was a research project," Tverdyshev notes. "There are automotive systems that already use project results in on-road testing and pre mass-production stages, and a brand new innovation project will pick up where EURO-MILS left off to target systems deployed in railway control systems, subway communication systems and smart grid control systems."

PROJECT
EURO-MILS – Secure European Virtualisation for Trustworthy Applications in Critical Domains

COORDINATED BY
Technikon – in Austria

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
euromils.eu

Innovative electronic IDs offer citizens vast range of public and private sector services

An EU project has built secure electronic identity infrastructure that could be used on a wide scale across the EU, providing many services and boosting competitiveness.

From a user account for government services to a user account with a clothing company, our daily transactions frequently take place online using several different electronic identities accessed via passwords.

But, these identities create security issues as well as problems in managing the many different passwords and accounts for the user. This could be overcome with a widely available, trusted and secure electronic identity system.

One EU-funded project, FutureID (Shaping the future of electronic identity), has created an innovative electronic identity system that could allow users to access a wide range of services from eHealth and banking to online shopping accounts – all within one secure system.

The concept is based on electronic identity cards that are already functioning in many EU countries such as Belgium, Austria and Estonia. However, FutureID expands the use of eID cards to cover access to health services, justice and law-enforcement, and secure tokens like those used by banks and the private sector.

"Identity theft is an enormous problem with password-based authentication and eID systems make ID theft much costlier for attackers," explains Heiko Roßnagel, FutureID project coordinator.

Moreover, "secure and trustworthy identities are increasingly important for allowing an ever growing number of transactions to take place on the internet. These are of vital importance to the functioning and efficiency of the EU's single market," says Roßnagel.

"Much of the competitiveness of Europe depends on finding a way of moving beyond the overly vulnerable electronic identities based on passwords," he adds.

Under the eID system developed by the project, users can use their existing electronic identities. The FutureID system is designed to support any eID card, token and mobile identity technology as well as being able to interact with current eID infrastructures.

"The FutureID approach is to take everything existing and add interoperability, enhance privacy and create a consistent user experience across a diverse range of services on top," says Roßnagel.

The project hopes to create a two-way draw: users will be attracted to the wide range of services. Meanwhile, service providers are attracted by the potential of a large number of users encouraging them to invest in the eID system.

"FutureID allows private sector players to offer services on what is essentially an open market place for intermediation services. This fosters competitive pricing, flexibility to market needs, support for niche markets as well as technological innovation," says Roßnagel.

At the same time, users can select how much personal information is disclosed, meaning that the system is attractive to users with privacy concerns.

Currently some eID systems disclose the full set of information contained in some eIDs to any service provider, even when only nationality or proof of age is required, explains Roßnagel. FutureID overcomes this, he says.

The FutureID approach is to take everything existing and add interoperability, enhance privacy and create a consistent user experience across a diverse range of services on top.

While eIDs are in their early phases, what is certain is that the internet has to mature beyond the use of passwords to remain useful and secure in the future. In some European countries roll-out of eIDs has already happened, but the availability of services that will attract users to activate their eIDs, install card readers or other systems and remember their PIN is still lacking.

"This is why FutureID has put so much emphasis on the private sector as only their services will make it worthwhile for citizens to actually use their eIDs", says Roßnagel.

With the project over, the key concepts are now in place for a successful and sustainable roll-out of very large-scale identity management infrastructures in Europe and beyond.

"Talks with a major stakeholder on how best to demonstrate very wide-scale use of this technology are already in their second round," says Roßnagel.

PROJECT
FutureID – Shaping the future of electronic identity

COORDINATED BY
Fraunhofer in Germany

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
futureid.eu

Novel protection against hardware trojan horses

Malware, viruses and other cyber-menaces typically target software. But equally dangerous – and growing – are the so-called trojan horses, that infect and physically manipulate computer hardware. The EU-funded project HINT has explored protective and detective technologies to keep computer systems free of these threats.

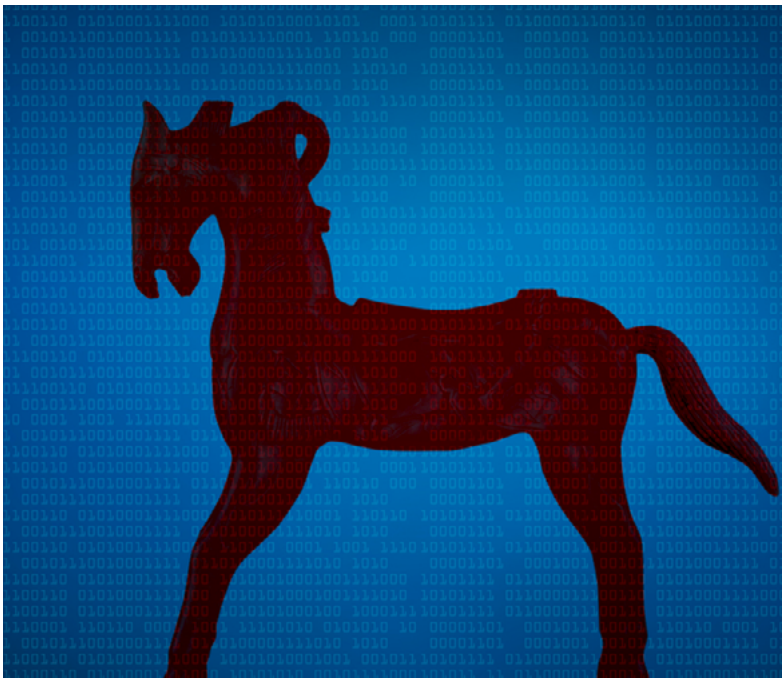
Trojan horses targeting computer hardware can take several forms, either as a physical alteration of original computer parts, a swap of counterfeited components into a computer system or hidden functions that manipulate the security features embedded in critical processing devices – particularly integrated circuits (IC) – in order to hijack, control or spy on their information.

These hardware trojan horses have been around for the past dozen years, though the computer manufacturing industry has traditionally been reluctant to talk about this because of fear of reputational damage.

Countering hardware trojan horses was the main goal of the HINT (Holistic Approaches for Integrity of ICT-Systems) project, whose research focused on developing 'integrity checking' of computer parts based on trusted computing technologies. After a 36-month, EUR 5.1-million effort co-funded by the EU that ended in September 2015, HINT participants are now working on commercialising the project's technologies. "This could save vast amounts of verification time and money", says Jacques Fournier, a researcher in embedded systems' security at CEA, French Atomic Energy Commission, one of the project's seven research consortium partners.

HINT was one of the first projects to produce tangible results in the area of IC aging and is now at a technology readiness level (TRL) of 3-4, with more tests planned to bring this level even higher.

"With the fast evolution of products and the complexity of the IC chain, there are now so many different actors in so many different locations that it is difficult to satisfy the trust of your supply chain," said Mr Fournier. "When it comes to niche markets you might be able to do that, but not for the large market where just-in-time delivery is imperative."



© wk1003mike, Shutterstock

Key to HINT was its research into "physically unclonable functions (PUFs) as a way to measure the unique characteristics, or fingerprint, of an IC and thus its security. The idea has been known about for 10-15 years but its commercialisation has been slow due to the plethora of technical issues that have to be addressed such as an IC's process variations, its sensitivity to temperature, aging, etc., all of which can alter its fingerprint.

HINT's innovation was to devise a PUF that addresses all of these, especially the aging function of an IC. It also developed a way to measure the malicious modification of a circuit as well as other tools.

According to Mr Fournier, HINT was one of the first projects to produce tangible results in the area of IC aging and is now at a technology readiness level (TRL) of 3-4, with more tests planned to bring this level even higher.

"For example, we've done a proof-of-concept for the integrity verification of programmable ICs and here we're at a TRL of 5-6. The next step will be a security proof-of-concept for other kinds of ICs such as application-specific integrated circuits. Once done, then we can go to classical chip manufacturers and promote it to them," said Mr Fournier. "Chip makers are very interested in this because the classical verification processes they currently have in place for smart cards are very costly."

PROJECT
HINT – Holistic Approaches for Integrity of ICT-Systems

COORDINATED BY
Technikon – in Austria

FUNDED UNDER
FP7-ICT

Working seamlessly and securely on multiple devices

EU-funded researchers have developed and tested a new corporate cyber security system – designed to fit with current trends of working on multiple devices – and identified a simple way of making corporate cyber space safer and more secure.

Mobility and modern living mean that work begun on the office computer is often completed on the laptop on the train home, or sent via smartphone to the client the next morning. While convenient and efficient, this practice can in fact expose corporations to cyber security threats.

"Company security protocols and practices have often failed to keep up with new technologies and how these are being used, both in the office and at home," explains project coordinator Sergio Zamarripa from S2 Grupo in Spain. "A key issue is the fact that the widespread adoption of mobile and portable devices has blurred the line between work and private life."

Trends, such as the spread of social networks and policies like Bring Your Own Device (BYOD), pose new risks. "Imagine an employee with a BYOD profile using the same device at home while some hours ago he was downloading a confidential document at work," says Zamarripa. "If the user is not aware that some actions could jeopardise confidentiality, a malicious attacker could obtain sensitive information."

In addition, large organisations are increasingly adopting complex ICT mechanisms, which require users to complete a series of complicated tasks. This increases the likelihood of human error.

© solarseven, Shutterstock

Adapted for the modern workplace

The MUSES (Multiplatform Usable Endpoint Security) project has addressed this weak link in the security chain through the development of a device independent, user-centric corporate security system, which is able to cope with the concept of seamless working on multiple devices.

The system interacts with users by sending them real-time notifications containing information and recommendations that relate to current user actions. Some notifications might simply offer suggestions on how to complete an action securely, while others will actively block an unsafe action and provide guidance to ensure that the action is completed safely (e.g. by connecting to a secure wifi).

"Corporate security policies should govern the way in which employees, devices and IT systems interact," explains Zamarripa. "What we wanted to do was to raise employee awareness of risky situations, and assist them in dealing with those risks. This will allow employees to carry out their work as usual, and help corporations to actively enforce security policies without introducing any new hurdles."

The MUSES consortium ran a number of field trials and found that the introduction of MUSES' usable corporate security led to a decrease in incidents due to improved user behaviour. "The trials revealed a gradual decrease in the number of incidents over time, as users were able to learn how they should perform their tasks in a secure way, through automatic recommendations provided by the MUSES software," explains Zamarripa.

Employer and employee benefits

The project has shown that engaging with users directly about cyber security can increase competitiveness and reduce direct and indirect costs associated with security incidents, such as down time and recovery costs, or indeed the cost of damage to reputation. "We have identified SMEs as the most likely target, since they usually do not have a security department," says Zamarripa. "The MUSES concept provides a cost-effective way of ensuring their assets, and a next step for the consortium is to look into ways of commercialising MUSES."

We have identified SMEs as the most likely target, since they usually do not have a security department. The MUSES concept provides a cost-effective way of ensuring their assets, and a next step for the consortium is to look into ways of commercialising MUSES.

The successful trials also resulted in increased awareness of the importance of trustworthy ICT among employees, and a better understanding of the legal and societal consequences of using both corporate and personal devices. Zamarripa also believes that the success of the project could open the door to future recommendations about standards, especially those related to BYOD.

PROJECT
MUSES – Multiplatform Usable Endpoint Security

COORDINATED BY
S2 Grupo in Spain

FUNDED UNDER
FP7-ICT

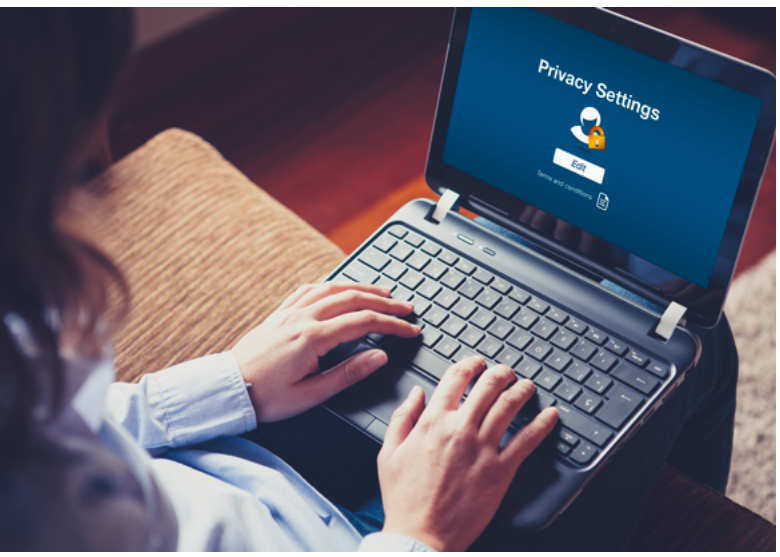
PROJECT WEBSITE
musesproject.eu

A holistic solution towards fair and transparent use of personal data online

Many online service providers still do not provide clear information as to how they protect personal data from their users. Combined with the latter's increasing wariness, this trend provides fertile ground for independent privacy service providers (PSPs). OPERANDO is trying to establish itself in this new market with easy-to-use privacy protection tools.

A PSP can be seen as a trusted link between the citizen (the data subject) and an organisation wanting to process their personal data (an Online Service Provider (OSP)). For the team running the OPERANDO (Online Privacy Enforcement, Rights Assurance and Optimization) project, this means allowing users to control access and use of their personal data, with the possibility of trading access to this data in exchange for economic or other benefits.

"Our main goal was to simplify privacy for end users. This is why OPERANDO offers a simple Privacy Dashboard allowing users to specify their preferences. These will be automatically compared with OSP privacy policies and translated into personal data access control decisions by the PSP," explains Reynold Greenlaw, coordinator of the project on behalf of Oxford Computer Consultants.



Over the past three years, the project has come up with four main innovations. The first is the PlusPrivacy application, which provides consumers with a unified dashboard to control privacy settings in the likes of social network accounts, email applications (hidden email identity), ad blocking, as well as the prevention of malware and unwanted apps from tracking and collecting private data. According to Greenlaw, PlusPrivacy is the most holistic solution available on the market.

The second innovation is a G2C privacy enforcement platform available to OSPs as a service. This platform includes a unique architecture for privacy protection, with modules for automated privacy policy decision making, user device privacy, user-centric privacy management and regulatory compliance.

For PSPs, OPERANDO provides an open-source software platform to offer privacy as a service, effectively turning these businesses into what the team calls a Privacy Authority (PA). "The PA may store the users' personal data securely and release it judiciously to authorised OSPs, based on the individual User's Privacy Policies (UPP). It further introduces the innovative concept of federation of Privacy Authorities, allowing PSPs to offer comprehensive privacy services in partnership with other PSPs," Greenlaw explains.

Finally, the project innovates by proposing a legally motivated privacy framework that aims for beyond-state-of-the-art ambitions to be standardised at European level. This includes translation of privacy and data protection into technical concepts and providing support for cross-border compliance with privacy laws of the EU, even if the OSP is located outside the EU. To privacy regulators, OPERANDO offers machine readable privacy guarantees, the ability to input privacy regulations in a semantic form, and automated compliance audits of OSPs. "The

project has also developed guidelines and tools for the privacy-by-design method used when developing the OPERANDO platform," Greenlaw points out.

All OPERANDO tools were tested through integration into existing services. These include: the handling of personal data by a UK volunteer-based social service providing support for vulnerable adults; the management of data from patients with specific dietary needs in an Italian hospital setting (FoodCoach); the management of personal information on adults being treated for gambling addiction (BetStop); and the registration of 'patient' (synthetic) data for fictional surgery.

Subjects reported greater awareness and engagement with their personal data, with a perception of being more empowered.

"Subjects reported greater awareness and engagement with their personal data, with a perception of being more empowered. As a specific example, 40 subjects were randomised to receive FoodCoach or FoodCoach + OPERANDO. The subjects from the OPERANDO group showed a greater engagement in terms of daily usage of the platform, due to the privacy enforcement offered through OPERANDO. They felt they had greater control of the data shared through the platform," says Greenlaw.

The project was completed at the end of April 2018. Project partners will now focus on commercialisation plans, which will include promotion in Italy following the recent evolution of the Italian online privacy protection legislation, as well as various social care scenarios in the UK. A global B2C PA based on the OPERANDO platform will also be set up for major online consumer services such as Facebook, LinkedIn and Google. "The cornerstone of the PA business model will be the virality of the service. We will particularly emphasise freemium pricing, the free basic service package for consumers and the various (paid) packages for OSPs," Greenlaw concludes.

PROJECT
OPERANDO – Online Privacy Enforcement, Rights Assurance and Optimization

COORDINATED BY
Oxford Computer Consultants in the United Kingdom

FUNDED UNDER
H2020-SECURITY

PROJECT WEBSITE
operando.eu

Achieving post-quantum cryptography before it's too late

With the ongoing global threat of unauthorised accumulation of encrypted data with the hope of eventually being able to break into it later, there is the real possibility that a large quantum computer could eventually fall into the wrong hands. This day will likely see current encryption systems fall like a house of cards.

This is a dire scenario, and companies and governments are starting to realise this. "Every day of waiting to roll out new systems is a day of data lost," says Tanja Lange from Eindhoven University of Technology. For the past three years, Lange has been running a EUR 4 million project to develop cryptology that can resist the power of quantum computers. And whilst the

consortium has made tremendous advances that single companies can already use, there is a growing risk that end-users will not have access to post-quantum cryptography by the time a big quantum computer is built.

Cryptography consists of two main components: symmetric cryptography – the workhorse for encrypting large volumes of data and for ensuring its integrity – and asymmetric cryptography, which is needed only at the beginning of the connection in order to get a shared key for the symmetric system. As Lange explains, "Asymmetric cryptography needs easy operations in one direction and impossibly hard ones in the other, except for those that have an extra key. Such a system can be compared to a padlock that can be closed with a simple push on the shackle but requires a key to be unlocked, so there is an asymmetry between closing and opening it."

Current computers are not very good at solving the mathematical problems used in current asymmetric cryptography, whereas quantum computers have some extra operations that make them trivial to break. And as these quantum computers are expected around 2025, the clock is clearly ticking.

Current computers are not very good at solving the mathematical problems used in current asymmetric cryptography, whereas quantum computers have some extra operations that make them trivial to break.

"With PQCRYPTO we have analysed exactly how vulnerable current systems are to quantum computers, how strong other, lesser-known systems are, and how to design new ones that can stand up to attacks using quantum computers while being more convenient to use," Lange explains.

Whilst the NIST (US National Institute for Standards and Technology) is currently running a competition to define the next-generation cryptosystems based on criteria such as confidence in the security of the system, speed, size and its practicality, Lange and her team have been trying to fulfil the demand of those who do not want to wait five or seven years to protect their data. "One encryption system we have very high confidence in uses cryptographic keys of 1 MB," she explains. "Before you can start sending encrypted data, you first need to download this key. But on today's internet, 1 MB can still be problematic when network connections keep cutting." Before this system can be widely deployed, many details still need to be worked out to avoid the likes of denial-of-service attacks. But it can already be used for file encryption or email, where keys are downloaded only once.

© Markusenes, Shutterstock

One of the post-quantum systems developed under PQCRYPTO (Post-quantum cryptography for long-term security), called New Hope, was recently at the centre of a Google-led experiment for some of their Chrome users. They concluded that the system was usable and, should it be needed, could be deployed for all connections to Google without feeling too much load on computation or bandwidth.

Despite all this progress, the road is still long before online communications become quantum-proof, and more research is needed to study the exact complexity of quantum attacks against NIST candidates, making the latter more practical and integrating them securely. As Lange points out, internet-wide deployment will only happen when all stakeholders have agreed on a single system.

PROJECT
PQCRYPTO – Post-quantum cryptography for long-term security

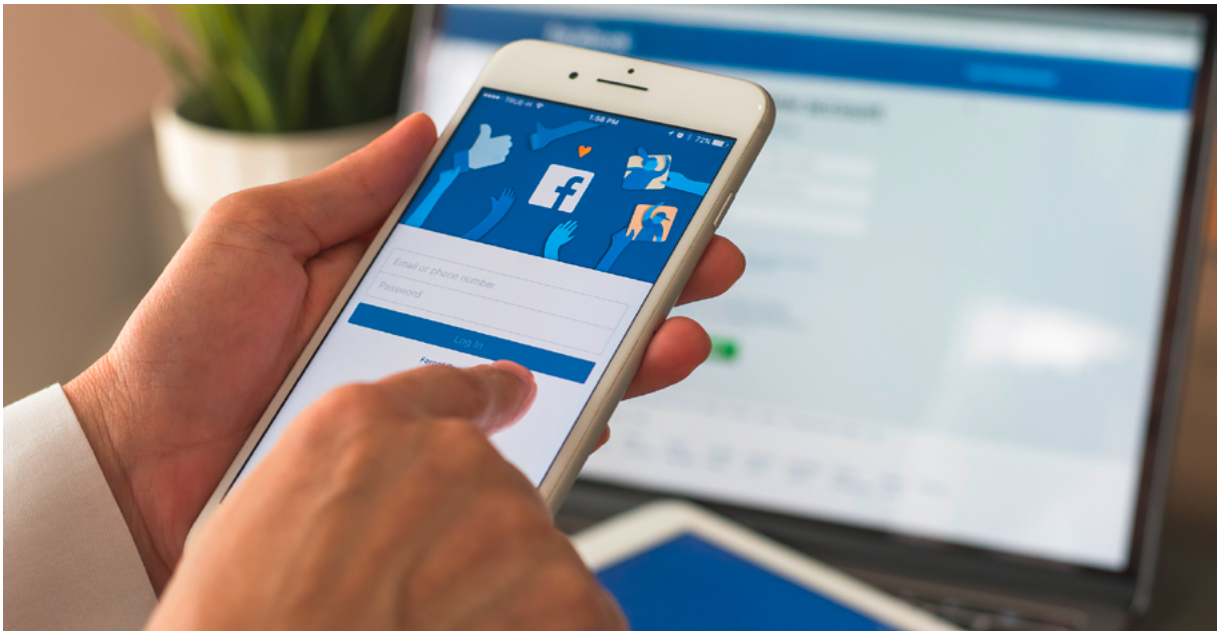
COORDINATED BY
Eindhoven University of Technology in the Netherlands

FUNDED UNDER
H2020-LEIT-ICT

PROJECT WEBSITE
pqcrypto.eu.org

A bottom-up approach to privacy protection

Recent events have shed some light on the gulf that can sometimes separate privacy-wary internet users from ICT businesses wanting to use the full potential of big data. The PRIVACY FLAG project aims to make them see eye to eye.



© Chinnapong, Shutterstock

Recent cases like the Cambridge Analytica data scandal made us all aware of how important it is to protect our privacy when using the internet. Yet, doing it is a different story. No one really has the time to go through the privacy settings of each app they are using, and the large spectrum of existing third-party apps can be confusing to say the least.

The PRIVACY FLAG (Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments) consortium's objective was to stand out with a unique combination of crowdsourcing, ICT and legal expertise. Their solution enables citizens to monitor and control their privacy with a three-headed combination of a smartphone app, a web browser add-on and a public website containing general information – all connected to a shared database. At the same time, companies can use PRIVACY FLAG services to become privacy-friendly with dedicated solutions, namely voluntary compliance and certification.

PRIVACY FLAG built upon the outcomes of 18 other EU-funded projects to create a new paradigm of privacy protection combining 'endo-protection' – with locally deployed privacy enablers – and 'exo-protection' – with a distributed and crowdsourced monitoring framework putting implicit pressure on companies to improve their privacy compliance. It transformed existing concepts into developed, tested and validated technologies, and whilst the PRIVACY FLAG platform as a complete solution was considered as TRL 2 when it was kicked off, it enables components which had already been tested prior to the project (TRL 4 or 5).

What makes the project unique is its use of crowdsourcing: "The basic view of crowdsourcing is that virtually everyone has the

potential to contribute with valuable information," Dr Ioannis Chochliouros, coordinator of the project on behalf of the Hellenic Telecommunications Organisation, explains. "The PRIVACY FLAG project developed a crowdsourcing-based process and a set of tools and solutions enabling the users to collectively assess and control the level of risk for their privacy in the different contexts of web applications, smartphone applications and Internet of Things deployments."

The PRIVACY FLAG platform is based on the Universal Privacy Risk Area Assessment Methodology (UPRAAM), which comprises the GDPR, Swiss and US data protection legislation respectively. By combining this methodology with distributed privacy monitoring agents and crowdsourcing, the platform enables a large-scale risk assessment process that could not be obtained with a regular 'top-down' approach. Moreover, as Dr Chochliouros says, "by mutualising the skills and capacities of the crowd, it reverses and rebalances the asymmetric relationship between individual users and large, powerful companies with a clear incentive to comply with privacy protection."

The 'crowd' here is organised around a community of privacy defenders. Through 'finger pointing' and avoiding websites and applications that are not privacy compliant, PRIVACY FLAG empowers citizens and enables them to select applications based on privacy criteria.

Business incentives

Enterprises can easily get support to become 'fully privacy respectful' and 'data ownership respectful', with a corresponding rating on the PRIVACY FLAG platform. SMEs and other interested companies can obtain an in-depth privacy risk analysis of their solutions with a report and recommendations for optimising their practices, which may constitute a competitive advantage for the entire European industry.

SMEs and other interested companies can obtain an in-depth privacy risk analysis of their solutions with a report and recommendations for optimising their practices.

"The data collected on European citizens is largely used by non-European companies to support marketing and get benefits vis-à-vis the competition. This creates an effective bias in the competition, advantaging companies with such data mining capacities which are mainly based outside of Europe," Dr Chochliouros explains. "By providing incentives for companies to offer privacy-friendly services/websites/products, the PRIVACY FLAG project also contributes to mitigating this unfair economic bias."

By the end of the project, PRIVACY FLAG solutions had been deployed and tested in an operational environment (TRL 7) and had reached a TRL of 9 with a large-scale exploitation. The consortium plans to generate most revenues from services and consulting, with potential complementary incomes from selective advertisements.

"If we manage to convince respectively 1 % of websites and 5 % of applications with a commercial interest or capacity to pay for professional services, we can expect to end up with about 200 000 websites and 4000 applications paying for your services," Dr Chochliouros says. In parallel, the consortium plans to approach 100 leading European smart cities and grant them a specific privacy risk analysis.

PROJECT
PRIVACY FLAG – Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

COORDINATED BY
Hellenic Telecommunications Organisation in Greece

FUNDED UNDER
H2020-SECURITY

PROJECT WEBSITE
privacyflag.eu

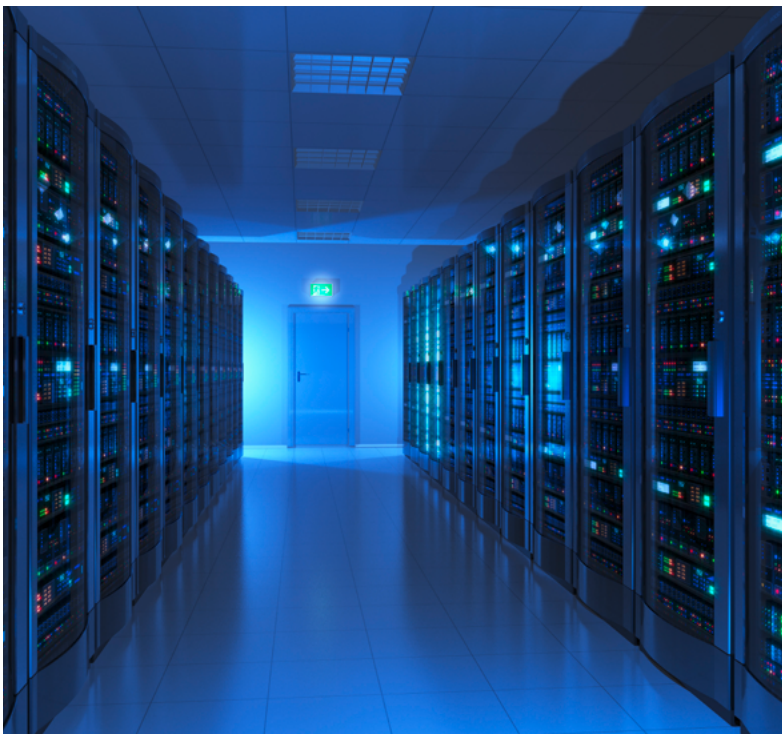
Pioneering a holistic approach to cyber security

An EU-funded project has delivered a toolbox and downloadable methods designed to help corporations and organisations approach cyber security in a more holistic manner. Positive results have also contributed towards the formulation of new industry standards.

Large corporations, public services such as hospitals and utilities such as energy suppliers rely on increasingly complex network systems in order to run efficiently and seamlessly. Such reliance however makes them susceptible to cyber hacking, which can cost companies millions in down time and damage to reputation, and in the case of compromised public services, can even put lives at risk.

So we aimed to find ways to better support companies and organisations eager to undertake comprehensive risk analysis of large-scale and networked systems.

"The fact that nine out of ten software security failures are caused by software defects represents a key vulnerability that hackers can exploit," explains Juergen Grossmann from Fraunhofer in Germany, who was in charge of standardisation issues in the RASEN (Compositional Risk Assessment and Security Testing of Networked Systems) project. "Protecting large networked systems, like the ones run by major companies, means understanding all the potential underlying security risks. A key problem however is that system complexity can make assessments and testing extremely challenging."



© Oleksiy Mark, Shutterstock

Holistic approaches to cyber security

The RASEN project has sought to address this by treating security risk assessments and security testing more holistically. Until now, both have been treated as distinct areas.

"While industry is demanding more integrated approaches in order to cope with security, no standard currently exists that sufficiently emphasises the need to systematically integrate security risk assessments and security testing," says Grossmann. "So we aimed to find ways to better support companies and organisations eager to undertake comprehensive risk analysis of large-scale and networked systems."

The RASEN project began by conducting a systematic composition of security assessment results. This allows individual parts of an ICT system to be analysed separately before a global assessment is made from the individual results.

Secondly, the team combined high-level security risk assessments with low-level security testing. "With this approach, risk assessments can be used to derive security test cases, and security test results can be used to verify or update the risk assessments," explains Grossmann. "Furthermore, these methods cover security risk assessments from different perspectives. Legal risk assessments for example address security threats in a legal context, while security risk assessments deal with threat probability and estimated consequences."

Results for the real world

The results of the RASEN project have now been translated into a toolbox to help companies and organisations combine security risk assessments and testing. The idea is to make the project's methodology as operational and practical as possible.

The RASEN method, along with some of the tools, are now downloadable from the project website, while the project's RACOMAT tool allows users to combine component-based security risk assessment with security testing. Testing can be integrated seamlessly into the incident simulations the tool uses for its compositional risk analysis.

"Our methods are repeatable, which means that continuous assessment through rapid reassessment will help to maintain the validity of results even as the target system or its environment changes and evolves," says Grossmann. "For example, our RACOMAT tool accesses libraries containing risk analysis artefacts like attack patterns and security test patterns, offering a high level of reusability. Much of the process can be done automatically."

The RASEN project has also laid the ground for several new research projects – Fraunhofer is involved in the PREVENT project for example – and contributed towards the formulation of new industry standards. "Several standardisation documents (e.g. ETSI EG 203251 and ETSI TR 101 583) have been adopted by the European Telecommunications Standards Institute and forwarded to international standardisation bodies," says Grossmann. "These documents reflect the project's results in the area of security risk assessment."

PROJECT
RASEN – Compositional Risk Assessment and Security Testing of Networked Systems

COORDINATED BY
Sintef in Norway

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
rasenproject.eu

Laying the secure foundation from which Europe can build the internet of tomorrow

EU-funded researchers are developing a security-testing tool to provide all Europeans with increased confidence in the Internet of Services.

By introducing a whole new level of internet-based supply and demand services, the Internet of Services (IoS) – the integration of connected items to provide a common service – is set to revolutionise how we go about our day-to-day lives. However, as society becomes increasingly dependent on the internet for all aspects of our lives, the need to ensure that this online infrastructure is secure and safe becomes of paramount importance.

© Ozz Design, Shutterstock

With a focus on internet infrastructures, the EU-funded SPaCIoS (Secure Provision and Consumption in the Internet of Services) project created sets of tools and techniques needed to provide IoS with a secure foundation to build from. For example, one set allows users to test specific security properties such as confidentiality and authentication. Another set allows the user to conduct vulnerability-driven testing, where tests are derived from the vulnerabilities most likely to invalidate security goals. A third set of techniques provides the user with an inference/extraction model derived from attack behaviour or the implemented code.

The SPaCIoS tool was designed as a proof-of-concept for a set of security testing problem cases drawn from the 'real world' scenarios seen by our project partners.

These techniques, along with an automated support system, have now been integrated into the SPaCIoS tool. By providing a formal description of the system under validation (SUV), security goals and model of the attacker, the tool automatically generates and executes a sequence of test cases on the SUV via a number of proxies. "The SPaCIoS tool was designed as a proof-of-concept for a set of security testing problem cases drawn from the 'real world' scenarios seen by our project partners, which paved the way for incorporating these results into such common industrial practices as SAP and Siemens business units", says project coordinator Luca Viganò. "We've taken the lessons we learned along the way and created a list of best practices that serve as a stepping stone for similar integrations in other industrial environments."

A public service

According to Viganò, although the SPaCIoS tool is primarily being used by industry, research institutions and standardisation bodies working on the development of a secure IoS, and ultimately all Europeans benefit. "At the end of the day, the SPaCIoS tool provides all Europeans with increased acceptance of – and confidence in – the IoS," he says. "This is especially important in the rapidly developing areas of e-health, e-government and e-marketing."

Because of this public benefit, the project has taken specific actions to engage the public. "We have incorporated SPaCIoS' results into numerous educational activities happening across the industry, at universities and in working groups and standardisation organisations," says Viganò. "Since the close of the project, we have organised a number of specific presentations, meetings and workshops, published nearly 100 papers on the project's work – including an impressive 10 PhD theses – and filed four patent applications." These actions specifically targeted service designers, developers and integrators.

Strengthening Europe's position in IoS

Europe is particularly well positioned to shape and drive the internet of tomorrow. Successful IoS initiatives will give Europe a competitive edge and create enormous opportunities for the economy, government and society.

"With its rich set of methodologies and technologies, the SPaCIoS project provided a comprehensive framework for the provision and consumption of validated secure services, thus serving as a major enabling technology for satisfying the security challenges raised by new communications and ICT paradigms," concludes Viganò. "We are confident these results will continue to help strengthen Europe's position at the vanguard of establishing the fundamentals of an emerging IoS vision and infrastructures where trustworthiness is considered a major differentiator and fundamental enabler."

PROJECT
SPaCIoS – Secure Provision and Consumption in the Internet of Services

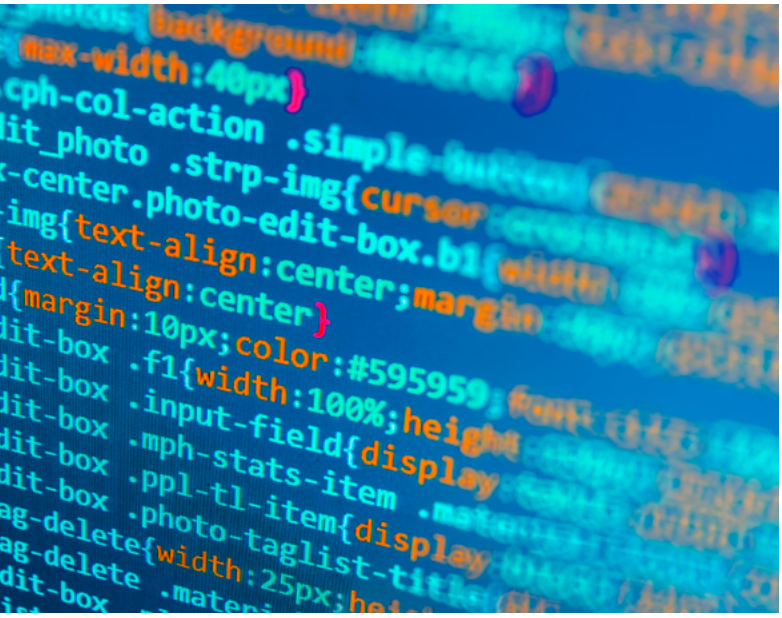
COORDINATED BY
University of Verona in Italy

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
spacios.eu

New security toolbox for software increases trustworthiness of existing processes

EU researchers have developed a set of source code analysis tools capable of verifying the security properties of applications written in C, C++ and Java.



In a society driven by information technology and communication, the safety and security of software have become crucial challenges. Answering this call is the EU-funded STANCE (A Source code analysis Toolbox for software security AssuraNCE) project, a multi-disciplinary initiative that has led to numerous scientific and technological breakthroughs in the field of software security.

Within its three and a half year timeframe, the project defined, implemented and distributed a toolbox – a set of source code analysis tools – capable of verifying the security properties of applications written in C, C++ and Java. Essentially, the toolbox brings together and coordinates the work of existing analysis tools, including the Frama-C platform, the VeriFast verifier and a 'fuzz' software testing tool. Frama-C is a software analysis platform that enables the design, implementation and dissemination of formal verification solutions. VeriFast, on the other hand, is an analyser for C and Java source code annotated with predicates written in separation logic.

"The STANCE architecture is based on the aforementioned analysis tools," says project researcher Armand Puccetti. "The project developed numerous plug-ins for these tools, allowing them to perform specific security analyses, such as modular code analyses." According to Puccetti, these are powerful tools for formally verifying the robustness of security sensitive applications. "The STANCE project further optimised their usefulness by creating methodologies for combining these tools for use in real-world case studies and within the context of Common Criteria Certification," he adds.

How it works

The STANCE tool specifies algorithms for detecting well-defined classes of security threats found in the source code. It accomplishes this by using, extending and expanding on known techniques for safety-oriented source code analysis – including abstract interpretations, deductive verifications and model checking. These analyses are then extended via diagnostic capabilities and model-based diagnosis and counterexamples. The analyses can also be conducted using dynamic analysis with fault injection and automatic test case generation. Following the completion of this initial phase, the tool provides the user with a theoretical foundation that formally guarantees that a given piece of software is free of any security flaws.

Increasing trustworthiness

With this toolbox and its supporting methods, the STANCE project successfully increased the trustworthiness and cost-effectiveness of existing security-oriented processes. "As a result of its work, the project positively altered the domain of software security assurance, having a broad impact on its legal, societal and economic aspects," says Puccetti. "Furthermore, among the new tools developed in the Frama-C and VeriFast platforms, several will be distributed in open source, while others remain as prototypes as further research continues."

As a result of its work, the project positively altered the domain of software security assurance, having a broad impact on its legal, societal and economic aspects.

From an economic standpoint, the STANCE project's findings will provide a strategic market differentiator for companies using its tool and methods, with long-term benefits as to development and maintenance costs. In a broader sense, the project has given society a new standard of trust – a much needed boost for the development of cyber-technologies.

"The STANCE project contributed to the fulfilment of the EU's policy strategies by providing a means for detecting security vulnerabilities in critical software applications, meaning EU citizens can have confidence that their software-driven applications are secure," concludes Puccetti.

PROJECT
STANCE – A Source code analysis Toolbox for software security AssuraNCE

COORDINATED BY
Alternative Energies and Atomic Energy Commission

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
stance-project.eu

Keeping unwanted trespassers out of your information

EU-funded researchers have developed a working toolset and methodology that support a navigation approach to preventing unwanted system trespassers.

The complexity of today's interconnected technical systems, along with the speed that these systems are evolving at, have far surpassed our capacity to even imagine – let alone evaluate – potential risk scenarios. As a result, we have entered uncharted waters when it comes to protecting ourselves.

To overcome this challenge, new technology-supported methods are needed to identify and manage these always-changing risks – a challenge that the EU-funded TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) project is addressing with its Attack Navigator solution.

Start with a map

"Of course it takes more than just a good metaphor to build a usable risk assessment system, but what the TREsPASS project provides is a working toolset and methodology that support a navigation approach to preventing unwanted system trespassers," says project researcher and Assistant

Professor at the Technical University of Denmark Christian W. Probst.

To achieve this 'navigation effect', the project turns to the most basic of all navigational tools: the map. Whereas in the real world maps represent cities, streets and points of interest, the maps used by the TREsPASS project are essentially system models – a formal representation of the socio-technical environment intended to be analysed. These system models are based on a number of components, including: actors (human players or processes), assets (items or data), locations (where actors or items may be situated), edges (possible relocation paths between locations), policies (access control), and processes (computer programmes, virtual machines, etc.).

"Unlike in the real world, there are no satellites to provide pictures of a system environment," says Probst. "Instead, the model is the result of a collection of processes that resemble the combination of satellite and geographer."

Creating attacker profiles

Once a system model is built, it's time for the Attack Navigator to get to work. The TREsPASS Attack Navigator is a graph-based approach to security risk assessment inspired by navigation systems. "Based on maps of a socio-technical system, the Attack Navigator identifies possible routes that an attacker might take towards reaching their objective," explains Probst. "By creating attacker profiles, attacker-specific properties, such as skill-level and available resources, can be included within the map, enabling those working to defend a system to explore possible attack scenarios and the effectiveness of defence alternatives."

Based on maps of a sociotechnical system, the Attack Navigator identifies possible routes that an attacker might take towards reaching their objective.

Probst notes that this attacker-focused approach represents a fundamental shift from the more usual defender-based approach of other risk assessment methods. Furthermore, just like navigation systems come in different shapes and sizes for different needs, the TREsPASS project also developed tools that work on different kinds of maps, for example where actors with money and service flows are represented to identify possible fraud.

Predicting and proactively defending

The most important property that influences a possible attack are the properties of the attacker. Similar to a vehicle navigation system, in many current security risk models these attacker properties are implicit. However, the TREsPASS project's Attack Navigator concept takes this one very important step further by leveraging threat agents as attacker profiles. The tool thus uses a combination of a navigator map and an attacker profile to predict an attacker's likely goals based on the attacker's motivation, feasible routes to that goal, and properties of these routes based on the skill and resources from the attacker profile.

© photodonato, Shutterstock

The attacker profile implies a link between attack navigators and security economics, meaning the actions of both attackers and defenders come with costs and benefits that must be managed within a limited budget. Thus, the Attack Navigator assumes that 1) attackers will seek to optimise their investments, 2) the defender will move before the attacker, and 3) as a result, the attacker will already know what the defender has done. With this information, one can then predict the likely actions of an attacker and therefore proactively develop defence mechanisms.

"The claim of the Attack Navigator is not a precise prediction of what will happen, but rather a prediction of what is possible or likely, and to what extent countermeasures improve the situation," adds Probst. "Although the exact numbers one would like to have are usually impossible to obtain, our analysis is useful in comparing options, or even in directing our thinking about possible attackers."

PROJECT
TREsPASS – Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

COORDINATED BY
University of Twente in the Netherlands

FUNDED UNDER
FP7-ICT

PROJECT WEBSITE
trespass-project.eu

Novel tools to make the web advertising industry more transparent

Market leaders Google and Facebook drive three quarters of internet advertising's growth. This online advertising explosion is raising serious data privacy and security concerns.

Advertisers track users when they're online by shadowing them as they browse websites, perform web searches or watch movies. Tracking companies build a profile of each user based on such activities.

Collecting and processing personal data and then offering it to interested parties often means maintaining a balance between sustaining the many gains the industry brings and concerns over the privacy of internet users. The TYPES (Towards transparencY and Privacy in the onlinE advertising businesS) project "protects individuals' privacy while empowering them to control how their data is used by service providers for advertising purposes," says Rosa Araujo, project coordinator for the EU-funded initiative. "By raising end user trust and advertiser transparency, all stakeholders of the advertising ecosystem stand to benefit."

Keeping internet advertisers in check

TYPES created tools designed to support the idea of a healthier, more transparent and thriving online advertising sector. This suite of tools enables users to "better understand how their personal

© angellodeco, Shutterstock

data is used online, ultimately building a strong foundation on which both industry and they can thrive," continues Araujo.

The Web Browser Plug-In (available as corporate and open-source versions) and Network Proxy tools concern privacy violation detection and safeguarding. Araujo explains that they allow users to "know what information is being collected and tracked by websites and advertisers, among others."

Data valuation tools estimate the value that the online advertising market or users associate with different data which is mostly unknown and particularly difficult to assess. Software includes the Web Survey tool, Data Valuation Web Portal, YouTube Video Valuation tool and Facebook Data Valuation tool. "Divulging such information would be beneficial for both end users and the online advertising industry," notes Araujo.

TYPES also developed Data Broker, a privacy-by-design advertising and marketing solution. Araujo stresses that it "helps end users to share and benefit from their data in the digital advertising ecosystem."

Products to boost business and protect privacy and personal data

Some solutions are ready to hit the market, while others are well on their way. The corporate Web Browser Plug-In is being commercialised for SMEs. One of the project partners, a digital agency, will offer the open-source version to its customers.

The subsidiary of a global security services company is expected to introduce the Network Proxy tool to its client base. "This is a huge success for the project and the potential it can offer, because the company has a portfolio of several dozen companies that purchase solutions for improving their users' web experience," emphasises Araujo.

The Web Survey tool is freely available on the project website. Several partners intend to offer the Web Portal as a public service, aimed at maintaining transparency and creating awareness among citizens of personal data's value.

TYPES protects individuals' privacy while empowering them to control how their data is used by service providers for advertising purposes.

There are plans to apply for public research funds to maintain the Facebook Data Valuation tool, which informs Facebook users in real time about the money they're generating for the social networking website. It's the only product of its kind in the marketplace. A patent has also been issued for the Data Broker algorithms.

"Key market players and national organisations from the advertisement sector have expressed concern about the impact the project will have on established business models," concludes Araujo. "Despite this, there's a certain underlying realisation that something needs to be done regarding transparency, and that the EU's new legislative framework for data privacy that comes into force in 2018 will make tools not only relevant, but needed."

PROJECT
TYPES – Towards transparencY and Privacy in the onlinE advertising businesS

COORDINATED BY
Eurecat in Spain

FUNDED UNDER
H2020-SECURITY

PROJECT WEBSITE
types-project.eu

Visionary solution for online data privacy

The EU-funded VisiOn project has developed a visual privacy platform to help public entities deliver transparent and privacy-enhanced e-government services that meet the highest privacy standards and offer citizens personalised control over their data.

The solution, which was successfully trialled through a series of pilot tests (in Spanish and Italian hospitals for example), empowers citizens to gain control of their digital privacy through the creation and monitoring of a personal Privacy Level Agreement (PLA). This provides a clear visualisation of privacy preferences about data that can be managed by public institutions.

"Results obtained from these pilots confirmed that the platform improves citizen awareness of privacy and data protection issues and increases their level of control on data management," says VisiOn (Visual Privacy Management in User Centric Open Environments) project coordinator Loredana Mancini from Business-e in Italy. The vision Privacy Platform (VPP) was also shown to be an effective tool for strengthening the transparency and accountability of public administration operations, ensuring that they are in full compliance with online data privacy laws.

"We have already received requests from other organisations to start pilots based on the VisiOn solution," says Mancini. "While the platform was developed and tested for public authorities, the model can be easily enlarged to cover any type of organisation that shares and uses personal data."

© ranjith Ravindran, Shutterstock

Smarter government

Online technology has developed at such an impressive speed that it is sometimes hard to appreciate just how much our lives have been transformed. Expectations have also evolved; citizens now expect instantaneous internet connections wherever they go, and to be able to use their mobile devices to perform all sorts of functions such as banking, reserving flights and hotels and getting real time traffic information.

"We increasingly expect the same level of ease in accessing services from public institutions such as local government and healthcare," notes Mancini. "We also expect these services to be secure and that our data are protected."

What is needed is an open data model that enables citizens to securely access their information as well as public services in a seamless way, wherever they are.

Delivering smart government services in a secure manner presents a challenge for the public sector. "Achieving this means being able to integrate and share information between different public authorities, and sometimes private organisation as well," says Mancini. "What is needed is an open data model that enables citizens to securely access their information as well as public services in a seamless way, wherever they are."

Ready for regulation

To make this possible, the VisiOn project focused on the issue of privacy. This is a key challenge for public administrations, which often lack the tools and expertise to carry out privacy analyses and integrate them naturally in their digital services. The General Data Protection Regulation (GDPR), which came into force in May

2018, introduced new stricter privacy-related policies for any organisation holding information of EU citizens.

The GDPR aims to give control over their personal data back to citizens. "The VisiOn platform provides support towards GDPR compliance through the creation of tailored Privacy Level Agreements, which take into account citizens' privacy needs and provides them with control over their data, and by providing organisations with methods and tools to achieve a privacy-by-design approach on their digital services," explains Prof. Haris Mouratidis from the University of Brighton, UK, who led the development of the PLA and the privacy-by-design methods in the VisiOn project.

The VisiOn consortium believes that the project's platform taps into a growing public and private sector need to empower citizens when it comes to data privacy. "To this end the GDPR could be a strong market booster, and many technology providers are keen to promote themselves as GDPR-compatible," says Mancini. "Our platform could give them the upper edge. We are looking at market analysis reports at the moment, and don't see a similar solution on the market."

PROJECT
VisiOn – Visual Privacy Management in User Centric Open Environments

COORDINATED BY
Business-e SPA in Italy

FUNDED UNDER
H2020-SECURITY

PROJECT WEBSITE
visioneuproject.eu

WISER's free tools will help large and small entities combat cyber threats

Companies and governments are bombarded by billions of cyber threats every day. Countering these threats ties down resources and manpower, with only the largest organisations able to afford full protection. But what about the small players who can't afford the time and cost? This EU project will develop free and easy-to-install but sophisticated tools to help them fight back.

The vast majority of SMEs have to sacrifice limited resources to get the cyber-defences they need, or limp along with sub-standard risk tools and hope for the best. The WISER (Wide-Impact cyber SEcurity Risk framework) project aims to change that by developing easy-to-use and free risk-management tools which heavily ICT-reliant SMEs and larger critical infrastructure operators can exploit.

"SMEs often do not have the resources or skills to use advanced methodologies and tools to handle cyber risk, while most can't afford to hire consultancy services," said Niccolò Zazzeri of Pisa-based Trust-IT Srl, a member of the WISER research consortium. "We aim to offer a sophisticated solution that is easy to adopt by the end user."

© JuliRose, Shutterstock

Launched in June 2015 as a 30-month project, WISER will carry out a number of short 'early assessment pilots' to test their tools. These will lead to three full-scale pilots focused on fraud detection, energy distribution and use, and energy procurement. The full-scale pilots will validate in real-time WISER's methodology and modelling tools based on realistic scenarios.

One of the free online tools the consortium has already developed and tested is Cyber-WISER Light, which consists of two parts: a questionnaire and a vulnerability test. "When we talk to SMEs we tell them to do this self-assessment regularly because threats change in nature and over time and geography," said Zazzeri.

The tool collects information about a private network and produces a report based on general cyber-security best practices, and then rates the entity risk-exposure. The next step is to run a vulnerability test, which consists of installing a token in the entity's server. "The user must have his organisation's cyber authorisation to do that, of course, but the token is not an intrusive one – simply a copy/paste operation. It then produces a picture of the network's vulnerability by ranking its top 10 weaknesses," he observed.

The project's next tool – dubbed Cyber-WISER Plus and to be released in late 2016 or early 2017 – will look for threats and trojan horses.

The project's next tool – dubbed Cyber-WISER Plus and to be released in late 2016 or early 2017 – will look for threats and trojan horses. For larger operators, the research team will also develop a risk platform as a service (RPaaS) version of the platform. This will be for critical infrastructures and highly complex cyber systems that need monitoring of the special controls within their ICT system in order to prevent tampering of the controls. Verification procedures will be based on encrypted public key infrastructure (PKI) functionality and components. These will check whether the signature in network messaging corresponds to the organisation's certificate contained in each message.

According to Zazzeri, his project's approach to addressing and mitigating cyber-security threats and in critical information infrastructure "will also empower decision makers in public and private organisations to more effectively assess cyber-risks."

PROJECT
WISER – Wide-Impact cyber SEcurity Risk framework

COORDINATED BY
Atos in Spain

FUNDED UNDER
H2020-SECURITY

PROJECT WEBSITE
cyberwiser.eu

A security and privacy framework for outsourced data

Is the cloud safe? This question has been feeding conversations among internet users ever since the first cloud services became accessible, and it is still far from being answered. The WITDOM project aimed to help close the debate by developing a new security and privacy framework for outsourced data in untrusted ICT environments.

Over the past decade, sensitive data has been shifting from 'trusted' domains – local computers hosting security-critical services – to cloud providers where virtually unlimited resources are available for heavy computational tasks. The problem is that clients only have limited control over these resources, unlike the cloud service provider, which makes these environments qualify as 'untrusted' domains.

This is where WITDOM (empoWering prIvacy and securiTy in non-trusteD envirOnMents) comes into play. Its platform, developed by a seven-strong consortium led by Atos Spain, orchestrates a variety of complex processes to protect sensitive data in the trusted domain, so as to enable secure and privacy-preserving processing, storage and sharing in an untrusted domain.

"WITDOM's main goal was to produce a framework for end-to-end protection of data in untrusted and fast evolving ICT-based environments. We put particular focus on data-outsourcing scenarios, where new threats, vulnerabilities and risks due to new uses require end-to-end security solutions that will withstand progress for the lifetime of the applications they support," explains Elsa Prieto, coordinator of the project.

To do that, the consortium investigated various data protection techniques such as homomorphic encryption, a method that allows computation on encrypted data and generates a result which, once decrypted, matches the result of the operation just as it had been performed without encryption. Other investigated techniques included anonymisation, secure signal processing (SSP), data masking, verification and integrity, and end-to-end encryption.

Our framework was instantiated and validated in two application scenarios: a health scenario based on genetic data sharing for large research data analyses and individual outsourced clinical analyses; and a financial services scenario based on the management of both customers' data and finance data of contracts.

The WITDOM framework uses the paradigm of service orientation to isolate applications from the specific implementation and location of its elements. It organises multiple protection components together in a comprehensive framework, and its architecture was adapted to hybrid cloud models. Its core components include a broker, a protection orchestrator, an identity and access management (IAM) component, and a key management (KM) service. Additional services can also be added as modular blocks.

"Our framework was instantiated and validated in two application scenarios: a health scenario based on genetic data sharing for large research data analyses and individual outsourced clinical analyses; and a financial services scenario based on the management of both customers' data and finance data of contracts as well as providing outsourced secure financial services over private and public cloud instances," says Prieto.

Additional functionalities were developed specifically for these scenarios. These include: a Genomic Laboratory Information

Management System (GLIMS) which supports DNA analysis activities that require a large computational effort and storage capability; services implementing the interface between end-used in-house financial applications and WITDOM components; statistical and machine learning services to satisfy the needs of the financial scenario; and genomic services including sequence alignment, variant annotation and variant reannotation.

Since the project was completed at the end of 2017, partners have been including its results in their portfolio of solutions for customers. Some patent applications were started, including a patent application by IBM on the data masking technology, two patent applications by UVIGO associated with the SSP component, one related to the genomic scenario, and another one related to the financial services scenario. "Some components, especially those that provide data protection functionalities, still need some maturation before going to market," Prieto points out.

PROJECT
WITDOM – empoWering prIvacy and securiTy in non-trusteD envirOnMents

COORDINATED BY
Atos in Spain

FUNDED UNDER
H2020-LEIT-ICT

PROJECT WEBSITE
witdom.eu

© Rawpixel.com, Shutterstock

CORDIS Results Pack

Available online in 6 language versions: cordis.europa.eu/article/id/400141

Published
on behalf of the European Commission by CORDIS at the
Publications Office of the European Union
2, rue Mercier
2985 Luxembourg
LUXEMBOURG

cordis@publications.europa.eu

Editorial coordination
Zsófia TÓTH, Silvia FEKETOVÁ

Disclaimer
Online project information and links published in the current issue of the CORDIS Results Pack are correct when the publication goes to press. The Publications Office cannot be held responsible for information which is out of date or websites that are no longer live. Neither the Publications Office nor any person acting on its behalf is responsible for the use that may be made of the information contained in this publication or for any errors that may remain in the texts, despite the care taken in preparing them.

The technologies presented in this publication may be covered by intellectual property rights.

This Results Pack is a collaboration between CORDIS and the Directorate-General for Communications Networks, Content and Technology (DG CONNECT)

PRINT	ISBN 978-92-78-41763-5	ISSN 2599-8285	doi:10.2830/583040	ZZ-AK-18-003-EN-C
PDF	ISBN 978-92-78-41707-9	ISSN 2599-8293	doi:10.2830/387267	ZZ-AK-18-003-EN-N

Luxembourg: Publications Office of the European Union, 2018

RESEARCH*EU MAGAZINE ISSUE 74: The future's bright, the future's Big Data

Did you catch the July issue of Research*eu? Get a sense of Big Data's future in the special feature's coverage of the results of 11 EU projects. Will Big Data become more accessible and change society for the better?

Research*eu is free of charge.
Browse, download or subscribe at
cordis.europa.eu/research-eu

Publications Office
- **eur-lex.europa.eu** • EU law
- **publications.europa.eu** • EU publications
- **ted.europa.eu** • Public procurement
- **cordis.europa.eu** • Research and development

Follow us on social media too!
facebook.com/EULawandPublications
twitter.com/CORDIS_EU
youtube.com/CORDISdotEU

EN