DIMECC

FINAL REPORT 7/2017

THE FINNISH CYBER TRUST PROGRAM 2015–2017

DIMECC PUBLICATIONS
SERIES NO. 20

The Finnish Cyber Trust Program 2015–2017

DIMECC

FINAL REPORT 7/2017
DIMECC Publications Series no. 20

DIMECC Program
CYBERTRUST

Images | iStock
Graphic design & layout | Katja Kuuramaa, Cultural Cooperative Vehrä

Publisher | DIMECC Oy
Korkeakoulunkatu 7
33720 Tampere
www.dimecc.com

ISBN 978-952-68735-4-1 (Print)
ISBN 978-952-68735-5-8 (PDF)

Helsinki, Finland 2017

Content

The Finnish Cyber Trust Program 2015–2017

In 2013, Finland created a national cyber security strategy and as a part of that newly defined strategy were also cyber security research. The goal was to form a consortium that would create first the Strategic Research Agenda and then to follow that with a cyber security research program. These activities were planned to be led by a company now known as DIMECC. The SRA was finalized in 06/2014 and the first version of Cyber Trust –program plan was approved in 10/2014. Our plan was to gather all key domains and contributors under one umbrella and form a consortium strong enough to meet the challenging target set in the national level strategy, to become the leading country in Cyber Security by 2016. Initially, this was also happening. With a large systemic program comes also other opportunities and since we had all the needed attributes in place (strong industry commitment, world class research and solid background), we got tremendous interest also internationally. Everything was good and we were ready to start the work, at least so we thought.

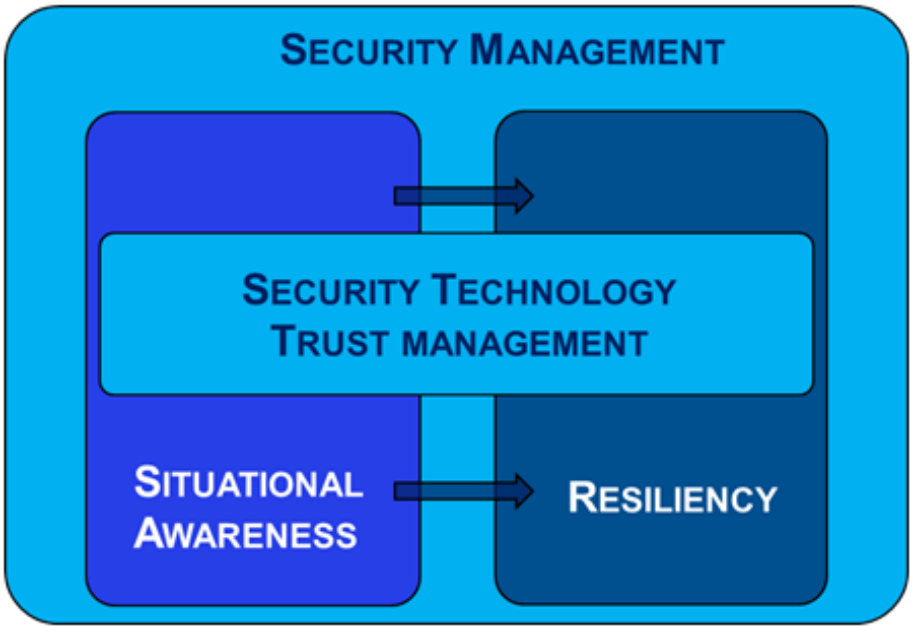
Back then, the funding environment as well as the political environment was different and when these change, the effect is difficult to predict. In our case, the change hit hard on us. We received the most unfortunate news, the negative funding decision. It is n Needless to say, that the consortium was shocked. We had two options, to give up or to keep pushing this important topic. So we pushed, hard. With strong and unified collaboration with national funding agency, TEKES, we managed to find a way to move forward. As there was very little we could do for the environment, we decided

to re-group our targets and change the program plan to match the frame we defined together with TEKES. Many man years were required for SRA and a first program plan, so we had enough material and also commitment to introduce these changes. What was planned to be 100 partners were cut down to less than half, volume went down to one quarter and length into half from the original. It is needless to say that our original target to lead the way in global cyber security field became even more challenging. But finally, after two years from the introduction of National cyber security strategy, the Cyber Trust -program was established. Looking back, this phase played an important role in the program creation. What might have been seen as a challenge in the beginning was actually helping us to build stronger collaboration with all key stakeholders. This collaboration carried us through program span and it is still playing role even after the program has ended.

The program was originally introduced as "Cyber Security -program" but the name was soon changed into "Cyber Trust" and our slogan was defined as "we bring the Trust to the Digital World". Main reason for the change was the fact that we wanted to create a positive reaction towards the program and "trust" is something that we all can attach to. Knowing that we had only a two years program, we defined our targets to be ambitious yet achievable. When introducing these changes, the agile working methods and processes used in DIMECC programs came in handy. Without those, this task would have been close to impossible. The program itself was formed around jointly defined tasks and deliverables called "business cases" where each case was reflecting the goals and targets of various partners. Input from the business cases and SRA were used when program structure and work packages were defined. With this approach, we managed to build natural collaboration between program partners and it was essential for the whole program execution.

Themes

In first version of Cyber Trust Program, we approached the cyber security with the following themes: security technology, situation awareness, security management and resiliency (see Figure 1). We need to be aware, have correct understanding of security incidents, network traffic and other important aspect that affect security. Therefore, we need situation awareness. For protection, we need security technologies, but we must not forget human aspects and managing security correctly, either. For that, we need security management. As a result, we will have resilient systems, services and infrastructures that are able to resist and recover from disturbances caused by the surrounding hostile environment.



Research themes of the research agenda.

From the beginning, the program targeted to provide a roadmap to the Vision for 2019, as defined in the SRA:

> *Finland will be a globally recognized hub for trusted and trust enhancing digital services based on top level cyber security solutions and services that are actively developed and maintained in international cooperation by leading experts and companies. Shortly, the program (?) presents Finland as trusted partner in Cyber Security domain.*

The aim as stated in SRA was to create a solid foundation for security-related research and technology development in Finland. During the program execution, various methods, tools and business models were planned to be taken into use in Finnish industry with the *main breakthrough target to return privacy and trust in digital world and to gain a global competitive edge in security-related business.*

Other breakthrough targets were defined as follows:

Proactive – design for security: A new proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries.

Self-healing – utilizing the toolbox: Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing.
Changing the mindset – building the Brand: Enable seamless cyber security integration into every-day life. By efficiently utilizing tools and methods provided through this program, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public awareness and understanding will move towards accepting cyber security as a natural element of a connected world. As a result, Finland will be recognized as an opinion leader in the cyber domain.

Even though the program ended up being shorter than originally planned, we still agreed to keep the same frame structure in our high level targets as we had in our first program plan. This was possible through focusing our work on most relevant tasks and deliverables of each business case. What came out from this process was defined as follows:

Overall target:
A new proactive approach of cyber security that is driven by knowledge of vulnerabilities threats, assets, potential attack impacts, and the motives and targets of potential adversaries.

Research objective:
The main **research objective** was to *improve the privacy, trust and decision making in digital infrastructure by monitoring, analysing, virtualizing, and visualizing traffic, objects and events.*

Concrete aims – based on the concrete WP –level targets:

- **Proof of concepts and demonstrations in major events and conferences**
    - Global visibility will help partners to improve their businesses
    - Showcase our capability for innovations through collaboration
- **World class results through ground-breaking research**
    - Research is done in close co-operation with industry partners
    - High quality publications
- **Establish international collaboration**
    - Cyber security research center established together with National Science Foundation (US).
    - Provide support for partners towards other international funding elements, e.g. Horizon 2020.

It's hard to say if any other program in the past has went through the same as we did in order to even start the work, it's possible, but I doubt it. At the end of the day, I do think that this process also made us stronger. With this history, we went to work.

Final words

Program consortium was committed to work towards the goals and with great success! In just two years, the results of the work are convincing, as can be seen from our website (http://cybertrust.fi/). Way more than 100 referenced publications already available and still counting! I can comfortably say that we've achieved the goals we defined and agreed. This all was possible with a truly remarkable consortium, easy-to-work with attitude and commitment to rely on. I do trust that this work done by program partners will be used as a baseline to build something new and I also trust that partners will continue their collaboration in new projects and challenges.

In my role as a program director in Cyber Trust, I can only thank all the program partners for your excellent participation and commitment you have shown throughout the program years, and our funding agency TEKES for the continuous support in making this happen. I've enjoyed the ride, hopefully you have done so as well.

Markku Korkiakoski
Program Director
DIMECC Cyber Trust

Battle For Cyber Security Continues

Cybersecurity is one of today's most challenging societal security problems, affecting both individuals and organizations such as large commercial companies, small to medium sized enterprises (SMEs), non-governmental institutions (NGOs) or governmental institutions. Deliberate or accidental threats and attacks threaten digitally administered data and digitally handled processes. Sensitive data leaks can ruin the reputation of companies and individuals, and the interruption of digital processes that organizations rely on in their daily work flow can cause severe economic disadvantages. Reaching beyond the technology-focused boundaries of classical information technology (IT) security, cybersecurity strongly interrelates with organizational and behavioral aspects of IT operations, and the need to comply with the currently actively developing legal and regulatory framework for cybersecurity. For example, the European Union (EU) recently passed the Network and Information Security (NIS) directive that obliges member states to get in line with the EU cybersecurity efforts. Most EU member states and the EU itself have a cybersecurity strategy in place by now, which will eventually lead to the introduction of laws and regulations to fulfil cybersecurity requirements.

Looking back to the setup and starting point of initiating the DIMECC Cyber Trust program, it probably could not be time wisely better selected. There was an earthquake situation arisen with Snowden revealing the black truth for public awareness of our everywhere reaching networking. If we had any trust transferring business related information via public networks, it was washed away with a massive amount of documents collected by a western

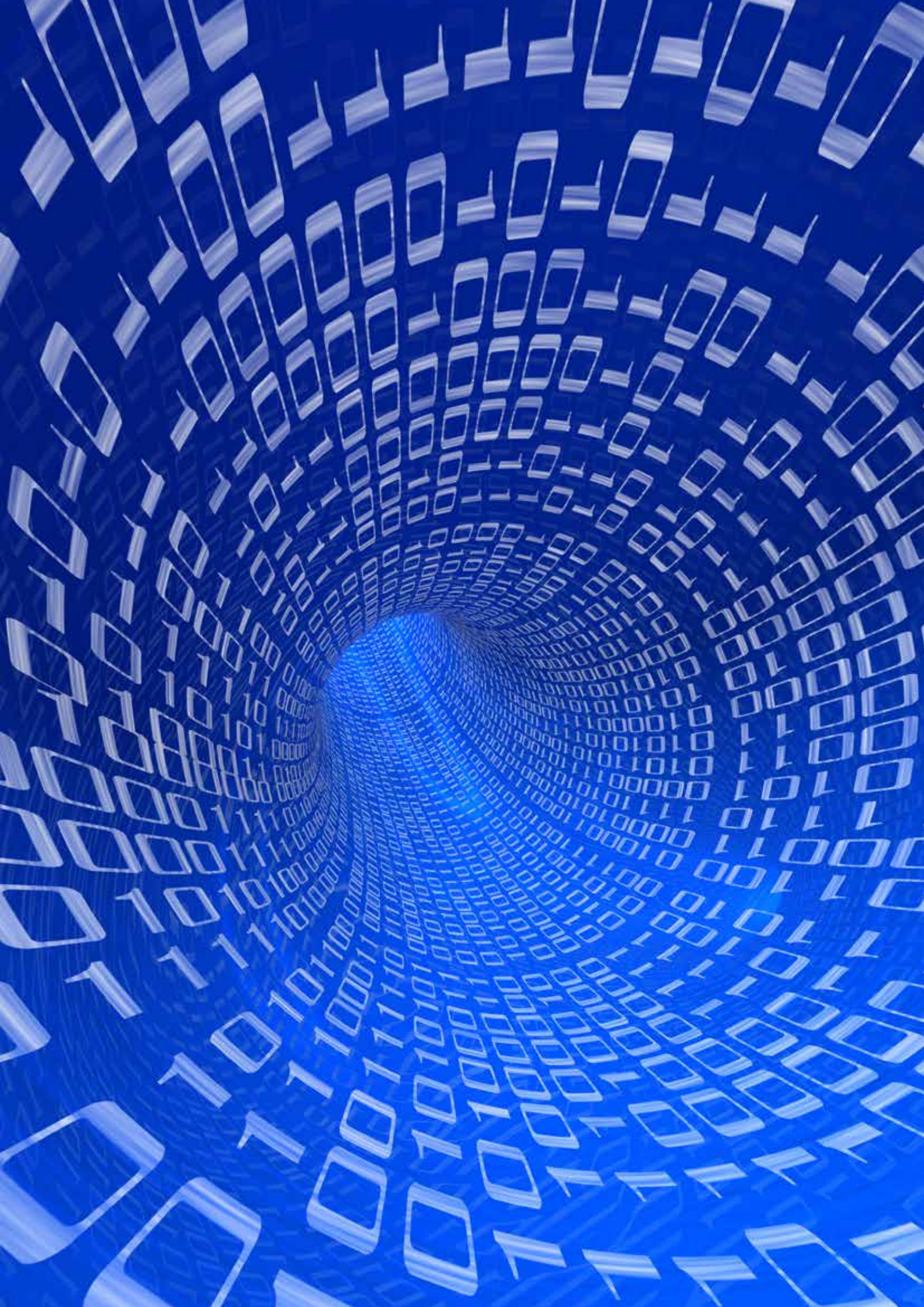
industrial country. This started even the bigger discussion what and who is following the network traffic and that even individual persons were not safe. Examples of high executive phones tapped came out daily. Already earlier, the bug hunting programs were turned upside down. White hat men (good and respectful researchers) could not concentrate anymore finding vulnerabilities or weaknesses from programs and systems. Opposite forces seemed to have more and more resources. Black hat men could offer a network shop to order a full blown DOS attack. A customer needs to just tick how many computers and type of an attack.

The NIS directive as well as the European cybersecurity strategies targets strongly cooperation and collaboration among relevant actors in cybersecurity. In the EU cybersecurity strategy, there is emphasis on decentralized prevention and response to cyber incidents and attacks. Coordination and information sharing are key elements of this approach, targeting a coordinated interaction between national, EU and international NIS authorities, law enforcements, defense authorities, as well as industry and academia. I think this is also one reason why Cyber Trust program has raised a lot of international interest and direct requests for collaboration. As a downside reflecting the real cyber world where we were living when the program has was originally established, we were contacted for international collaboration proposals even before the program was publicly announced. So definitely there are no secrets anymore in the internet world.

In Finland, we have a healthy situation, given that it is natural to have real co-operation with industrial and academic partners. One of the cornerstones settled already on preparation phase of the Cyber Trust program was the demand that more than one industrial partner was required for all business cases to be accepted to be part of the program. This was a challenging goal because traditionally security, and especially cyber security, practices are not handled by a company itself and not shared with others.

DIMECC CyberTrust was a success in many ways. It pushed the state-of-the-art of cyber security in many areas; it showed that successful collaboration can be achieved even in the cyber security area with small and large enterprises together with research organizations. The starting of deep NSF collaboration provides a good starting point for larger international collaboration; after all, Cyber Trust and Security is a global thing. The battle will continue.

Prof. Juha Röning
Academic Coordinator



Impact

There is a great potential in Finland to be the leading country in cyber security. Finland has the cleanest computers in the world. Finland has also decent legislation that obligates critical partners to implement security, but at the same time, the legislation mostly allows cyber security research. Finland enjoys a good position and strong expertise in a number of relevant areas, such as boundary defense, anti-malware, filtering of unwanted content, intrusion detection, and security testing. There are also many consulting and service companies providing security assessment, penetration testing, auditing, and training. This is a solid foundation for moving forward to international growth of business for Finnish industry and recognition for Finnish Universities, in particular, through collaboration in the Cyber Trust program.

We all need to be aware, and have a correct understanding of security incidents, network traffic and other important aspects that affect security. Therefore, we need situation awareness. For protection, we need security technologies, but we must not forget human aspects and managing security correctly, either. For that, we need security management. As a result, we will have resilient systems, services and infrastructures that are able to resist and recover from disturbances caused by the surrounding hostile environment. In the Cyber Trust program, the new design for security with novel and effective tools were created. The result is a sophisticated security policy for stakeholders.

Proactive – design for security. The program created a new proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries.

Self-healing – utilizing the toolbox. The program developed novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing.

Changing the mindset. The program enabled seamless cyber security integration into every-day life. By efficiently utilizing tools and methods provided through this program, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public awareness and understanding will move towards accepting cyber security as a natural element of a connected world.

Finland has an excellent research infrastructure supporting cyber security research and collaboration, including an extensive number of cyber security laboratories. These laboratories allow researching and experimenting cyber security threats and infrastructures without restrictions of the public Internet. Finland enhances automated and other more efficient forms of cooperation towards cyber security in the operational practice of Internet Service Provider (ISP), corporate and other networks. The research by the Cyber Trust program created methods and tools for fast, accurate, robust and privacy preserving forms of cooperation among the networked entities towards the goals for better cyber security and the capability of effectively responding to threats, even on the level of national security. Proof of concepts and demonstrations offered global visibility and helped to improve partners' businesses. Ground-breaking research together with industrial partners led to breakthroughs and over 100 high quality publications.

Finland also created Cyber Security Strategy that is seen as an example at the European Union level. Based on the strategy, The National Cyber Security Centre Finland (NCSC-FI), was established together with National Science Foundation (NSF).

Security and Software Engineering Research Site

Establishment of the Security and Software Engineering Research Site of Oulu was one aim of the Cyber Trust. The site is planned to be a part of Software Engineering Research Centre (S2ERC, https://www.serc.net) that is one of the National Science Foundation Industry/University Cooperative Research Centers (I/UCRC) operating since 2010 in US. The mission of S2ERC is to conduct a program of applied and basic research on software security, system security and software

technology problems of interest to its members. The goal of this research is to enable security and software technology gains within member organizations. S2ERC consists of thirteen participating universities and over twenty industrial and government affiliates in US. Security and Software Engineering Research Site of Oulu consists of three Finnish universities (University of Oulu, Tampere University of Technology, and University of Turku) and five industrial affiliates.

Security and Software Engineering Research Site of Oulu (later on, Oulu site) is for all Finnish universities and research institutes. It will physically be based on the University of Oulu. It's funding is based on the investment and project funding. An industrial partner that is interested in to join to the S2ERC activities sings a commitment letter for the project fee. An industrial partner also signs an Industrial Membership Agreement with the S2ERC. Oulu site sings an Academic Agreement with the academic partners of S2ERC. Finnish Universities sign an agreement with the Oulu site.

New project proposal snapshots are submitted to the Industrial Advisory Board (IAB) that consists of industrial and government affiliates. IAB approves/disapproves projects in the closed IAB meetings twice a year and endorses approved projects to the NSF and TEKES. Approved proposals are enlarged to new project proposals and submitted to TEKES or/and NSF by a Principal Investigator (PI) of the research site and project manager. A typical project consists of a research party and an industrial party. Parties can be either Finnish or a US party. Multiple parties are possible as well.

The operation of the Oulu Site will consist mainly of cooperative projects funded by participating companies, Tekes, and University of Oulu, Tampere University of Technology, and University of Turku. The approval of the IAB will be a precondition of Tekes' financial decision. The aim of public research networked with companies is to achieve competence and results that can be used as a springboard for the companies' own research and development projects. Additionally, the international site at Oulu will be working in close collaboration with DIMECC Ltd.

Principal Investigator's (PI's) and Researchers at the Ball State University (BSU), Virginia Tech, and Georgetown sites will jointly work on projects, conduct exchange visits, communicate via web-conferencing, and will begin planning future funding collaborations. The new international site will allow for training opportunities for U.S.-based S2ERC Graduate Students to get international research experience. With the addition of Oulu site, students as well as faculty at the BSU, Virginia Tech, and Georgetown sites will have the opportunity to incorporate an international focus into their professional experience. This new partnership will also allow for the Industry Advisory Board members to build personal ties with the new companies that are joining the S2ERC as industry members. The Oulu site and affiliates of the Oulu site will all abide by I/UCRC principles.

Cyber Security Ecosystem

Stakeholders in Finland can become prime drivers of a global Cyber Security ecosystem. To strengthen the operation of an international research site of the S2ERC in Finland, DIMECC will provide tactical support to the Oulu site. DIMECC is devoted to increasing, e.g., the pace of development of Finnish Internet Economy Competencies to enable global business opportunities. To accomplish this, DIMECC has brought together projects and organizations (academic and commercial) to foster productive collaboration and supports innovation with common frameworks and resources.

S2ERC's IAB members will obtain access to a wider and deeper array of research projects, gain a greater ability to tap into technical expertise of new faculty, access potentially new funding sources through direct interactions with DIMECC, and have an opportunity to collaborate with international industry members and students. The addition of an international Oulu site within Finland will allow researchers, faculty, and students within BSU, Georgetown, and Virginia Tech access to a broader base of knowledge and will enhance the intellectual property that results through S2ERC research.

Secure Services

Data of critical services is currently migrating to the cloud. Software Defined Data Centers (SDDC) will become viable in the near future as numerous new services will emerge into the cloud for industry, government and citizens. Big data will be used for creating new services for end users, and therefore, the partnerships between cloud service providers and security solution providers will become more common.

CyberTrust program studied state-of-the-art security technologies and methods for cloud applications and services. The virtualisation of security measurements and security focused cloud service design aims at taking a step further towards cyber security as a service (CSaaS). By utilizing validated and vendor neutral security artefacts from security concept and component development, developers can piggyback solutions in the design of secure application services in a more scalable manner.

Different services and products are increasingly reliant on IT, both directly, e.g., online banking and entertainment, and indirectly, for example, health services and air traffic control. These services and products process or contain information that is sensitive in terms of information security, privacy or both.

The ultimate goal is to provide a secure and cost efficient cloud security model where privacy, identity and resiliency issues are considered. The purpose is to utilize static security ensuring protection against known threats and also enable dynamic security for bringing adaptive mechanisms to provide added resiliency against yet unknown threats. This objective is achieved by analysing

potential security threats, develop solutions for effective resiliency for complete Cloud service systems and develop solutions for rapid recovery of cyber-attack situation.

The trade-offs between security, privacy, convenience and cost for end users were analysed. Also situational awareness understanding, analysis technologies, and visualization means were developed to achieve the required level of understanding from the current security status of a given operational environment. New methods and technologies for identity management, access control and management were created.

Proof of Concept for Secure and Resilient Cloud Based Services

The main objective was to enhance security and reliability of application production services so that customers can be confident to have their business critical applications to be hosted and managed by IT service providers. This requires correct and timely situation awareness information for the various stakeholders and laboratory environment to test and simulate the solutions.

New kinds of cloud services that are produced to end users via a complex business ecosystem will emerge in the future. Consequently, it is an extreme challenge to protect the private data of individuals in these complex ecosystems with various service interdependencies. For instance, data with varying protection requirements may be composed in one service, which in turn violates requirements set in the data origin. This will require new kind of features for cloud services such as Business Support System (BSS).

Due to this trend of rapid increase in usage of cloud services in all sectors, comprehensive business operations management as well as novel security techniques, and management of security in cloud service environment are needed. The novel techniques include application continuity and availability management, governance model management, security policy management, identity and access management, and situational awareness, including forensic.

The outcomes of the Cybert Trust program were trusted and secure service frameworks, and technologies, processes and component implementations to support both the public sector and private companies with business critical applications. Moreover, a generic model and practices for secured application management – applicable in public and private sector organizations in Finland – were created.

Cyber Trust program developed a comprehensive security model for all types of cloud based services to ensure confidentiality, integrity and end-users' privacy, even in complex and interdependent cloud

services. The purpose is that the security solution for the cloud service environment is a service itself. Various cloud service scenarios for industry, government and private citizens were analyzed from the cyber security viewpoint. Common security related nominators as well as individual service case related security requirements were analyzed.

The current practices and utilization of all needed components for secure and resilient cloud services were analyzed together with potential security threats relevant for cloud services. Special attention was payed to privacy and data protection, i.e., how to protect user and users' data in the processing phase (not only in storage).

Research efforts combined with cross-company expertise provided a fertile ground for new security enhancing approaches, innovations and breakthroughs in providing trustworthy ICT and situation-awareness services. Moreover, the program closely collaborated with the SAICS project (Situation Awareness in Information and Cyber Security) in order to share information with other companies and research parties working in the field. SAICS collaboration made it possible to find customers for the developed situation-awareness solutions from the industry.

There is a big and growing market, especially for healthcare, public sector and financial institutions, and a great demand for secured "Internet-able" critical infrastructure ICT services. Sufficient security is required in service provision, and each vertical has dedicated security requirements and provision practices. Moreover, and not depending on the vertical domain, the security position of the target systems and running applications must be communicated to the relevant stakeholders with relevant accuracy.

Common Flexible Certificates

Part of the work of this research theme was to create common certificates as a guideline for the commercial projects so that the platform and services fulfill the requirements and are also scalable. The major difference compared to traditional practices is that guidelines are agile and transparent. Guidelines are thus flexible but they fulfill the criteria. Also ITIL standard evaluation and analysis on security perspective was done.

There was a strong need to do research around common high level security standards. KATAKRI 2015, ISO 27001, and VAHTI 2 were chosen for research program. KATAKRI is the Finnish authorities' auditing tool, which authority can use in assessing the target organization's ability to protect classified information. KATAKRI can be used as an auditing tool when assessing a company's security

arrangements in the facility security clearance and in evaluations of the security of the authorities' information systems. It can also be used to help companies, organisations and the authorities in other security work and in development of it. VAHTI, the Government Information Security Management Board, provides information security instructions that are one of the most comprehensive set of information security instructions in the world.

New guidelines were issued and new certificates were implemented. Companies participating in this research theme made experiments on access management and user rights in cloud service environment. Security analysis and evaluation on KATAKRI 3 cloud environment were made. KATAKRI 3 level data center is the strongest certification level currently being certified. Security and quality standards also worked well as a platform for system and best practice development.

Evaluating the business model, operations and security controls toward these standard´s requirements were in the central part of the whole research. Netox for example, achieved the goals and finished their new head quarter construction, which gave the company the possibility to certificate the whole business against the KATAKRI and VAHTI standards as well.

Proof of concept trials were made on new secure features on cloud based IoT services. Some of them were applied to production use and are currently tested in actual services. Proof of concept design and implementation of IoT Cloud Service was implemented so that these can safely exploit off-the-shelf legacy alarm systems. The first proof-of-concept implementation was installed and experimented in the laboratory hosted by MPY.

BSS System

One focus of Softera was to study BSS system associated with the use of mobile use cases mapping. Softera did experiment with web based services, which enables transactions for third-party devices and services. BSS system was able to generate customer contracts. Work orders were made, and after the installation, the system started charging automatically. Softera conducted NFC payment analysis and proof of concept application: BSS integration into the payment terminal that enables nearby NFC payment.

Softera started SIEM software evaluation and testing (e.g., Alienvault Ossim). SIEM software would be possible at present to expand the use of IDS software (Intrusion Detection System).

In the first stage, the testing was done confidentially through a VPN tunnel between VTT premises and target system. Therefore, a

remote connection to a computer with required test tools within the target system perimeter is needed. The tester's computer must contain tools and virtual OS's installed by the testers and also remote desktop and file transfer services are required.

Customer account for using Softera services is needed in the second stage. It is assumed that the customer account will enable the testers to make an encrypted connection to the target system in order to enable confidentiality of the testing. It is also assumed that the customer account will enable the testers to install necessary test tools within the system, operate the test tools and transfer file between VTT premises and the test system.

Privacy of Digital Personal Identities

Digital personal identity defines a person in the digital world, in the context of an online service or a software application, and represents the person in a digital product or service. People increasingly create multiple digital personal identities for the digital services and products they are using. A growing concern among people is the privacy and security of these digital identities against digital wrongdoers, ranging from identity theft for financial benefit to online bullying or stalking, to tracking the digital and physical behavior of people.

In this business case, F-Secures aim was at essential improvements in understanding of the notion of privacy in the context of digital personal identities. F-Secure also planned to develop and validate solutions to enhance the capabilities for individuals and business users to access and use their preferred digital products and services in a trustworthy way, and ensure that their personal information stays private. As we are moving towards a more privacy-conscious era in online services, service providers who can communicate to their prospective users that their services will handle the users' data in privacy, will have competitive advantage over less-private competitors. The studies will be extended to the area of public safety and use cases in governmental / state organizations with their special requirements and priorities.

Activities around credentials management software included analysis of security-related functionality of the product and studies of actual customer needs and preferences and ways of communicating the product features to the customers. The primary collaborators were Aalto University, University of Jyväskylä, and Tampere University of Technology.

Security in Cloud Services

The research by VTT enabled security-by-design approach in cloud service platform development and supported planning of secure service provision. There is an increasing demand for cloud services. Companies are moving from dedicated server rooms to IaaS and private and public cloud services, for flexibility and economic reasons. Resiliency and security are expected of these services, often running business-critical systems and managing data with confidentiality requirements. Beside business criticality, the tightening governmental regulation and globally harshening security environment are posing new security requirements for these services. Jointly with the companies, VTT developed approaches to answer this call, to enable homemade data-centre services that are globally competitive and contending for best ROI in dedicated sectors (such as storage and management of personal private data, health data and classified data).

For the construction of novel cloud services, various security and safety aspects were studied and analysed, attributing to effective security controls, measurable system situation, and well-managed security of the service, and targeting to known security, with case-specific emphasis on the resiliency and security aspects set by the anticipated customers (e.g., via security regulations of the business vertical, or standards commonly applied in the business domain). The research covered cybersecurity risk analysis, information and network security measurement and security indicators, security and safety standards, novel authentication methods, and practical precautions and effective security controls in connected systems managing fleets of mobile and IoT devices.

Securing Platforms and Networks

The research theme investigates selected technologies and engineering processes that have the most potential for mitigating the inevitable vulnerabilities of software platforms. Security and reliability of modern distributed information systems depends critically on both mobile and cloud computing platforms and on the communication networks that connects them. Both the computing platforms and network are highly complex and based on open architectures. In such systems, the presence of malicious users, code and network traffic is almost guaranteed. It is therefore necessary to harden the platforms against attacks and to create a small trusted computing base on which secure applications can be built. Similarly, the communication networks need to be designed to be resilient under continuous attacks and to provide safe, isolated environments for critical functions and applications.

During the project, trusted and data secure service frameworks, technologies, processes and implementation were created to support public sector and private companies with business critical applications. The goal is to build up a generic model and practices for secured application management that can be utilized in public and private sector organizations in Finland.

The research theme investigated selected technologies and engineering processes that have the most potential for mitigating the inevitable vulnerabilities of software platforms. The focus areas were applications of secure hardware, hardware-supported software isolation and virtualization, and the standards and processes, such as

rigorous security testing, which help ensure the resilience of critical system components.

Since the connectivity in modern highly distributed information systems is typically provided by wired and wireless network operators, the research focused on new IP networking technologies, especially software defined networking (SDN), and the resilience of operator and datacenter networks built on these technologies. The end-to-end security and resilience of communication is typically part of the service design and implemented on the platform or application level. Business-critical applications must take responsibility for end-to-end cryptographic protection and security policy enforcement, and they must be built to withstand disruption of the underlying communication channels.

Situation awareness is important for a large number of organizations but is not among their core business activities. Thus, cyber security visualization, situation awareness and the related training require business models to enable service providers to provide sensitive real-time situational information (possibly across organizational borders) to the client organizations. Some of the situational information could be directed to public bodies.

The focus areas were applications of secure hardware, hardware-supported software isolation and virtualization, and the standards and processes, such as rigorous security testing, which help ensure the resilience of critical system components. The connectivity in modern highly distributed information systems is typically provided by wired and wireless network operators. Computer network architectures are currently undergoing the biggest change in decades: new networks are built using software-defined networking (SDN) technologies and patterns, such as OpenFlow and network virtualization. In this respect, the research focused on new IP networking technologies, such as SDN, and the resilience of operator and datacenter networks built on these technologies. The end-to-end security and resilience of communication is typically part of the service design and implemented on the platform or application level. Business-critical applications must take responsibility for end-to-end cryptographic protection and security policy enforcement, and they must be built to withstand disruption of the underlying communication channels.

Security Technologies and Secure Management for Future Networks

There is a fast on-going change in the technical architectures and topologies of the Internet: in the near future, network architectures may be based on Software Defined Networking (SDN) and Network

Functions Virtualization (NFV). These concepts create new virtual network elements and interfaces, which affect the logic of the network operation and traffic management and the entire system architecture.

In data centers, new network technologies like wide-area networks and cellular mobile networks enable the flexible and elastic on-demand provisioning of secure network services. This evolution will lead to a significant change of network architectures, protocols and management. It will also create new business possibilities such as multi-tenant core-network models, as well as other unforeseen opportunities, especially in the security area.

Cyber Trust program developed a technical SDN environment that act as a testbed for integrating the NFV and SDN architectures and for the investigation of business opportunities, and well as for analysis of the related cyber threats, using existing Realistic Global Cybersecurity Environment (RGCE) as one source. Also the new technical security solutions were developed, and these were improved and built based on the existing network technology. The goal was to both solve identified security issues in SDN and to exploit SDN technology for enabling new security services and business.

As sharing of mobile network resources becomes more common – this is also encouraged by the EU – it will open up new revenue opportunities for classical mobile operators to leverage their network infrastructure and services. Thus, they will exploit the new SDN and NFV technologies. The new network topologies and a different kind of NFV architectures will not only bring new flexibility, but also threats, such as spreading of attacks through the network. Those attacks need to be prevented and detected. This highlights the need for isolation mechanisms and for the effective deployment and chaining of security-related services.

Future SDN

New networks will be built using SDN technologies where routing and network topology are defined at a software-based controller rather than at the routers, switches and physical links. The controller will be the one of the key components in the SDN.

Puikkari SDN platform provided by JAMK is a proof of concept implementation of a customer portal for a modern next generation computer network using SDN and Network Function Virtualization (NFV) technologies. The platform enables the network to provide different kinds of services for the network users and administrators. The service could be for example a firewall that is placed in front of a network customer or a network traffic monitoring tool for network administrator that is used to debug network problems.

The platform was developed to handle a network of a small imaginary ISP in a virtual test internet setup. The project focused on researching what kind of business opportunities these new network technologies could have and how they affect the network security. Although the main target for the platform in the development phase was a small ISP, this platform could also be used in a network of any size, for example, campus networks or even small home networks.

JAMK created virtualized Cyber Trust SDN testbed in the Realistic Global Cyber Environment (RGCE). This environment has been available for the research consortium. This testbed was developed to serve as a platform to test multiple different scenarios in a SDN network. The environment includes a controller network where any SDN controller can be deployed with ease. In the data plane, SDN switches are virtualized Open vSwitches and routers are Vyos virtual machines. The network BGP (Border Gateway Protocol) peers to RGCE to imitate a real Internet connection as much as possible.

Puikkari and RGCE testbed has been used by JAMK students to learn SDN. Both test environments has been used by thesis workers to learn SDN, create proof of concepts and test the solution for their thesis. Both test environments can be seen as valuable assets for further research.

For Elisa, the background for this work was the upcoming change in the technical architectures and topologies of the Internet. A great part of the work concentrated on business cases and developing related technical architectures. Together with JAMK and University of Oulu, Elisa set up test systems and validated the use cases, which concentrated on Software Defined WAN (SD-WAN) technologies and corporate network CPE systems. Furthermore, Elisa took part in business model development with Ericsson and University of Oulu.

Joint testing with JAMK provided us good technical and business insights into corporate customer CPE and FW management. New know-how on SD-WAN security was gained and how to manage large global WAN networks in the 2020s.

Elisa also tested with JAMK a number of SDN based CPE cyber security scenarios, which will guide further product development and productization. Main focus of the collaboration was to investigate how HPE SDN VAN Controller, along with the SDN applications such as HPE Network Protector, can be used to filter malicious DNS traffic in different parts of the network. The aim was to find out how the system needs to be configured in three different network topology cases, each having the switch located **either** inside the ISPs core network, at the edge of the network or inside the customer premises, or where ? The or part in either –or structure seems to be missing here.

In terms of SD-WAN products and services, Cyber Trust offered Elisa a context to study next generation WAN services and how cyber security technologies will be and should be implemented there.

Part of the research of VTT involved the advancement of the SDN-security. The tasks included setting up and experiment with the latest SDN platform technologies, including their management (technology basing on OpenStack). The technology development was highly experimental. The goal of this work was to gain more know-how for securing Network Functions Virtualization (NFV) elements in OpenStack environment.

The SDN security work with a major company produced a new environment for experimentation, with insights into its capabilities and weaknesses, and future improvements. The technology is still nascent, and VTT was able to provide some stepping-stones eventually leading to its future adoption.

The research group of University of Jyväskylä analyzed the security vulnerabilities of the SDN networks. The main outcome was the method they developed to analyze SDN network traffic in order to find out anomalies (attacks) of the network traffic. Researchers concentrated on timely detection of intentional co-residence attempts in cloud environments that utilize software defined networking. **As SDN** enables global visibility of the network state **which** allows the cloud provider to monitor and extract necessary information from each flow in every virtual network in online mode. Here, the main clause after the relative clause seems to be missing after the As clause at the onset of the sentence.

Researchers analyzed the extracted statistics on different levels in order to find anomalous patterns. The detection results obtained showed that the co-residence verification attack can be detected with the methods that are usually employed for botnet analysis. SDN security research was done by other research organisations as well.

5G Security

It was important to gain more understanding on how novel technologies will mold new networks, especially 5G. 5G networks are not only faster, but they provide a backbone for many new services, such as IoT and the Industrial Internet. Those services will provide connectivity for everything from autonomous cars to remote health monitoring through body-attached sensors, smart logistics through item tracking to remote diagnostic. Most services will be integrated with cloud computing and novel concepts, which will require smooth

and transparent communications between user devices, data centers and operator networks.

Together with Ericsson, Oulu University and Elisa made research, the results of which were disseminated, e.g., in NSS2017 conference and in a book Comprehensive Guide to 5G Security by Wiley.

The book provides a reference material to a comprehensive study of 5G security. It is the first comprehensive guide to the design and implementation of security in 5G wireless networks and devices. It offers an insight into the current and future threats to mobile networks and mechanisms to protect them. It covers the critical lifecycle functions and stages of 5G security, and how to build an effective security architecture for 5G based mobile networks. The book offers security considerations for all relative stakeholders of mobile networks. It covers critical lifecycle functions and stages of 5G security and how to build an effective security architecture for 5G based mobile networks.

Cyber Trust -program and its results will guide also Finnish cyber security research. One important aspect is here the wide scope and holistic view on this topic. Another aspect is the relevance of cyber security in 5G, and how the SDN/NFV technologies will affect this development.

Petri Ahokangas, Sara Moqaddamerad (University of Oulu), **Marja Matinmikko** (VTT), **Alhussein Abouzed** (Rensselaer Polytechnic Institute), **Irina Atkova, Julius Francis Gomes, Marika Iivari** (University of Oulu): ***Future micro operators' business models in 5G . The Business and Management Review. Vo. 7, number 5., 2016.*** http://cybertrust.fi/publication/future-micro-operators-business-models-in-5g/

Secure Wireless Technology Platform

There are approximately 180 million Enterprise BYOD (Bring Your Own Device) devices globally and the number is expected to increase to 390 million by 2015. The total BYOD and Enterprise Mobility market is expected to reach $181.39 Billion by 2017 with a CAGR of 15.7%.

Commercial technology is adopted in systems where closed solutions were earlier used. In US, FirstNet has been allocated a nationwide spectrum license where they will provide a 3GPP Long-Term Evolution (LTE) technology based network that will provide the first broadband network dedicated to public safety. Similar development is also taking place many countries in Europe, Middle East and Asia, UK Home Office being the prime example. Security plays an increasingly important role in all these markets, on top of their other specific requirements.

Device manufacturers have received requests from corporate customers on adding further privacy and security features to their offering. The requests for privacy and security stem from the US and Asia dominance in smartphone operating systems and related cloud based service businesses, which have raised vocal concerns about the security, privacy and trustworthiness of current (mobile) digital environment.

Certification Requirements

How a company can convince the customer that the security features offered are really there and working flawlessly? Product certification is one way to show that a product does what it promises. Bittium studied national security certification requirements for restricted (ST-IV) and confidential (ST-III) information handling. Advanced authentication means were defined and demonstrated to meet the requirements.

The research done in the various DIMECC projects has been also taken into account in standardization work in different standard organisations. These are 3GPP (the 3rd generation partnership project), IETF (Internet Engineering Task Force) and ETSI (European Telecommunications Standards Institute). The 3rd Generation Partnership Project unites seven telecommunications standard development organizations. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and Internet technologies.

Products are today more and more complex, typically including tens, even hundreds open source components. No software can be tested completely and security vulnerabilities can be found in a certain software component, even years after its release. Therefore, it is essential that possible software vulnerabilities and exploitations are checked regularly. Process improvement and tool development were done on this area during the CyberTrust program. The developed process was demonstrated successfully in Bittium and it has been taken in to daily use.

Public safety and security areas have been until today very different from commercial solutions and devices. The situation is changing and commercial consumer based technology will be adapted in the future also in public safety. This changes the business model for

the ecosystem. University of Oulu Business School has analyzed the current and new business environment.

Improving Security in Wireless Product

During the program, the special *Cyber Trust Handbook for Improving Security in Wireless Product* was created by Bittium, University of Turku, University of Oulu, VTT, and Capricode. The focus of the book is the improvement of the security of wireless product during the product's life cycle from development to the product's end of life.

Integrity Protection

Integrity protection means how the software's integrity can be maintained and possible changes by malware can be detected without a delay. Integrity protection requires hardware trust anchor and mechanisms to protect both boot chain and user space components. Integrity protection ensures that the platform software's integrity is kept. However, in many products, software applications can be downloaded and at the same time devices can be mobile. Cybert Trust program presents improved methods to secure that applications cannot use the device resources in a malicious way.

Integrity protection mechanisms are needed to prevent unauthorized modifications to system software and applications. Sometimes, this can even be a safety issue if unauthorized modification is causing danger, like radio interface exceeding permitted Specific Absorption Rate (SAR) values. Integrity protection is also a corner stone of security and it is needed to guarantee that all protection mechanisms designed will operate as expected.

.Whether there are complex access control or Digital Rights Management (DRM) mechanisms to protect content, those all will fail if attackers are able to manipulate components that are supposed to be trusted. Therefore, trust requires that integrity of components handling confidential information should be verified before these components are used.

Integration protection mechanisms are developed to support chained verifications where each component in the boot chain is verifying the next component before passing control to it. For example, the first stage bootloader should verify the second stage bootloader and the second stage bootloader should verify kernel image.

Verification is typically done by calculating a cryptographic hash of the component and then verifying the result using the signature of the verified image. This verification chain requires that there is a

trusted starting point. The system must have security hardware like Trusted Platform Module (TPM) or ARM TrustZone, which allows binding of device identity and the use of device specific signing keys.

Integrity protection requires a mechanism to protect both components of the boot chain and users pace components. A hardware-based trust anchor is needed to establish root of trusts for measurement. Linux kernel provides many alternatives for integrity protection. Either file-based or block-based approach can be used. The software update mechanism should also be protected as it can be misused to install malware to the system. Remote attestation can be used to provide integrity proof of the system to remote verifier.

Fuzz Testing in Agile Test Automation

No design is perfect and less is the implementation. Therefore, testing is needed and fuzzy testing has turned out to be a very effective testing method. Cybert Trust program introduces methods to make fuzzy testing more effective and easier to use.

Fuzz testing (fuzzing) is a practical way of testing software for security vulnerabilities arising from processing external input and is usually included in secure development lifecycle models. In 2015, nearly all high-impact vulnerabilities with a Common Vulnerabilities and Exposures (CVE) entry were found with fuzzing. Fuzzing is clearly something that should be done when developing secure software, but applying it efficiently as a part of an agile process can be challenging.

Fuzzing can be integrated into agile software development and test automation, but there are difficulties. The main challenge is that fuzzing needs to continue to show value while requiring minimal effort.

The effectiveness of fuzzing depends on how well it is executed. This begins from

data flow based threat modelling, which should be continuously updated. Threat modelling should also take results from previous fuzzing into account. If new issues are found with fuzzing, the interface should be a candidate for increased fuzzing efforts. Even limited dumb fuzzing with manual instrumentation can find some low-hanging fruit, and thus should be done for all inputs of the system. The quality of third party components should also be considered.

To stay in use, fuzzing needs to be automated. Even then, the infrastructure will eventually stop finding new bugs. Up to a point, improving test case generation (better models or samples, adding new fuzzers) and instrumentation (use of new type of memory debugger, custom test harness) will continue to find new bugs. Many of these activities only require a small one-time cost, and are easily justified. Others require more significant efforts, including the use of experts.

Coverage guided fuzzing is a promising field, and can improve the quality of fuzz test campaigns. In addition, coverage provides insight into whether placing further effort into improving the test campaign would be useful.

A key question is the availability of the skills required to setup an effective fuzz test campaign. The Software Security Group is pivotal, but eventually testing will have to be done by developers with the proper tools and skills. Setting up ways of working to make fuzzing more effective is one way of doing this. This could be, e.g., standardized ways of building instrumented builds and ways of leveraging results from other activities, like automatically reusing API documentation as a model for fuzz tests.

The workflow used by fuzzing is somewhat different from traditional testing and this needs to be accounted for. Instead of being an activity that responds to the previous development increment, automated fuzzing is a background process that needs maintenance. Currently, this requires some expert knowledge, but better tools could also fill this gap.

Coverage-based methods are an efficient method of improving the test case corpus, thus improving test quality. Ideally, they would also make it possible to automatically direct fuzzing efforts into areas, which have recently changed in the code. This would also serve as evidence that the new functionality has been tested.

Pietikäinen, P., Kettunen, A., & Röning, J. (2016) Steps Towards Fuzz Testing in Agile Test Automation. *International Journal of Secure Software Engineering. 7, 1, 2016.*
http://cybertrust.fi/publication/steps-towards-fuzz-testing-in-agile-test-automation/

Product Security Incident Response Team

Product Security Incident Response Team describes how product software's vulnerabilities can be easily monitored. All organizations are connected to the outside world using computer networks. Companies and societies are depending on working communication networks. The security of the communication is more important today than never before. Several means are applied to improve the security. Computers have anti-virus and malware detection software. Firewalls protect companies' networks; all connections are passed through proxies which makes it easier to leverage organization level policies. Network traffic can be monitored with an intrusion detection system which alerts if suspicious traffic is detected. There are administrative tools that help information management personnel to check the status of computer software versions and automatically install security patches.

A new and even bigger challenge comes when different control systems, including critical infrastructure and autonomous machines, are connected to large scale networks which can be accessible from public internet and therefore being vulnerable to same kind of threats as computer networks. An industrial site can have hundreds, even thousands of different types of devices connected to industry network. Although accessing these devices is much harder than computers in a computer network, it is still possible. Same kind of administrative tasks are much harder to execute for industrial network than in a typical computer network which includes Windows machines and Linux servers, for example. Therefore, it is crucial that all the vendors follow good practices for building secure devices from the very beginning.

Cyber Trust program introduced one approach how the security of a product's software can be monitored during the product's life cycle. Product Security Incident Response Team (PSIRT) is an organization whose responsibility is to proactively scan new vulnerabilities related to the product software and react if those can be found. Vulnerability scanning is an important part of PSIR operation. A concrete example is presented how the vulnerability scanning can be organized.

There is not only one way to organize PSIRT activity but it depends on several issues. One thing is, however, common to all solutions. The organization has to define what PSIRT does. PSIRT operation costs may come from new tools and equipment and from personnel cost. No matter how small the operation is, someone still needs to do something and that needs money. However, the overall cost may be less than with the current operation but usually organization sees all new functions as an additional cost. Therefore, there has to be a clear mission statement what the new function – PSIRT – does and delivers.

Checking of software vulnerabilities is an important part of software development and maintenance. It is also a fundamental part of PSIRT operation. Vulnerability scanning is not a one shot activity but it has to be done on a regular basis because new vulnerabilities may be found at any time. At a development phase, it is important to check that a new software component, which is planned to be used, does not contain such vulnerabilities which prevent the use of the component in the product. In the case of an open source component, the initial vulnerability analysis may be done as part of open source governance when also open source licenses are checked. After that, the software components should be checked constantly.

For vulnerability scanning, the access to the vulnerability database is mandatory.

There are several public Common Vulnerability and Exposure (CVE) databases like http://cve.mitre.org, https://web.nvd.nist.gov/view/vuln/search, https://www.exploit-db.com/, https://www.circl.lu/services/cve-search/. There are also product specific databases as

WindRiver's https://www.windriver.com/security/cve/main.php and non-public commercial database as Risk Based Security's https://www.riskbasedsecurity.com/vulndb/.

Because security is everyone's concern, the basic CVE databases are public and common for all database providers. However, there are still differences how data is presented. For example, Mitre and NVC have a very close relation. Mitre feeds the CVE list to the U.S. National Vulnerability Database (NVD), which then builds upon the information included in CVE entries to provide enhanced information for each CVE Identifier such as fix information, severity scores, and impact ratings. NVD also provides advanced searching features such as by individual CVE ID; by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range, and impact.

Although public CVE databases can be accessed directly, it might expose critical information if the access is used to query information related for the product software. If the queries are monitored, then a listener can get the information about all the software components related to the product and then possible uncovered vulnerabilities which can be utilized on targeted attacks. A better approach is to setup and maintain a local CVE database from which the product specific CVE searches are done.

Product security is not something which is built into the product during the development and then forgotten. Especially today when the software is built from hundreds open source components, it is impossible to verify thoroughly all the components. Therefore, the vulnerabilities should be monitored constantly. That is an important function of Product Security Incident Response Team (PSIRT). There are no strict guidelines how the organization should organize PSIRT. That depends on the number of products, company size and many other things. Nevertheless, a solution for vulnerability scanning was introduced. The presented framework was developed in the Cyber Trust program and it has been successfully used in Bittium. However, not all open source projects report formally CVEs the security flaws found in the project. Many security errors are corrected and the track for that can be found only in the changelog or version control system's commit comments.

Mobile Device Management

Digitalization and cyber security trends will continue and form a basis also for the device management needs and evolution. Everything will be connected, all data is analyzed and cyber security awareness brings market growth possibilities for device management products. Product life cycle and window of opportunity for growth are all the time shorter and all markets are global.

In emergence of IoT, one important issue to consider is who will take the responsibility for IoT devices. In the case of company using IoT as part of their process (e.g. factory), the answer is quite obvious: the IT department, that manages also all other devices, takes responsibility over IoT as well. In a case where the IoT enables new business via digitalization, the business unit could take responsibility directly. Usually, this is done through utilizing a separate innovation department in the research and development organization or Operational Technology (OT) organization.

In the past, Information Technology (IT) and Operational Technology (OT) were seen as two distinct domains of a business. The former focused on all technologies that were necessary in order to manage the processing of information, whereas the latter supported the devices, sensors and software that were necessary for physical value creation and manufacturing processes. One of the factors that is reshaping IoT market is the convergence of Information Technology and Operational Technology which is basically a "must have" in order to scale to IoT vision device amounts and to keep security at proper level.

Convergence of networks – both industrial (OT) and enterprise (IT) -- are enabling applications such as video surveillance, smart meters, asset/package tracking, fleet management, digital health monitors and a host of other next-generation connected services.

Main items in future device management systems are related to scaling, customization, flexibility and integrations of the device management system. Main need and growth in device management business will be in IoT due to automation and cyber security needs in that field.

Cyber Security is one of main concerns and major roadblock for vast expansion in the amount of connected devices. Security and IoT evolution will need standardization, alliances, good co-operation capabilities and close integration between different technology providers.

Evolution in enterprise device management will divide into large enterprise EMM needs and small and medium enterprise basic MDM needs. Organization needs are also divided into basic security level needs and advanced security needs as for example in governmental organizations.

Contributors of this research theme: Bittium, Nokia, Ericsson, Elisa, Capricode, VTT, University of Turku, University of Oulu

Advanced Threats and Security Assurance

Most of the society's critical infrastructure and key processes in companies and organizations are controlled by computer systems, which makes such systems a natural target for attacks, often for the reasons of industrial espionage, damaging, or intelligence gathering by nation-state actors.

In digital public services, cyber-attacks threaten the privacy of clients' sensitive information, and can cause potentially fatal consequences if the data are altered or removed, e.g., in health care systems. In energy sector, failures in a control or monitoring system can lead to high financial losses and prevent operations of other dependent services, including safety-critical ones, and in the worst-case scenario, they can paralyze the whole critical infrastructure. Successful attacks on mobile networks will lead to similarly dire consequences.

Cyber Trust program studied key threats across societies and economies, designed effective methods and tools for detecting and countering threats. The program also validated these methods and tools via modern security assurance techniques and practical testing. Forensic analysis and incident response were used in security and privacy assurance of information systems and components, including

open source ones, and support of personnel in operating protections systems and dealing with security incidents. Program explored new approaches for detecting targeted attacks within the privacy framework set by local legislation, through collaboration between experts in handling security incidents and experts in network security.

Targeted attacks are attacks against specific companies or industry sectors and governments, often for the reasons of industrial espionage, damaging critical infrastructure (for instance, mobile networks and IT infrastructure of organizations), or intelligence gathering by nation-state actors.

Recently, customers have become very interested in this topic and the participating companies and institutions regard the topic of targeted attacks as a business critical area for their future security service offerings, and this project is targeted to improve significantly the expertise, detection, and mitigation effectiveness against targeted attacks.

Today, most detection approaches focus on general malware. Malware detection is often based on signatures, static analysis, and simple behavior-related rules. The program aimed at significant improvements in the capabilities of detecting, reacting to, and preventing targeted attacks, which typically have more complex attack patterns than conventional ones, including, for instance, sophisticated logic of attack escalation. Real attacks were analyzed and malicious objects used in those. Based on that improved understanding, one can construct "behavioral signatures" of attacks that can be used for their effective identification. Open interfaces to the analysis systems were provided and tools were created to aid in the incident response operations. This will also help organizations recover from intrusions faster and more effectively.

A number of Cyber Trust partners, including F-Secure, joined the recently established European Organization for Cybersecurity (ECSO), which was actively discussed within the program, and have already contributed to such ECSO efforts as the SRIA preparation for the Horizon 2020 Work Programme 2018-2020.

Collaboration with National Science Foundation Industry/ University Cooperative Research Center (I/UCRC)) was initiated through DIMECC Cyber Trust. As a result, the S2ERC site was established in Finland. The Security and Software Engineering Research Center (S2ERC) has been operating since 2010. The Finnish cyber security and software engineering research site is open for all Finnish universities and research institutes and it will physically be based on the University of Oulu. The number of Cyber Trust partnerships is expected to continue within S2ERC, for instance, between University of Turku and F-Secure.

Rapid Detection Service

F-Secure studied approaches and technologies for detecting advanced attacks on organizational systems and networks. This led to a foundation for Rapid Detection Service (RDS). The key partners were University of Turku and nSense.

This service is related to the threat Intelligence work. F-Secure regularly publishes threat reports and analysis of specific attacks, attacker techniques and tactics, which brought insights for developing RDS. In particular, that led to establishing a working relationship with ENISA (The close partners were Nokia, nSense, Ericsson). The research and exploration of techniques for collecting and pre-processing relevant data from endpoints and of methods for detecting attacks via the collected data contributed significantly to RDS success. F-Secure has now a great business opportunity for the service and the technology. The RDS pilot enabled University of Turku to work with F-Secure on data analysis approaches which was an important learning experience and helped us prepare better for various chal

The RDS-related collaboration with the researchers of University of Turku brought valuable data sets for attack detection analytics. The aim was to introspect live events coming from various programs running on top of an operating system. The introspection targeted profiling and then attaching normal features to either programs or program users. The aim of the work was to develop machine learning based advanced methods to find signs of unnatural, malicious behaviour. So far, researchers have collected for six months operative RDS data, and the analysis of it. They are developing advanced recognition methods. The continuous analysis of a stream of program events is a completely novel approach for enhancing software security. Researchers have about 1 Terabyte of RDS data collected and its analysis & malicious activity recognition method development is in progress.

New Open Source Sandboxing and Fuzz Testing Environment

Research for the new sandboxing environment and technology supported F-Secures's Incident Response and Threat Intelligence work. The task was to extract behavioral features for identifying malicious and unwanted files and web resources. This has led to further collaboration plans with University of Turku in the framework of S2ERC. Major parts of the Sandboxed Execution Environment (SEE) were open-sourced and access to them was provided for Cyber Trust partners. There are clear opportunities for the technology in the Corporate Security business, and there are plans to continue collaboration with University of Turku in that domain within S2ERC. Open sourcing of F-Secure's sandboxing technologies led to

interesting plans of academic research both within and outside of Cyber Trust. Access to F-Secure's threat intelligence backends enabled several program partners to validate results of their research work.

https://github.com/F-Secure/see

Research, development, and adoption of fuzz testing techniques were done in collaboration with Oulu University Secure Programming Group(OUSPG). OUSPG's work on cloud-based coverage-aided fuzz testing is state-of-the-art worldwide. It compares to tools used widely in the industry, such as afl, but uses more advanced techniques for mutation. This reduces test performance somewhat, but the researchers have shown that the techniques used are able to find problems other tools are not able to easily find. Furthermore, researchers can scale the approach in the cloud. Purpose of fuzzing is to automatically generate lots of test input and to make code crash and increase code coverage. The collaboration on fuzzing resulted in an open-source project (libfuzzerfication) and consistent efforts for applying fuzz testing in F-Secure's R&D as a part of the standard software development process. LibFuzzer is a library for in-process, coverage-guided evolutionary fuzzing of other libraries.

https://github.com/ouspg/libfuzzerfication

Pekka Pietikäinen, Atte Kettunen, Juha Röhning (University of Oulu): *Steps Towards Fuzz Testing in Agile Test Automation. International Journal of Secure Software Engineering. 7, 1, 2016.*.

http://cybertrust.fi/publication/steps-towards-fuzz-testing-in-agile-test-automation/

Credentials Management Software (F-Secure KEY)

F-Secure KEY is a credentials management software. During the program, security-related functionality of the product was analyzed and studies of actual customer needs and preferences and ways of communicating the product features to the customers were made. The primary researchers were from Aalto University, University of Jyväskylä, and Tampere University of Technology. They contributed on the both security and user experience sides, supporting in addressing technical challenges, in understanding user problems and preferences, and in identifying ways to position F-Secure KEY for direct users and telecommunication operator partners.

F-Secure is now exploring how to turn the technology into a corporate offering and how to sell it via our network of ISP and mobile operators. F-Secure is also shaping business plans for services based on threat intelligence and sandboxing and observing healthy demand from security-conscious corporate customers.

Detection of Fake Accounts at the Social Media Sites

SOMEA research group at the University of Jyväskylä was primed to inform methods and software for social media monitoring and analysis. The group was interested in finding new collaboration possibilities, and supporting the existing research activities regarding application of social media analysis methods to detection of fake identities, and understanding the role of false identities at early stages of targeted attacks.

Over the past two decades, online social media resources have experienced a rapid growth. Now nearly 70% of adults in developed countries have social media accounts. Most online social media sites bypass the verification of new users' identity in favour of ease of access, thus opening a door for such fake identity-enabled activities as spamming, phishing, and trolling. Together with F-Secure and nSense, the research group performed repeated crawls of metadata of 200,000 newly registered users at social media site VK.com. The crawling lasted nearly one month, and the goal was to collect and analyze activity of these accounts over a large period of time, detect anomalies in their behavior (such as rapid growth of friend list), and analyze URLs presented at these accounts using API provided by F-Secure.

Aleksei Romanov, Alexander Semenov, Jari Veijalainen (University of Jyväskylä): R*evealing Fake Profiles in Social Networks by Longitudinal Data Analysis. Scitepress, 2017.*
http://cybertrust.fi/publication/revealing-fake-profiles-in-social-networks-by-longitudinal-data-analysis/

Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis, Jari Veijalainen (University of Jyväskylä): *Detection of Fake Profiles in Social Media – Literature Review. Scitepress, 2017.*
http://cybertrust.fi/publication/detection-of-fake-profiles-in-social-media-literature-review/

Research on Denial-of-Services Attack

A denial-of-service attack (DoS attack) is an attack where a machine or network resource is made unavailable by disrupting services of a host connected to the Internet. Security specialist Silke Holtmanns from Bell Labs Nokia and other researchers from her group have studied how hackers can conduct DoS attacks on 4G cellular devices around the world. Holtmanns, who has participated in the Finnish Cyber Trust-programme, presented the results of the research at the Black Hat conference in November 2016.

Holtmanns presented different DoS attacks that can affect any platform or device on mobile LTE (Long-Term Evolution) networks: mobile phones, tablets, and devices connected to the IoT. These attacks can disconnect mobile phone users from their network.

Although the new technique and new communication generation with 4G/LTE is believed to provide a better world, we still need to be awake. LTE with DIAMETER has a similar functionality as the earlier technique (SS7). The security researchers have provided clear results that we will face similar interconnection weaknesses with LTE/DIAMETER as SS7 if network do not take protection measures.

Ever since the public revelation of global surveillance and the exploits targeting the mobile communication backend, the general awareness of security and privacy in telecommunication industry has increased. Misusing the technical features of mobile core network technology – specifically the Signaling System 7 (SS7) – has disclosed numerous ways to locate, track and manipulate the routine cellular activities of cellphone users. In fact, the SMS-based key recovery mechanism is becoming vulnerable because of the SS7 vulnerabilities.

Many mobile network operators rush to upgrade their networks to 4G/LTE from 2G and 3G, not only to improve the service, but also the security. With relatively more security and privacy features, Diameter protocol – the successor of SS7 in Long Term Evolution (LTE) networks, are believed to guarantee more protection to the network itself and to the end-users. However, Diameter inherits many functionalities and traits of the SS7 network and attention need to be paid to proper security measures like filtering. Therefore, some attacks are also possible there, e.g., location tracking in LTE by abusing the Diameter-based interconnection.

Read the rest of Holtmanns's article here:
http://cybertrust.fi/publication/detach-me-not-dos-attacks-against-4g-cellular-users-worldwide-from-your-desk/

Security Protections for Mobile Networks

The US government was supported by Nokia on drafting security protections for mobile networks (Federal Communications Commission and the Department of Homeland Security). Nokia also supported the Nordic regulators on the evolution of mobile network security. Nokia had a further thesis, e.g., on machine learning, trusted NFV and related topics.

Nokia and Finland are seen as a worldwide leading trusted expertise center for advanced attacks and protections of mobile networks. This recognition has resulted in many customer requests and orders, which in turn bring capital also to Finland. With the help of Cyber Trust program, Nokia was able to pool the critical resources to have the leading edge in the area of advanced attacks. Nokia

shared this information freely between the partners, to enhance the Finnish expertise level. Specifically, Cyber Trust program has given Nokia the possibility of creating a demo testbed (with robotic arm, virtual reality control, and 5G connectivity) which will serve as a great demonstration platform for most of the work done in the program.

Cyber Security Standards in Power Grids

Jyväskylän energia focused on current cyber security standards in power grids (water, electricity and heat) and the security of automation systems. The research on threats in energy production was completed. Also security collaboration in the energy industry was conducted. Better understanding of the information security level of the electricity network was achieved. An information security analysis of SCADA system was done. Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations control and monitor industrial processes locally or at remote locations

In order to possibly purchase a Security Operations Center (SOC) service, Jyväskylän energia surveyed the existing services and service providers. Jyväskylän energia also surveyed the data protection audit providers in order to start preparing for the EU General Data Protection Regulation (GDPR). It replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

Jyväskylän energia and University of Jyväskylä analyzed cyber security management, situational awareness and resiliency. Pardco Group provided an environment for the research regarding honeypot utilization for analyzing cyber- attacks.

Otto Hrad, Simo Kemppainen (University of Jyväskylä): H*oneypot utilization for analyzing cyber attacks. ACM, 2016*.
http://cybertrust.fi/publication/honeypot-utilization-for-analyzing-cyber-attacks/

Diversification & Obfuscation

University of Turku applied large scale diversification statically to the different layers of operating systems, applied obfuscation and diversification to other well-known application areas (e.g., AJAX web applications and the SQL query language), applied diversification to operating systems of IoT devices (e.g., memory layout scuffling and binary symbol diversification), and studied the possibilities of applying diversification techniques to cloud-based systems (e.g., JavaScript and various API diversifications). Diversification and obfuscation

can be applied to binary files in large scale. Diversification could be applied successfully in various application areas, and diversification is extremely useful for securing the IoT devices which themselves are generally very poorly secure or completely non-secure; trusting on physical separation.

Honeypot, Sandbox & Monitoring

University of Turku committed surveys to establish fake entity proposals from scientific literature, malware's anti-honeypot and introspection methods, and current sandboxing implementations. Researchers executed development to implement a diversified honeypot which operates at the system call level and an experimental honeypot proxy framework for deceiving attackers with fabricated content. Finally, they conducted a survey of application-level sandboxing technologies. The survey analyzed notable sandboxing solutions with a focus on the mechanisms enabling application containment. Additionally, researcher's aimed to identify key trends in this area of research. As the diversified interface is only known by the trusted binaries, calls outside this interface clearly reveal non-trusted, suspicious or malicious binaries. The proof-of-concept showed this method to be practical for implementing honeypots for real-world systems.

Trusted Computing & Virtual Environments

Researchers of University of Turku made a survey to identify trends and objectives of using TPM (Trusted Platform Module) in the cloud, proposed and implemented a vTPM (virtual TPM) architecture for enabling TPM in container-based virtualizations, and created a secure live migration protocol for VMs (Virtual Machine). Majority of the research in this area has focused on security of traditional hypervisor-based virtualization. The research has made notable efforts to bridge these solutions to container-based systems, and thus, through vTPM research and other commitments, advanced security solutions in the area.

Secure Agile Software Development

A literature review was made to discover evidence about contemporary use of agile development methods in contexts wherein software security regulations apply, provided a theoretical

framework for assessing the interoperability of agile and secure software development activities, and created a secure modification of an agile software development method. The review on prior application of agile methods for security constrained software development accumulated a notable amount of evidence which indicates that agility and security are not mutually exclusive aspects of software development. Further, researchers demonstrated a generalizable proof-of-concept case study of developing a secure system with agile means.

Software Vulnerabilities and Exploits

Researchers of University of Turku modeled delivery of security advisories, provided a description for how exploits can be traded online, described software vulnerability lifecycles and reacted them against aging software products, and revised clustering and disclosure of software vulnerabilities in products delivered by large software vendors. They committed several in-depth but wide breadth reviews into existing vulnerabilities and exploits in varying software environments. These reviews allowed them to accumulate a mass of data on top of which robust statistical analyses were committed. The results of the analysis allowed to classify and describe several vulnerabilities and argue for example for their common properties which are still disregarded by several software development and vendor organizations; undermining software security by providing exploitation routes into otherwise secure systems.

Security-Motivated Web Crawling

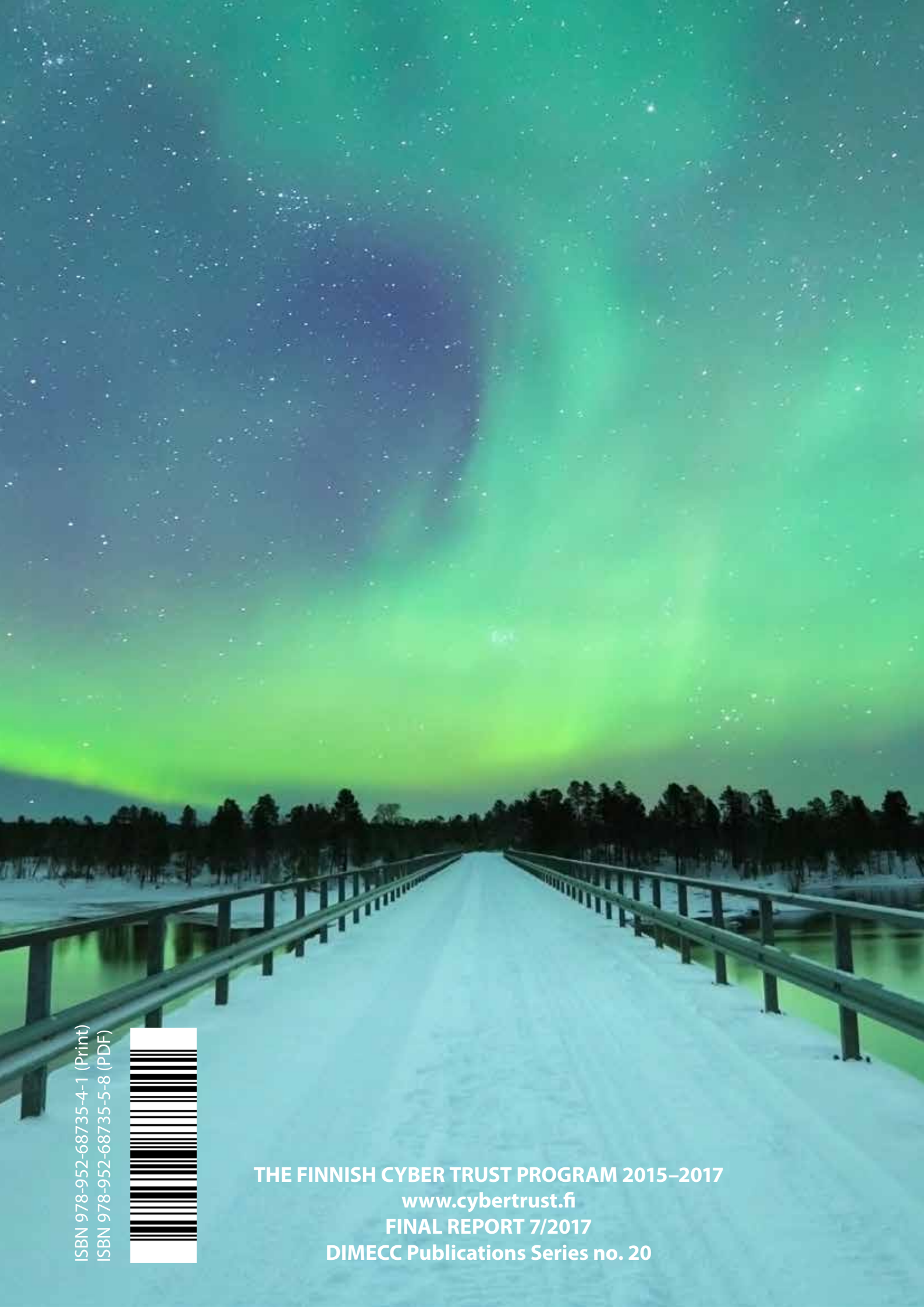
Researchers of University of Turku provided a post-mortem of the popularity and distribution of malware files in the contemporary web-facing internet (F-Secure's Riddler data), analyzed name server IP address importance for the forensics related to DNS-targeting (Domain Name System) malware, and provided design guidelines for simple network resolvers for DNS mining. Many of the efforts committed in this topic area have resulted in a rather exhaustive model of the commonly available web. The modelling has also collected data on the routes and behaviour of a plethora of malware operating in the captured web. This has allowed to acknowledge several limits and discrepancies of the infrastructure; especially of the DNS. Consequently, the research has allowed to design and propose appropriate security enhancements.

Scientific Publications

http://cybertrust.fi/publication/

Partners

Aalto University
Bittium
Capricode
Contrasec
Elisa
Ericsson
F-Secure
University of Helsinki
JAMK University of Applied Science
Jyväskylän Energia
University of Jyväskylä
Central Finland Health Care District
MPY
Netox
Nixu
Nokia
Pardco Group
Silverskin
Softera
Space Systems Finland
Tampere University of Technology
University of Oulu
University of Turku
VTT
Åbo Akademi



ISBN 978-952-68735-4-1 (Print)
ISBN 978-952-68735-5-8 (PDF)

THE FINNISH CYBER TRUST PROGRAM 2015–2017
www.cybertrust.fi
FINAL REPORT 7/2017
DIMECC Publications Series no. 20