Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
ICT 32-2014

Secure Hardware-Software Architectures for
Robust Computing Systems [†]

Deliverable D6.3: Exploitation report, year 2

Abstract: The purpose of this *live* document is to provide an exploitation plan of the SHARCS project through the course of its duration. The industrial beneficiaries report on their exploitation intentions in the form of a business plan. The research institutions report their use plans in a quantified manner, i.e. new teaching and research activities inspired from SHARCS, intentions to create a spin-off company or other commercial activities, as applicable. Potential collaborations and outreach programs are included as well.

Contractual Date of Delivery	Month 24
Actual Date of Delivery	Month 25
Deliverable Dissemination Level	Private
Editor	Christos Strydis
Contributors	All SHARCS partners
Quality Assurance	Dmitry Pidan, John Thomson

[†] The research leading to these results has received funding from the European Union Horizon 2020 Program (2014-2020) under grant agreement n° 644571.

The SHARCS Consortium

Foundation for Research and Technology – Hellas	Coordinator	Greece
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Chalmers Tekniska Högskola	Principal Contractor	Sweden
Technische Universität Braunschweig	Principal Contractor	Germany
Neurasmus BV	Principal Contractor	The Netherlands
OnApp Limited	Principal Contractor	United Kingdom
IBM - Science and Technology LTD	Principal Contractor	Israel
Elektrobit Automotive GMBH	Principal Contractor	Germany

Document Revisions & Quality Assurance

Internal Reviewers

1. Dmitry Pidan
2. John Thomson

Revisions

Ver.	Date	By	Overview
0.1.0	23/11/2016	C. Strydis (NEU)	New version compiled
0.2.0	29/11/2016	C. Strydis (NEU)	General text added
0.3.0	02/11/2016	C. Strydis (NEU)	General text added
0.4.0	07/11/2016	C. Strydis (NEU)	NEU exploit. plan updated
0.5.0	09/11/2016	C. Strydis (NEU)	Text modifications
0.6.0	14/12/2016	J. Thomson (ONAPP), T. Kamm (EBA)	ONAPP and EBA exploit. plans updated
0.7.0	15/12/2016	D. Pidan (IBM)	IBM exploit. plan updated
0.8.0	17/12/2016	G. Christou (FORTH), I. Sourdis (CTH)	FORTH and CTH use plans updated
0.9.1	19/12/2016	C. Giuffrida (VUA)	VUA use plan updated
0.9.2	21/12/2016	M. Tsantekidis (TUBS)	TUBS use plan updated
1.0.0	27/12/2016	C. Strydis (NEU)	Consolidated partner inputs; 1st complete draft
1.1.0	29/12/2016	C. Strydis (NEU)	Text updates based on 1st internal review
1.2.0	14/01/2017	C. Strydis (NEU)	Text updates based on 2nd internal review
1.3.0	20/01/2017	C. Strydis (NEU)	Final document version released

Contents

1 Introduction

1.1 Scope

This Deliverable D6.3 reports on the exploitation activities carried out in SHARCS. This document is part of a series of deliverables that provide annual updates.

In the SHARCS context of creating secure-by-design systems that achieve end-to-end (E2E) security, the goal of the exploitation effort for the consortium industrial partners (IBM, ONAPP, EBA, NEU) is to identify potential markets and opportunities in their respective fields and, then, proceed to plan out suitable exploitation strategies. For the academic partners (FORTH, VUA, CTH, TUBS), the objective is to highlight the SHARCS-generated innovations that will lead to the creation of new educational material, to new research directions and, if possible, to the valorization of research ideas for commercial exploitation, as well.

1.2 Document structure

The presentation of exploitation is organized around two pillars, *industry* and *academia*. The work carried out as part of the SHARCS project will give the opportunity for the industrial partners of the project to acquire knowledge and the possibility to exploit results. Industrial exploitation involves the following important activities:

- Identification of new possible application scenarios for SHARCS technologies;
- Introduction of new commercial activities and products; and hopefully
- Consolidation of partner competencies.

On the academic front, SHARCS findings will permit the universities and research organizations involved in the project to stay on the forefront of scientific research in their respective fields (refer also to the updated Dissemination deliverable D6.4). For academia, exploitation involves the following activities:

- Advancement of scientific knowledge on SHARCS-related research fronts;
- Knowledge transfer across other trans-disciplinary fields of research;
- Enrichment of academic education in the form of upgraded syllabi and new courses; and
- Promotion of partner specialities and increased community awareness.
- Technological innovation leading to new commercial activities, spin-offs etc. in Europe.

SHARCS is an interdisciplinary project that brings together experts from a wide range of technological and research fields with the goal of delivering E2E techniques in digital systems. The three SHARCS use-cases considered (implant, automotive, cloud) are represented by three companies (NEU, EBA, ONAPP) active in different market sectors and are sufficiently diverse to make a uniform treatment of exploitation activities possible. The second project year has been mostly occupied by collecting various software and hardware techniques while the pilot partners spent most of their efforts in specifying and implementing the proposed SHARCS techniques. In effect, the first successful steps towards full-system integration and working demos have been made (see also deliverables D5.1, D5.2 and D5.3). Therefore, exploitation strategies are reported in this document once more in separate sections. Any opportunities for joint exploitation on the part of the companies will be reported in the final year.

2 Exploitation strategy of industrial partners

In this chapter we detail the outlook of exploitable results and future strategies per industrial partner.

2.1 Neurasmus BV

NEURASMUS B.V. is a not-for-profit research and development company that operates under the holding of Erasmus Medical Center (EMC), Rotterdam. The company was founded in April 2010 by members of the Department of Neuroscience. The mission of the company is to valorize intellectual property created within the Department of Neuroscience as well as to develop new high-tech systems that can be used either as cutting-edge research tools or in the treatment of neuroscience-related diseases. In 2010, Neurasmus launched the first commercially available projects, ranging from completely automated tools for mouse behavioral phenotyping (Erasmus-ladder) to a high-tech mobile lab unit for patient visits during clinical trials (NeurasBus). Since Neurasmus has access to all scientific data and intellectual property that exists within the Department of Neuroscience, and contracts software and hardware experts, it is well equipped for rapid development from idea to prototype of complex systems.

Neurasmus acts as a use-case provider for the SHARCS project. By partaking in the project, Neurasmus intends to develop a prototype implant SoC encompassing various hardware and software security techniques for achieving end-to-end security in IMDs.

2.1.1 Product description & added value

Implantable Medical Devices (IMDs) have been around since the late 1950s with the invention of the first implantable pacemaker [3]. IMDs have come a long way since then, nowadays comprising a wide range of implantable

systems for various pathoses. Over the last decade [18], they have been equipped with wireless-communication capabilities, effectively becoming *active* devices capable of interacting with the outside world; namely, servicing commands and transmitting back requested data, such as patient data logs.

Wireless connectivity has led to a new generation of IMDs with great potential, albeit at the cost of becoming amenable to wireless security attacks. The public has identified the need for implant security [13] and research has already started accumulating knowledge to tackle the problem [40, 22]. However, due to the unique challenges of IMDs, a universal and fool-proof solution has not been proposed yet; IMD security and privacy remain open topics in the research community and, of course, in the market. Given the substantial interest in IMD security, Neurasmus has positioned itself in expanding its expertise in IMD security and privacy. It aims at providing off-the-beaten track, yet practical and generic solutions for E2E IMD security. Currently, Neurasmus anticipates the following two products.

2.1.1.1 Product 1: Secure IMD SoC and Communication Protocols

Neurasmus has been researching various aspects of IMD design for a number of years. We have, so far, proposed some pragmatic software- and hardware-based techniques for security and privacy. Along these lines, we are aiming at offering an IMD System-on-Chip (SoC) demonstrator platform featuring various techniques for security and privacy. Through SHARCS, Neurasmus aims at subjecting its IMD-SoC design to the expertise of the consortium experts, yielding an improved version of the system featuring E2E security, and hopefully, proposing a more generally applicable solution for IMDs at large. It is expected that this solution, which features novelties in both implant-system design and security protocols, will gradually draw commercial interest from major IMD companies. Besides, with the strong push toward sports/health wearables for the masses nowadays, there is also a chance that other, large-scale companies might find such novelties relevant and applicable to their trending health-&-fitness product lines (e.g. Nike, Apple). However, we have not studied these markets sufficiently to make any predictions or devise specific commercial strategies.

Our targeted implant SoC offer can also work as a "sandbox" for demonstrating or assessing the potential of current and future security solutions. We can use it to mix and match different security protocols, different modules dedicated to security (such as the SISC core), different ciphers etc. or to try simulating other SoC-environment conditions (e.g. EMI-rich environments such as a metal detector or an MRI scanner). This SoC is also the stepping stone to later co-opting other, ex-vivo system components such as the patient's smartphone acting as a local auxiliary processor or a hospital Cloud acting as a remote resource for more, in-depth, offline analytics and

Figure 2.1: The SJM PROCLAIM family of implantable stimulators.

treatments. In short, the SoC is the stepping stone for researching secure Cyber-Physical Systems (CPS) (in this case, medical CPS). Such devices are already closer than one might think: In late 2015, St. Jude Medical (SJM) has introduced a new family of Spinal-Cord-Stimulation (SCS) implantable pulse generators called PROCLAIM[1] (see Figure 2.1). Thus, it is the recently added (wireless) connectivity with the outside world, combined with the extended (remote) capabilities that are transforming traditional IMDs to next-generation, medical CPS.

2.1.1.2 Product 2: Evaluation of Proposed Security Solutions

This is not as much a designed product as an offered service. We have already performed and published research on the great potential of dynamic biometrics, when employed in implant security [37, 35, 38]. Dynamic-biometrics-based authentication has become a very popular theme in recent years, resulting in multiple proposals offered for tackling (parts of) implant security. We have, however, shown that such approaches can be successful only under strictly defined conditions [36], [34, Chapter 4]. Their potential is greatly affected by various aspects. For instance, the biometric-

[1] Online: https://www.sjmglobal.com/en-int/professionals/featured-products/neuromodulation/spinal-cord-stimulation/implantable-pulse-generators/proclaim-elite

sensor type and technology used directly affects security: Selecting a Photoplethysmography (PPG) rather than an Electro-Cardio-Gram (ECG) sensor (for dynamic-biometric measurement) makes the IMD susceptible to remote-measurement attacks e.g. through use of high-definition cameras. As another example, the health condition of the patient (healthy, sportive, arrhythmic etc.) directly affect the strength of generated security keys or – conversely – the key-generation time, making it intractable for practical use under certain conditions.

To be in a position to assess implant-security solutions reliably, we believe experts need to sit in the crux of engineering and medical science which is exactly the position of companies like Neurasmus. Building upon our significant implant-related expertise, we are currently expanding our security-related knowhow and will aim for offering consulting/evaluation services to interested 3^{rd} parties in the future.

2.1.2 Market analysis

IMDs are a segment of the medical-device market which has slowly but steadily increased over the last decades; see Figure 2.2 for the market trends in the USA which is the dominant market, currently. Nowadays, IMDs represent highly sophisticated devices with high market value. More specifically, by assuming average numbers reported by current market studies [29, 41] the average IMD cost is about $30,000 (€26,000). This leads to reported annual revenues worldwide set at $4.3 B (€3.7 B). The IMD market has roughly increased . Cardiac IMDs represent roughly half of all devices being implanted annually while the total number of implanted devices is 142.000 annually (1 per 700 in US/EU). According to a new market report published by Transparency Market Research [33], the U.S. implantable medical devices market was worth $43.1 B in 2011 and is expected to reach $73.9 B in 2018, growing at a CAGR of 8% from 2012 to 2018. This agrees with another report by the Freedonia Group reporting a rough increase of the IMD market by 8% per year since 2005 [16]. Similar numbers are reported by Ector and Vardas [12].

2.1.2.1 Market placement & competitor analysis

Market division 2005–2010: Three major companies St. Jude Medical, Boston Scientific and Medtronic are currently dominating the market. Medtronic (annual revenue: $17.00 B 2014; 49,000 employees) is the biggest manufacturer of cardiac devices. Likewise, St. Jude Medical (operational income: $5.50 B, 16,000 employees; $10.25 B in assets) dominates the neurostimulator market.

Since IMD security is still a heavily researched theme, no commercial device exists that provides E2E security. Of course, the three major IMD manu-

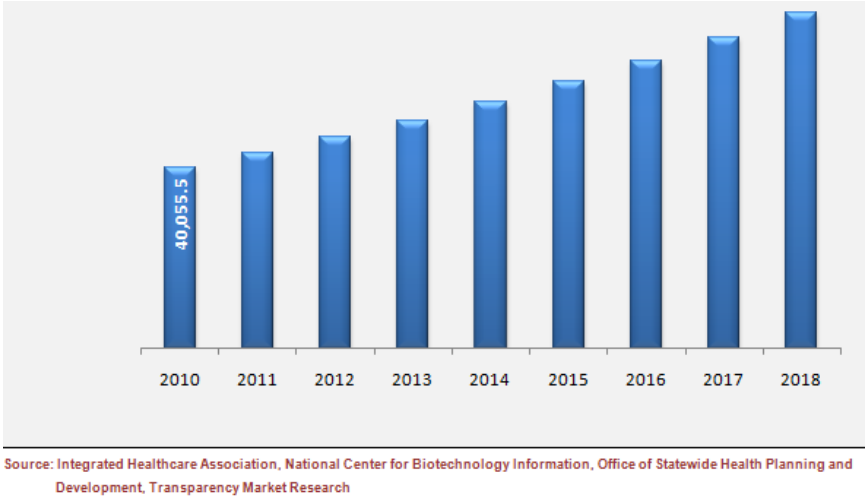

Figure 2.2: Market for IMDs between 2010–2018 in millions of USD.

facturers have taken steps in securing their devices and, in a similar manner, other companies are expected to appear specifically aiming at security solutions for IMDs. At the time of this writing, we are not aware of any serious competition in this market segment of medical devices, although there is a good chance that industrial competitors exist and are hard at work, given the secrecy characterizing this field. We will keep investigating this field in the following years.

Provided that implant companies are deeply interested – albeit secretive – in implant security, as it directly affects patient safety, the question of market analysis becomes, then, one of general implant-market size and trends.

2.1.3 Business model & future plans

The added value for Neurasmus from participating in SHARCS is to be found in improving its security expertise and in further advancing its existing implantable solutions for prototyping one new, cutting-edge system with novel security characteristics. As implantable devices become more wide-spread and accessible to an ever-aging population, the concepts of end-to-end security from hardware all the way up to the software and even across communication links, as envisioned by the SHARCS framework, are of high exploitation value for Neurasmus and its commercial objectives.

Neurasmus typically employs an IP-licensing business model, which exempts it from all production, advertising and distribution costs, and yields limited but low-maintenance revenues (due to ongoing licensing). The company is specialized in cutting-edge products which involve high novelty but sometimes come at the cost of high risk in commercialization potential. This

risk can be amortized by offering significant breakthroughs in science and novel, specialized, products. This, in turn, usually translates into a small-to-medium-sized market consisting of lab-to-lab sales and, on occasion, niche customers. It also translates to a significant number of high-impact publications resulting in renewed investments and new R&D cycles (such as SHARCS) in the company.

There is, currently, no immediate commercial-exploitation plan devised for implant security. Our growing experience in the field suggests that there are two ways to break into this market:

1. Come up with a *complete* solution that can then be licensed to 3^{rd} parties, or;

2. Directly collaborate with any of the major implant companies worldwide including joint IP development, consulting services, and so on.

Based on the trends witnessed so far in the field, marketing a product that can compete head-on with the competition is extremely risky and fail-prone, given the high costs involved in releasing a new implantable product and the aggressive strategies practised by the large enterprises. They typically engage in blocking patents, (in)direct financial asphyxiation or aggressive acquisition of any upcoming competitors. Neurasmus neither has the capacity nor the mission to engage in such "market wars". As a result, we are orienting mostly towards providing security-related IP (instead of complete solutions) that can, then, be licensed. Another possible venue is consulting or joint-exploitation strategies with large implant manufacturers.

To this end, in the second quarter of 2016, we have engaged in important but slowly progressing discussions with one of the three leading US manufacturers. Our past expertise, published work and valid security concerns with old and new devices released in the market have allowed us to make a strong case with the manufacturer. In effect, at the moment of this writing we are working towards a joint research/exploitation venture through signing a series of NDA and CDA documents. We expect that, towards the end of the SHARCS project, we will be in a position to define a more concrete business strategy.

2.1.3.1 Stakeholders

With respect to benefiting from SHARCS technologies, the primary stakeholders of the Neurasmus secure-IMD technology are the patients themselves that stand to benefit from more secure implants, as end users. Another set of stakeholders (as potential customers) are the three major IMD providers that stand to benefit by imbuing their current IMD product lines with end-to-end security and privacy techniques. Outright benefits for them

are more direct (i.e. extra device features) and less direct ones (i.e. less lawsuits due to reduced risks). A third set of stakeholders is the scientific world which can draw concepts and paradigms from the IMD-security domain to other neighbouring domains. One such example are Wireless Sensor Networks (WSNs) that are used in medicine, environment, industrial and city contexts.

2.1.3.2 Pricing

There is no clear strategy to monetize the security improvements at the time of writing.

2.1.3.3 Revenues

Revenue values are not available at the moment of this writing.

2.1.4 Customers & product promotion

As explained in Section 2.1.2.1, vertical penetration of the market is quite unrealistic an approach in this domain, especially for a small company like Neurasmus. Consequently, potential customers of the SHARCS-generated IMD technology are aimed to be one or more of the three major leaders in the field: Medtronic, St. Jude Medical or Boston Scientific.

Depending on the strategy to be implemented when results become available, product promotion will happen indirectly at first through high-impact publications in the field, reporting of use-cases in the Erasmus MC ecosystem and elsewhere as well as other scientific- and commercial- dissemination events/footnoteSee Deliverable D6.4 for a detailed presentation of such current activities.. In effect, this step is already going on for a few years and will only be reinforced through participation in the SHARCS project.

As a second step, and subject to future communications with the three leading IMD companies, promotion may be internal-only, for the benefits of those companies. It can also come as part of the general promotion of their products through their own channels.

2.1.5 Strategic collaborations with consortium members or other parties

Neurasmus has, so far, established close collaboration with two of the SHARCS consortium partners: Chalmers University of Technology (CTH) and Technical University of Braunschweig (TUBS). With CTH, the next generation of the IMD SoC is being developed and prototyped, and new security/privacy techniques are being explored. With TUBS, an exhaustive security attack tree for IMD security is being populated which is intended to be a reference

document for the whole IMD-security community. Furthermore, such a tree will help the SHARCS partners to identify current omissions in IMD security and better design end-to-end security techniques. TUBS also collaborates in the development of an improved security protocol for the SoC.

2.1.5.1 Identification of R/D opportunities

Almost all activities performed by Neurasmus have research and scientific value as the company is, primarily, R&D-oriented. All current activities within SHARCS are intended to lead to scientific publications and/or patents or licensed-IP for 3^{rd} parties to exploit. So far, only important publications have been scored.

2.1.6 Exploitation assessment for project-year 2

Although an IP-licensing approach is generally considered – in line with the standard Neurasmus approach – there is currently no exploitation plan for the IMD SoC technology. A plan will be formulated subject to the results of the SHARCS project, synergies with major IMD manufacturers and – less likely – any potential joint ventures with other consortium partners.

2.2 Elektrobit

Elektrobit Automotive (EBA) is an award-winning and visionary global supplier of embedded solutions, cloud computing and services for the automotive industry. A leader in automotive software, with over 25 years of serving the industry, Elektrobits products power over 70 million vehicles and offer flexible, innovative software solutions for connected car infrastructure, human-machine interface (HMI) technologies, navigation, driver assistance, electronic control units (ECUs), and software engineering services. Elektrobit has a long history in the development of various security solutions for the automotive market. It implemented different kinds of security modules and supports standards like HIS, SHE and AUTOSAR. Elektrobit was founded in 1988 as 3SOFT GmbH and was acquired in 2004 by the Finnish Elektrobit Corporation. Since the middle of 2015 Elektrobit is a wholly owned, independent subsidiary of Continental AG.

Elektrobit acts as a use-case provider for the SHARCS project. The main focus will be on research and development of new hardware and software security techniques to make Electronic Control Units (ECUs) more secure.

2.2.1 Product description & added value

Within SHARCS, the goal of Elektrobit is to enhance the Electronic Control Units (ECUs), as well as the on-board and off-board vehicle communica-

tion with security-oriented hardware and software components to prevent attackers from manipulating functionality or gaining unauthorized access to those ECUs. Such protection is essential for the safety and security of passengers on the road. In order to meet this objective the newly developed security features are evaluated and, if suitable, integrated into a prototype which can be shown to potential automotive customers to help them solve their security issues. Depending on the customer feedback, further development will be initiated to make a product out of it.

2.2.2 Market analysis

2.2.2.1 Technology trends

Vehicles are becoming ever more connected, and thus evolving into a mobile communication node in various directions. A smart car may communicate with other cars (Car-to-Car), with all kinds of infrastructure (Car-to-Infrastructure), with Cloud Services (e.g. real-time navigation or backup of settings) and with user appliances, such as smartphones, which can control it remotely. In this complicated setup all inter-connections and the components responsible for them (e.g. Electronic Control Units) must be secured. One of the major threats is the remote exploitation of vulnerability in an entire vehicle fleet. This must be prevented by new security concepts at all hazards.

2.2.2.2 User trends

The public is becoming more aware of security concerns in vehicles. There are plenty of press reports about cases where cars are hacked. A very prominent example is e.g. the Jeep attack [21]. End users are interested to have intact security measures in cars for several reasons. The most important might be the integrity and safety of their vehicle to allow smooth operation and a flawless and safe user experience they know for decades. With the new trends to connect vehicles and an increasing set of features being realised in software end users expect features and flexibility they know from e.g. the mobile industry. So topics like e.g. secure over the air software updates, introducing new features via additional apps over the lifetime of their vehicles, connectivity to social media or other online functionality. They would like to install new apps (e.g. navigation) or activate new functionality (e.g. driver assistance). Car sharing is also a prominent example for the usage of new and connected features via multiple platforms. E.g. the end user shall be able to release the door lock from the rental car with his smartphone and the interior like the seat shall be automatically adjusted to the needs of the driver. To realize such possibilities one needs to have virtual identities, payment options and probably many more personal data

exchanged with and maybe stored in vehicles. All these data shall not be exploitable, but introduces also a lot of privacy aspects to fulfil either personal and/or legal requirements.

2.2.2.3 Market placement & competitor analysis

Elektrobit provides security mechanisms for more than 15 years to car manufacturers. For several typical automotive use cases those mechanisms are partially standardized. In addition, many individual solutions exist and are used in vehicles already. Examples of this are mileage protection, Secure Onboard Communication and Secure Hardware Extension (SHE). However, as the car is ever more connected, new security concepts must be introduced. Currently, there is no common security solution available on the automotive market, but efforts are made throughout the industry to cope with the exploding number of new challenges for connected and autonomous vehicles.

2.2.3 Business model & future plans

The newly developed security features are evaluated and, if suitable, integrated into a prototype which can be shown to potential automotive customers to help them solving their security issues. Depending on customer feedback, further development will be initiated to make a product out of it.

2.2.3.1 Stakeholders

The stakeholders are the car makers (OEM), ECU producer (Tier1) and of course the end user (car owner/driver). They will all benefit from the enhanced security features and concept.

2.2.3.2 Pricing

There is no elaborated strategy to monetize the security improvements at the time of writing. Security is a fundamental and integral property of future vehicle infrastructure and the mobility ecosystem. It is neither feasible nor correct to put a price tag on a single mechanism. Insecure solutions will simply not be accepted by the market anymore. An indication for the necessity of such mechanisms can be derived from the costs of the latest recalls, e.g. by BMW or Jeep for implementing no or not feasible security solutions. Those costs easily reach million dollar figures.

2.2.3.3 Revenues

Revenue values are not available yet.

2.2.4 Customers & product promotion

During our 25 years in business, we've established deep relationships with carmakers and suppliers. We have been working with carmakers, including Audi, BMW, Daimler, Ford, GM, Volkswagen Group, Volvo, and more on their global technology. We will promote our new security concept to the carmakers and suppliers as soon we have evaluated the introduced security technologies and a prototype is available.

We had some initial discussion with major OEMs and presented the current state of the SHARCS project as well as our future plans. As the newly developed techniques are promising to them we will have follow-up meetings as soon as the project progresses.

2.2.5 Strategic collaborations with consortium members or other parties

We established close cooperation with two of the SHARCS consortium partners: FORTH and IBM - Science and Technology LTD. With FORTH we worked on the hardware Instruction Set Randomization (ISR) to prevent the injection of malicious code. Furthermore, we cooperated with IBM to be able to analyze parts of an automotive software stack with the IBM software model checking tool ExpliSAT. We also started the discussion with Chalmers University of Technology (CTH) on the usability of Control Flow Integrity (CFI) in an automotive environment.

2.2.5.1 Identification of R/D opportunities

Based on the discussions with FORTH we will evaluate Network Intrustion Detection System (NIDS) based on OpenCL. As some automotive microcontrollers are integrating graphics processors supporting OpenCL, this is a promising direction to speed up the deep package inspection process.

2.2.6 Exploitation assessment for project-year 2

Currently, we have not exploited any features of SHARCS.

2.3 OnApp Ltd

OnApp Ltd. is an SME that builds and provides cloud software platform solutions based on multiple layers of cloud services. It was created as a spin-off from a UK web-hosting firm in 2010. Its portfolio includes a CDN offering, a Federated Market Place, load-balancers, edge-servers, Disaster Recovery as a Service and an Integrated Storage system.

The main product, OnApp Cloud, is a platform that allows users to control and manage their own cloud services in a simple way. This links with a novel, distributed storage platform that provides an integrated storage solution that is an alternative to costly Storage Area Network (SAN) systems.

The Cloud use-case aims at securing the current public-cloud offerings and is extremely relevant to both OnApp and SHARCS, since it demonstrates real progress towards meeting the increased demands for security and trust that are expected to prevent public security scares. Security features, once integrated into the platform, will be available to all customers. If specific hardware extensions are developed, they will be incorporated in the platform in a way that they will be ready when a production-ready solution is released.

2.3.1 Product description & added value

Within SHARCS, the goal of OnApp is to develop an end-to-end secure platform for its customers by building security from the hardware up. Exposing Trusted Platform Modules and other hardware-based security primitives to the software platform is essential to ensure that security flaws at lower layers will not compromise the application execution. Providing and validating security in the cloud is extremely important for market sectors including enterprises, financial services, large-scale industry and governmental organisations such as health-care. Sensitive information cannot be guaranteed to be secure in the current cloud offerings. By addressing this problem, the public cloud market becomes accessible to these large sectors that up until now have held off from moving from their dedicated hardware infrastructures. This provides new opportunities for large-scale cloud deployments using consolidated data-center resources and thus lowering operating expenses. OnApp is investigating and working on integrating the findings of SHARCS through its proposed use-case.

OnApp intends to meet the following objectives outlined in ICT–32–2014[2] through its development work on improvements to its OnApp Cloud platform:

- ICT designed in Europe offering a higher level of security and/or privacy compared to non-European ICT products and services;
- ICT with a measurably higher level of security and/or privacy, at marginal additional cost compared to ICT technology following the traditional designs (i.e. implementing security as add-on functionality);
- Increased user trust in ICT and online services;

[2] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/273-ict-32-2014.html

- Improved ability for users to detect breaches of security and privacy;
- Improved protection of the user's privacy, in compliance with applicable legislation;
- More resilient critical infrastructures and services;
- Security and privacy provided as a built-in feature, simpler to understand and manage for the user compared to traditional ICT.

2.3.1.1 Product 1: Hardware-assisted security for OnApp Cloud

OnApp will expose hardware security primitives such as TPM (Trusted Platform Module) and Secure-boot from UEFI (Unified Extensible Firmware Interface) for secure computing. This will help with authentication and non-repudiation. It will also look at promoting hardware security accelerators available in modern processors for allowing increased utilisation of encryption to improve the confidentiality of data throughout the platform. These features will then be exposed, with changes to the UI (User Interface) that clearly show how improved security can be realised. As of December 2016, the TPM integration into the UI is fairly advanced. It has not yet been launched as a commercial offering but will undergo QA testing and should be ready for Year 3. Initial collaborative work has been carried out with FORTH to see how a GPU based, security acceleration framework could be integrated into the main version of OnApp Cloud.

2.3.1.2 Product 2: OnApp Cloudboot platform

OnApp will look at improving the security of its PXEboot environment, Cloudboot, which is used by a large amount of its customers. The Cloudboot platform is controlled by OnApp and provides a hypervisor (primarily Xen or KVM) with a number of open-source and proprietary components.

2.3.1.3 Product 3: OnApp continuous testing and QA framework

As an internal product for use within the QA system, OnApp will look at improving its current testing framework to include security testing that searches for known exploits. This will help avoid releasing software with known security vulnerabilities and will promote a high-quality, security-focused set of products.

2.3.1.4 Product 4: OnApp SHARCS secured template

Although not yet started as of Y2, OnApp intend to work with the security partners on the project to provide a secure, minimalistic Linux environ-

ment that has been hardened by SHARCS techniques. This template will offer improved security over non-hardened Operating Systems and may have specific security packages installed that make use of the security primitives exposed via the hypervisor platform mentioned in Product 2.

2.3.1.5 Product 5: CTH FPGA based NIDS, used in OnApp Cloud

Initial discussions regarding getting an implementation of a Network Intrusion Detection System (NIDS) from CTH integrated with the OnApp Cloud platform have started. The FPGA-based NIDS device will be installed on the OnApp Control Panel Server and possibly the backup server to monitor network traffic on the management and storage networks and raise any discovered attacks to the management platform for possible automated mitigation. More details of the expected integration are described in Deliverables D3.2 and D5.2.

2.3.2 Market analysis

2.3.2.1 Technology trends

Various reports exist as to how security will grow in the Cloud, but most sources agree that the trend is for cloud security to grow. Transparency Market Research in a January 2016 report has stated that it expects the cloud security market to grow to $11.8 BN (USD) by 2022 [15].

There have been suggestions that self-encrypting hard disk drives (2011 report [8]) and hardware with improved security would take a large part of the market. Trusted Platform Modules were for instance expected to be in most computing platforms, especially on high-end server appliances but this has not been the case. Where it has succeeded has been in the consumer market when tied with a good application, which is the case on Windows laptops with BitLocker [30] encryption. Intel as of the end of 2015, have released SGX [27] security extensions that enable secure memory enclaves for running trusted applications, which takes on a number of ideas from the TPM onto some of their SkyLake processors. To use SGX features, requires that both the CPU and the BIOS have support for SGX.

2.3.2.2 User trends

The EU Council adopted the General Data Protection Regulation [11] in April 2016 with it entering into force in May 2018[3]. It is a large change since the previous legislation that came into force in 1995 [32] (Directive 95/46/EC). This adds regulatory requirements into how companies will

[3] http://www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx

need to handle data, which in turn will mean platforms need to support these requirements.

Users are becoming more aware of data security concerns. This includes Snowden revelations (June 2013 [17]) and also widely published cases of data compromises. Data breaches are increasing in number and damage. A visualisation of the data breaches can be seen at the following link [26].

2.3.2.3 Market placement & competitor analysis

Current public cloud platforms like Google, Amazon and Microsoft, have been relatively slow at exposing security primitives to end-users except in the case of specific, customised applications. IBM's SoftLayer has provided access to the Intel TXT platform [39] for bare-metal offerings [5]. There has also been some effort from Intel to introduce security to OpenStack [14]. Amazon AWS [1], Google Cloud [19] and Microsoft Azure [31] promise that security and availability are their primary concerns. It is not clear though if Amazon, Google and Microsoft expose TXT/TPM features on their cloud offerings. For other hardware features such as AES acceleration the companies do offer solutions and differentiate accordingly [2, 20, 28].

2.3.3 Business model & future plans

2.3.3.1 Stakeholders

The primary stakeholder of the output for OnApp's contributions to SHARCS will be the OnApp customer-base. Another set of stakeholders are the OnApp cloud developers who will benefit from internal dissemination regarding security features and primitives.

Ultimately the largest set of stakeholders that will benefit from the improvements are OnApp's customers' customers, the end-users. They will benefit from a more transparent and secure platform and will potentially be able to offer new services based on the increased transparency in the platform.

2.3.3.2 Pricing

There is no clear plan to monetise the security improvements at the time of writing. Security features should be made available to all customers as and when they are integrated. The monetisation will only be realised through having a product that has better security than the other Cloud Service Providers. If an additional service is created then it may be possible to market this as a separate product that will have its own business plan and associated revenue.

2.3.3.3 Revenues

No projections on estimated revenue are possible at this time. A market survey, determining how many customers would be willing to pay either in money, degraded performance, or a reduced feature set for a security focused platform has not yet been carried out. It is expected, though, that – with the additional security features – the OnApp Cloud platform will differentiate itself from other competitive solutions and subsequently allow us to grow our customer base.

Although not a direct revenue, OnApp also envisages that by complying with regulations and also providing best-of-breed services, the security mechanisms will help prevent the risk of the company and its customers losing money from lawsuits related to security breaches. OnApp relies on ensuring that its customers are market competitive and are in a position to pay on-going licences so it is in OnApp's interest to provide security mechanisms to customers.

2.3.4 Customers & product promotion

Any new security features that are exposed in the product will be part of the standard publicity process, including release notes and tweets. Given that the outputs are also part of the SHARCS project, it will be possible to update the SHARCS twitter feed and webpage when new SHARCS security features are added to the OnApp product range. Additionally, OnApp will be able to provide press releases if there are particular security features that are of interest to the more general community.

2.3.5 Strategic collaborations with consortium members or other parties

Currently, there have been no specific, strategic collaboration activities to report. The work that is being carried out into integrating various security features may lead to further projects being proposed and for potential joint marketing into joint product offerings.

2.3.5.1 Identification of R/D opportunities

Based on initial discussions with CTH, it is expected that a Network Intrusion Detection System (NIDS) will be worked on as an FPGA that could be added into the Cloud environment and then exposed to customers if they have installed the CTH FPGA solution.

Discussions have also taken place with FORTH for working on GPU-based security mechanisms that could also be exposed in the Cloud platform.

2.3.6 Exploitation assessment for project-year 2

Currently, we have not exploited any features of SHARCS within the OnApp product range but it is planned to release many features that are integrated in the prototype by the end of the project. The TPM hardware module has been integrated with the OnApp Cloud but this is not yet available in the commercial product offerings. The identification of R/D opportunities mentioned previously, have now progressed further into designing the actual implementations of the security features and also determining how to best integrate them into the OnApp Cloud product.

2.4 IBM - Science and Technology LTD

For more than sixty years, IBM Research, as the world's largest IT research organization has been the innovation engine of the IBM corporation. Since the beginning of 2000, IBM has spent $75 billion in R&D, enabling IBM to deliver key innovations and maintain U.S. patent leadership.

The Quality and Security Department of the IBM Haifa Research Lab is a part of an assembly of cyber security research facilities in Israel which are at the heart of IBMs growing investments in cyber-security. The Quality and Security Department combines cyber security and privacy research with research in areas of verification, operating systems, compilers, data analytics and systems. In recent years, IBM as an international entity, makes significant investments in the area of cyber-security in Israel. The Quality and Security Department of the IBM Haifa Research Lab serves as a bridge between cyber-security in Israel, European cyber-security research and IBM. Through its investments, IBM has become a leader in the area of cyber-security.

2.4.1 Product description & added value

Within SHARCS, the goal of IBM Research is to develop tools to support secure-by-design applications and services. IBM tools detect security vulnerabilities at design time and help the developer debug their software and make it secure.

2.4.1.1 ExpliSAT

ExpliSAT is a formal verification tool for C/C++, based on symbolic interpretation. Given the C/C++ source code of the application, ExpliSAT explores the control flow graph of the application path by path using symbolic (non-deterministic) inputs, aiming at detecting feasible execution paths on which "bad things", such as assertion failures, null pointer dereferences etc. may occur [4] [7]. In the SHARCS project the tool is being extended to automatically detect security vulnerabilities in C/C++ software, such as buffer

overflow in malicious-input-based allocated buffers (see, e.g. Heartbleed bug in OpenSSL). Also, IBM develops novel technologies capable of proving that a user application is free of certain types of vulnerabilities, to support the secure-by-design principle. Finally, in order to automate the process of security-vulnerability detection, IBM is building a platform consisting of emulation of the behavior of the functions defined in standard libraries (such as libc and libstdc++), for achieving full source code observability required for a precise checking. The tool is being built for all types of users, focusing on software developers that are not experienced with formal verification.

2.4.2 Market analysis

To the best of our knowledge, the current offer for formal-verification tools for C/C++ software comes mainly from Academia, e.g. the CBMC tool from the Oxford university [6] or the CPAChecker tool from the Passau University [10]. The purpose of those tools – as is common for tools developed in academia – is more to provide a platform on which novel algorithms and technologies can be developed and evaluated, and less to target the goal of verifying real industrial-scale software projects, which requires extensive development of different features that are beyond pure research.

There are, also, several static-analysis tools available for vulnerability detection such as Coverity [9] and AppScan source [24]. These tools are performing scalable code scanning, however they suffer from a high rate of false positives due to their aggressive abstractions. In addition, it is much more difficult for these tools to generate concrete tests that demonstrate vulnerabilities. These tests are essential for analyzing, debugging and resolving vulnerabilities in the code under test.

2.4.3 Business model & future plans

The ExpliSAT for security tool is planned to be used both internally and externally:

- Internally, the ExpliSAT for security tool has started to be used in the IBM system division to detect security vulnerabilities in firmware code, and in the IBM security division to detect security vulnerabilities in OS code and software services.
- Externally, the ExpliSAT for security tool is evaluated by a small number of IBM customers for verifying firmware code.

We plan to integrate our technology with a vulnerability detection service developed by IBM Appscan [23] provided on the IBM Bluemix PaaS offering [25] (IBM's next generation cloud application development platform). Enabling use of the tool by all software developers without prior

knowledge and experience in verification makes our technology a good candidate to be deployed in many software companies and particularly internally at IBM. As part of our exploitation strategy, we plan to continue deploying the ExpliSAT technology internally to promote secure-by-design IBM products.

2.4.4 Strategic collaborations with consortium members and/or other parties

Within SHARCS, the main collaboration is with use-case providers: NEU, ONAPP and EBA. As a part of this collaboration, software formal-verification trials for security-vulnerability detection will be performed for the software components of the SHARCS applications in the relevant domains, respectively, of medical implants, cloud and automotive software.

2.4.5 Exploitation assessment for project-year 2

So far, we have managed to deliver the ExpliSAT tool internally to software teams. Also, ExpliSAT tool is evaluated by several semiconductor companies. Within the scope of SHARCS project, ExpliSAT was delivered to use-case providers, for being applied to the software components in the applications they are developing.

Patent application number 15/084617 “Dynamic control-to-data transformation to cope with path explosion in symbolic execution” was filed by IBM.

3 Exploitation strategy of academic partners

In this chapter, exploitable results and future strategies per academic partner will be detailed.

3.1 FORTH

FORTH has adopted an evolving strategy towards promoting the commercial exploitation of R&D results by providing services, licensing specific products to industrial partners, contracting with industrial partners to jointly develop new products, and participating in start-up/spin-off companies and joint ventures. FORTHnet S.A., a spin-off company of FORTH, was founded in 1995, and is now quoted in the Athens Stock Exchange, while it continues to be involved in related R&D activities. FORTH has played a major role in the development of the Science and Technology Park of Crete (STEP-C). FORTH aims to exploit the SHARCS assets both by research and innovation actions.

3.1.1 Current exploitation progress vs. targets

The main objective of FORTH participation in SHARCS is to perform research in the area of secure processor architectures, system software security, and high-performance attack detection and mitigation. The goal is to produce new knowledge that can be used both for education and training of young scientists, but also lead to commercial exploitation if possible. More specifically, our strategy is to explore the possibility of migration of software security techniques onto the processor hardware, and adaptation of system software to exploit these new features. Also, utilization of existing hardware capabilities to build more secure computing systems is investigated: In particular, use of graphics-processing units (GPUs) to accelerate detection of network based attacks in real-time, up to speeds of tens of gigabits

per second. Lastly, implementation of security techniques on hardware and operating system level.

3.1.2 Teaching/education

As FORTH is a Research Center it does not have the teaching activities of University partners. However, FORTH has been contributing towards education via its fellowship and practical training programs. FORTH engages a number of post-doctoral, doctoral, masters and undergraduate students in research and innovation projects. This is also the case in the SHARCS project. In this way, young scientists and early-stage researchers gain the skills necessary to succeed in the marketplace. Furthermore, permanent research staff from FORTH are advising university students performing their undergraduate and graduate theses. Moreover, graduate students affiliated with FORTH collaborate with University of Crete, as teaching assistants in a variety of computer science courses. Lastly, university faculty, are also employed at FORTH and transfer knowledge to the university students through the regular courses taught as part of the curriculum.

3.1.3 Valorization, spin-offs and other commercial activities

FORTH has developed extensive cooperation with R&D centers and companies throughout Europe and the world and is a member of the European Research Consortium of Informatics and Mathematics (ERCIM), and a cofounder of EuReCCA the European Research Center on Computer Architecture. EuReCCA is currently establishing an innovative mechanism to promote entrepreneurship and the commercial exploitation of research results in Computer Architecture and Computing Systems. FORTH has recently been successful in commercializing storage-related technologies that it has developed in the context of FP7 programs. The technology has been licensed to a major international corporation. In addition, FORTH has an established relationship for further interaction on technology issues. FORTH has applied for a number of patents in the area of infrastructures as part of its overall exploitation plans. FORTH will use this project to identify potential components that may evolve into new products and services, as has happened in the case of FORTHnet and the more recently licensed technologies. The SHARCS results give FORTH a critical advantage in technology and help FORTH establish solid alliances with business stakeholders for commercializing innovative ideas applying the SHARCS end-to-end security approach to its pre-commercial products.

3.1.4 Synergies and collaborations with other parties

FORTH participates in SHARCS with the Distributed Computing Systems laboratory (DCS). DCS has many collaborations with other top institutions in Europe and in the United States. More precisely, this year, collaborations with Vrije University Amsterdam, Stony Brook University, Qatar Computing Research Institute have been established which have led to publications in international research conferences. Here are some representative ones relating to project SHARCS:

- Collaboration with Qatar Computing Research Institute and Stony Brook University. **Efficient Software Packet Processing on Heterogeneous and Asymmetric Hardware Architectures** In the IEEE/ACM Transactions on Networking.

- Collaboration with VU University Amsterdam. **GRIM: Leveraging GPUs for Kernel Integrity Monitoring** In Proceedings of the 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID). September 2016, Paris, France.

We are currently in close collaboration with Neurasmus BV and Chalmers University on the design of secure IMD SoCs, and with Chalmers University on research regarding hardware implementations of Instruction Set Randomization, a defensive technique against code injection attacks. Also, we have implemented with Elektrobit a FPGA prototyping platform to demonstrate and evaluate SHARCS hardware with Instruction Set Randomization (ISR).

3.2 Technische Universität Braunschweig

Established in 1745, the Technische Universität Braunschweig (TUBS) is the oldest technical university in Germany with Carl Friedrich Gauß as one of its early students and lecturers. Embedded systems are one of the core research areas of the EE department that continuously ranks in the top 10 EE departments in Germany.

The Institute of Computer and Network Engineering (IDA) also has more than 20 years experience in the architecture and design of reliable computers and fault tolerant mass memories for space applications. Based on this work, embedded system reliability has become a second research focus. In the ongoing ARTEMIS project RECOMP that covers reduced cost certification of mixed criticality multicore systems, IDA coordinates the large work-package on HW/SW technologies. Further collaborative projects in multiprocessor systems-on-chip reliability are concerned with dependable

networks-on-chip funded by the German BmBF and with reliable microkernels implemented on unreliable technologies for safety applications funded by the German DFG (Deutsche Forschungsgemeinschaft).

3.2.1 Current exploitation progress vs. targets

TUBS will leverage its expertise in instruction randomisation, and policy definition and enforcement by the runtime environment to contribute to the software system and tools that will be developed in WP4. TUBS leads WP6 (Dissemination and Exploitation) where it will coordinate the activities that will improve the impact of the work done by SHARCS.

3.2.2 Teaching/education

We have already integrated SHARCS material in our graduate Advanced Operating Systems course and we have made SHARCS-based presentations in the graduate seminar program.

3.2.3 Synergies and collaborations with other parties

We are currently in close collaboration with Neurasmus BV on the design of secure protocols for the communication of IMDs with attendant devices. We are also pursuing collaboration with Elektrobit in order to better understand the specific constraints of software systems in an automotive environment.

Finally, we are cooperating with the Controlling Concurrent Change (CCC) Forschungsgruppe funded by DFG on securing the execution of software components in complex distributed real-time systems (space-based and vehicular platforms).

3.3 Vrije Universiteit Amsterdam

Vrije Universiteit Amsterdam hosts one of the leading Computer Science departments in the Netherlands. Our primary research focus is on computer systems, with a strong emphasis on security, high-performance computing, and distributed systems. Our research output is characterized by high-quality publications and the development of experimental software. Software products developed within the department, such as Argos, MINIX, IBIS, and SWI Prolog, are actively used by many industrial and academic institutes worldwide. Internationally, we collaborate in many EU projects including several coordination actions and networks of excellence. On the global level, we have special partnerships with several countries, such as Brazil, China, India, South Africa, and the United States. The department has also nurtured extensive collaboration with industry and applied research

outside the university. Our project partners include Google, Microsoft, Amazon, Symantec, Philips, Yahoo!, SAP, IBM, CISCO and INFOSYS.

3.3.1 Current exploitation progress vs. targets

As an academic partner, our exploitation plan mostly consists of courses and publications.

3.3.2 Teaching/education

At the moment, we have eight courses related to the SHARCS project.

- B.Sc. level

    1. **Operating Systems** gives an introduction to the internals of operating systems, and covers topics such as operating system architectures, processes, threads, synchronization, memory management, file systems, input/output, and virtualization.
    2. **Computer Networks** covers the fundamental concepts in digital communication and computer networking. Topics covered include: the datalink layer, the network layer, the transport layer, and the application layer. The focus of this course is on the Internet and the popular protocols that are used in the Internet (TCP, UDP, Ethernet, Wifi, etc.).
    3. **Computer Systems** gives an overview of fundamental topics in Computer Architecture and Operating Systems, illustrating how high-level software interacts with the operating system and with the underlying hardware. Examples of concepts covered during the course are: pipelining, Amdahl's law, fault detection and correction, and caching.
    4. **Secure Programming** allows students to familiarize with programming software that incorporates useful features for security purposes. For example, students develop programs that perform cryptographic operations, communicate using encrypted connections, exchange certificates, and so on. During the course, students are exposed to APIs (OpenSSL) for cryptographic operations, such as symmetric/asymmetric encryption, cryptographic hashing, cryptographic protocols, digital certificates, encrypted sockets, and SSL/TLS.

- M.Sc. level

    1. **Kernel Programming** features a number of hands-on assignments accompanied by lectures on advanced operating system kernel design and programming concepts. In each assignment, students

are expected to start with a minimal kernel implementation and exercise their kernel hacking skills on one of the major operating subsystems (i.e., memory management, drivers, etc.). This involves programming in both C and assembly as well as directly interfacing with the hardware. The course also links lectures and assignments to modern operating system features and offer insights into state-of-the-art OS research efforts.

2. **Computer and Network Security** is a challenge-based course covering a wide spectrum of security issues. We explicitly focus on systems security to show students how attackers penetrate systems. Specifically, the course covers topics on (1) network security (sniffing, spoofing, hijacking, exploiting network protocols, DDoS, DNS attacks, etc.), (2) memory corruption and application security (buffer overflows, format string bugs, dangling pointers, shellcode, return oriented programming, ASLR/DEP/canaries, control flow integrity and advanced new ways of exploitation), (3) web security (XSS, SQL injection, CSRF, http cache poisoning, SOP, authentication, etc.), (4) botnets (centralised/P2P, fast flux, double flux), (4) crypto (basics, systems aspects).

3. **Secure Software** focuses on advanced exploitation techniques that can compromise software systems of different domains. Students need to complete 4 self-contained assignments during the course. Three assignments are oriented towards advanced exploiting of applications in three different domains: (a) the Linux kernel, (b) a mobile device, (c) a web application and the browser. The fourth assignment targets understanding and implementing defenses that could potentially protect the systems that are compromised in assignments (a)-(c).

4. **Binary and Malware Analysis** deals with the hard problem of analyzing malware binaries, which, other than source code, does not provide human readable information on used data structures or the actual behavior of the code.

3.3.3 Synergies and collaborations with other parties

Vrije Universiteit Amsterdam participates in SHARCS with the Systems and Network Security (VUSec) group. VUSec has many collaborations with other top institutions in Europe and in the United States. For example, collaborations with FORTH and Ruhr-Universität Bochum have led to publications in top academic venues in computer security. Here are some representative ones:

- Collaboration with FORTH. **ShrinkWrap: VTable Protection without Loose Ends**. In Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC), 2015. **Best student paper award**.
- Collaboration with FORTH. **HCFI: Hardware-enforced Control-Flow Integrity.** In proceedings of the 6th ACM Conference on Data and Applications Security and Privacy (CODASPY), 2016.
- Collaboration with Ruhr-Universität Bochum. **A Tough call: Mitigating Advanced Code-Reuse Attacks At The Binary Level**. In Proceedings of the 37th IEEE Symposium on Security and Privacy (Oakland), 2016.
- Collaboration with Ruhr-Universität Bochum. **Undermining Information Hiding (And What to do About it)**. In Proceedings of the 25th USENIX Security Symposium (USENIX SEC), 2016.

We expand more on the content of these publications in deliverable D6.4.

3.4 Chalmers Tekniska Högskola

Chalmers University of Technology is among the top technical universities in Sweden. The Department of Computer Science and Engineering (CSE) has already participated in a large number of research projects. Our activities address the needs of Swedish and European industry and cover a wide spectrum of ICT needs, with the goal to develop advanced technologies and products. The outcome of our research has led in several occasions to commercialization and exploitation. We work closely with the R&D of large companies such as Ericsson, RUAG and Volvo, creating opportunities for industrial uptaking of our research. In addition, research results have enabled us to create startup companies, such as the ZeroPoint Technologies AB, founded by Prof. Per Stenström. Such activities are facilitated through the Chalmers Innovation Center, which has as a main goal to facilitate the commercialization of promising research results.

3.4.1 Current exploitation progress vs. targets

The main objective of Chalmers participation in SHARCS is to perform research in the area of Secure SoC architectures. Our activities in the project are expected to:

1. Create new knowledge and enhance our research activities;
2. Develop new software modules and hardware IPs of potential exploitation interest;

3. Be used for educating young researchers and for improving our teaching activities.

Below, we attempt to identify future opportunities for exploitation, and describe current exploitation activities.

3.4.1.1 Identification of academic/research opportunities

We have so far identified the following opportunities for using project results. In the SHARCS project, Chalmers will contribute to the following topics: (i) Secure IMD SoC architectures, (ii) secure IMD communication, and (iii) FPGA-based Network Intrusion Detection Systems. New knowledge produced from our research in the project will include hardware IPs, software modules and system-level methodologies. We have not yet exploited any project outcomes as we are still in a design of early implementation phase of our techniques. While working on the above topics we will be frequently looking for potential opportunities for exploitation.

3.4.2 Teaching/education

As an academic partner, Chalmers actively seeks ways to exploit the SHARCS project activities for educating young researchers. One new PhD student has been recruited and works in the project and one more (industrial PhD working for Neurasmus) is co-advised by a Chalmers faculty member in SHARCS-related topics. In addition, we intend to propose MSc-thesis topics related to our project activities in order to attract MSc students. Finally, we intend to include the experience gained from our involvement in the project to improve our teaching activities (i.e., courses, labs, tutorials).

3.4.3 Valorization, spin-offs and other commercial activities

We will consider the exploitation of our project results, such as the ones described in the previous subsection, through licensing, patenting or even through potentially creating a spin-off company. Such activities will be facilitated by the Chalmers Innovation Centre. Chalmers Innovation offers services which shorten the time to market for newly started, science-based companies; it assists on finding capital or even provides capital, offers know-how on setting up a start-up company, and offers offices to host such company. In the past, Chalmers Innovation has assisted with setting up companies, which were based on interesting research results of our group; one such example is ZeroPoint Technologies AB, founded by Prof. Per Stenström.

3.4.4 Synergies and collaborations with other parties

We are currently in close collaboration with Neurasmus BV and FORTH on the design of secure IMD SoCs. In addition, we discuss security-related topics with Volvo Group, who is active in security related research for automotive systems.

Bibliography

[1] Amazon. AWS Cloud Security. https://aws.amazon.com/security/.

[2] Amazon AWS. Protecting Date Using Server-Side Encryption. http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html.

[3] O. Aquilina. A brief history of cardiac pacing. *Images in Paediatric Cardiology*, 8(2):17–81, 2006.

[4] S. Barner, C. Eisner, Z. Glazberg, D. Kroening, and I. Rabinovitz. ExpliSAT: Guiding SAT-based software verification with explicit states. In *Hardware and Software, Verification and Testing*, pages 138–154. Springer, 2007.

[5] Business Cloud News. IBM SoftLayer adds Intel chip security tool to bare metal cloud. http://www.businesscloudnews.com/2014/09/08/ibm-softlayer-adds-intel-chip-security-tool-to-bare-metal-cloud/, sep 2014.

[6] CBMC. Bounded model checking for software. http://www.cprover.org/cbmc/.

[7] H. Chockler, D. Pidan, and S. Ruah. Improving representative computation in ExpliSAT. In *Hardware and Software: Verification and Testing*, pages 359–364. Springer, 2013.

[8] T. Coughlin. Solid security: The rise of self-encrypting solid state drives. http://www.snia.org/sites/default/files/Solid%20Security%20012412.pdf, 2011.

[9] Coverity. Homepage:. http://www.coverity.com/.

[10] CPAchecker. The configurable software-verification platform. http://cpachecker.sosy-lab.org/.

[11] EC. EC Proposal for General Data Protection Regulation. http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf, jun 2015.

[12] H. Ector and P. Vardas. Current use of pacemakers, implantable cardioverter defibrillators, and resynchronization devices: data from the registry of the european heart rhythm association. *European Heart Journal Supplements*, 9(suppl I):I44–I49, 2007.

[13] B. J. Feder. A heart device is found vulnerable to hacker attacks. http://www.nytimes.com/2008/03/12/business/12heart-web.html, mar 2008.

[14] C. Forrest. Intel Security Controller Aims to Better Secure OpenStack Clouds. http://www.eweek.com/cloud/intel-security-controller-aims-to-better-secure-openstack-clouds.html, sep 2015.

[15] C. Forrest. Cloud security market to be worth $12 billion by 2022, here's why. http://www.techrepublic.com/article/cloud-security-market-to-be-worth-12-billion-by-2022-heres-why/, jan 2016.

[16] Freedonia group. Report: U.S. Demand for Implantable Medical Devices to Reach $52B in 2015. http://www.qmed.com/mpmn/medtechpulse/report-us-demand-implantable-medical-devices-reach-52b-2015, mar 2012.

[17] M. Gidda. Edward Snowden and the NSA files timeline. http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, aug 2013.

[18] B. Goldsmith. First wi-fi pacemaker in us gives patient freedom. http://www.reuters.com/article/us-pacemaker-idUSTRE5790AK20090810, aug 2009.

[19] Google. Google Cloud Platform Security. https://cloud.google.com/security/.

[20] Google CS. Google Cloud Storage now provides server-side encryption. http://googlecloudplatform.blogspot.co.uk/2013/08/google-cloud-storage-now-provides.html, aug 2013.

[21] A. Greenberg. Hackers remotely kill a jeep on the highwaywith me in it. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, jul 2015.

[22] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, 2008.

[23] IBM. AppScan Mobile Analyzer Service . https://www.ng.bluemix.net/docs/services/AppScanMobileAnalyzer/index.html?S_TACT=.

[24] IBM. AppScan Source. http://www-03.ibm.com/software/products/en/appscan-source.

[25] IBM. IBM Bluemix . http://www.ibm.com/cloud-computing/bluemix/.

[26] InformationIsBeautiful. World's biggest data breaches. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks.

[27] Intel. Intel Software Guard Extensions (Intel SGX). https://software.intel.com/en-us/isa-extensions/intel-sgx.

[28] J. Kornich. Using AES-128 Dynamic Encryption and Key Delivery Service. https://azure.microsoft.com/en-gb/documentation/articles/media-services-protect-with-aes128/, feb 2016.

[29] K. Kumar and S. Bishop. Financial impact of spinal cord stimulation on the healthcare budget: a comparative analysis of costs in canada and the united states. *J Neurosurg*, 10:564573, 2009.

[30] Microsoft. BitLocker Drive Encryption Overview. http://windows.microsoft.com/en-gb/windows-vista/bitlocker-drive-encryption-overview.

[31] Microsoft Azure. Microsoft azuere cloud security. https://azure.microsoft.com/en-gb/documentation/infographics/cloud-security/.

[32] L. Musthaler. Will the European Union's new General Data Protection Regulation impact your business? http://www.networkworld.com/article/3020031/security/will-the-european-unions-new-general-data-protection-regulation-impact-your-business.html, jan 2016.

[33] A. M. Research. World medical implants market: Opportunities and forecasts 2014 – 2022. Technical report, Aug 2016.

[34] R. M. Seepers. *Implantable Medical Devices: Device security and emergency access*. PhD thesis, Erasmus University Medical Center, Rotterdam, Netherlands, December 2016.

[35] R. M. Seepers et al. Peak misdetection in heart-beat-based security characterization and tolerance. *IEEE EMBC*, 2014.

[36] R. M. Seepers et al. Enhancing heart-beat-based security for mhealth applications. *IEEE J-BHI*, 2015.

[37] R. M. Seepers et al. On using a von neumann extractor in heart-beat-based security. In *IEEE Trustcom*, pages 491–498, 2015.

[38] R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, and C. Strydis. Secure key-exchange protocol for implants using heartbeats. In *Proceedings of the ACM International Conference on Computing Frontiers*, CF '16, pages 119–126, New York, NY, USA, 2016. ACM.

[39] SoftLayer. Intel Trusted Execution Technology. http://www.softlayer.com/intel-txt.

[40] C. Strydis, D. Zhu, and G. Gaydadjiev. Profiling of symmetric-encryption algorithms for a novel biomedical-implant architecture. In *Proc. 5th Conference on Computing Frontiers*, pages 231–240, Ischia, Italy, May 2008.

[41] J. Turner, W. Hollingworth, B. Comstock, and R. Deyo. Spinal cord stimulators (scs) for injured workers with chronic back and leg pain after lumbar surgerya prospective study to describe costs, complications, and patient outcomes: Final report. Technical report, Washington State Department of Labor and Industries, Olympia, WA, September 2008.