|  |  |  |
| --- | --- | --- |
| C:\Users\s.evangelatos\Dropbox\EXUS_Innovation\EU-Project-GHOST\Project logo\LOGO white.png | GHOST Research Activities |  |
|  | |  |
| Co-funded by the Horizon Η2020 Framework Programme of the European Union under grant agreement No 740923. | | Introduction Within the lifespan of the GHOST project several scientific papers were published in prestigious peer-reviewed journals, workshops and conferences. This issue is dedicated to all these publications that aimed at raising awareness for all the scientific work done in the GHOST project. The GHOST academic partners provided cutting-edge research and insights on what is important to the scientific community in topics such privacy and security in IoT applications. In the next pages, a short summary of each publication is presented but the full-length papers can be found in our website <https://www.ghost-iot.eu/> and in the [OpenAIRE](https://explore.openaire.eu/search/project?projectId=corda__h2020::97479961f9e1c768f0cca13cea64e0ce) repository under the GHOST project. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | A Concept and Evaluation of Usable and Fine-Grained Privacy-Friendly Cookie Settings Interface *Kulyk, O., Mayer, P., Volkamer, M., Käfer, O.*  As cookies are commonly used on websites, they can constitute a significant threat to user’s privacy by tracking surfing behaviour. The browsers provide a variety of options for cookie settings, thereby potentially enabling the user to execute some control over the extent of being tracked. However, studies show that the interfaces for these settings are often deemed too confusing or complex for lay users, often failing to provide necessary explanations, and therefore preventing the users from properly using these setting interfaces to protect themselves against tracking. In this paper, we present a concept for a privacy-friendly cookie setting interface that is meant to support the user in configuring their cookie settings. The setting interface in our concept (1) uses an assistant to guide the user towards their preferred cookie settings via a series of questions; and (2) enables the user to set their cookie settings manually, providing explanations for each of the options available to the user, including the potential advantages and disadvantages of each option. To gauge the viability of the proposal, the concept has been implemented as a Chrome extension and evaluated in a user study with 21 participants. The results have shown, that the extension is well received by the participants and provides better usability than the standard cookie settings interface in Chrome. |  |  | A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective *Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D.*  The IoT makes our lives much easier, more valuable, and less stressful due to the development of many applications around us including smart cities, smart cars, and smart grids. Protecting IoT data of such applications at rest, either on the objects or in the cloud, is an indispensable requirement for achieving a symmetry in the handling and protection of the IoT. Unauthorised access to such data may lead to harmful consequences and possibly jeopardise the existence of IoT applications. IoT objects have limited capabilities in terms of memory capacity, battery life, and computational power. Furthermore, the lack of widely accepted IoT security and privacy guidelines for data at rest is another major influencing factor. We first briefly describe the main IoT security goals, identify stakeholders and discuss the most well-known data protection frameworks. Second, we highlight potential attacks and threats against data at rest and show their violated security goals. Third, we review a list of protection measures. Fourth, we propose a framework of security and privacy guidelines for IoT data at rest to enhance IoT security and privacy by design and establish a symmetry with the protection of user-created data. Our framework also presents the link between the suggested guidelines, mitigation techniques, and attacks. Finally, we review open issues the limitations of our suggested framework |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Advancing Trust Visualisations for Wider Applicability and User Acceptance *Kulyk, O., Reinheimer, B., Gerber, P., Volk, F., Volkamer, M., Mühlhäuser, M.*  There are only a few visualisations targeting the communication of trust statements. Even though there are some advanced and scientifically founded visualisations-like, for example, the opinion triangle, the human trust interface, and T-Viz-the stars interface known from e-commerce platforms is by far the most common one. In this paper, we propose two trust visualisations based on T-Viz, which was recently proposed and successfully evaluated in large user studies. Despite being the most promising proposal, its design is not primarily based on findings from human-computer interaction or cognitive psychology. Our visualisations aim to integrate such findings and to potentially improve decision making in terms of correctness and efficiency. A large user study reveals that our proposed visualisations outperform T-Viz in these factors. |  |  | Combining Statistical and Machine Learning Techniques in IoT Anomaly Detection for Smart Homes *Spanos, G., Giannoutakis, K.M., Votis, K., Tzovaras, D.*  In this paper, a security solution is proposed for IoT smart homes based on constructing behavioral device templates. These templates are being calculated by combining statistical and machine learning techniques according to their network behavior, captured within a smart home. The generated statistical metrics are being processed in order to produce the appropriate features, which are then used for constructing clusters of devices. The main idea relies on the fact that during an abnormal event, the device will be moved away from the center of the cluster, generating an alert that can be further used for proposing mitigation actions. The methodology followed in the proposed approach is given in detail, while validation is performed on a real smart home dataset. |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Deep Learning with Dense Random Neural Networks for Detecting Attacks against IoT-connected Home Environments *Brun, O.,* *Yin, Y., Gelenbe, E.*  In this paper, we analyze the network attacks that can be launched against Internet of Things (IoT) gateways, identify the relevant metrics to detect them, and explain how they can be computed from packet captures. We then present the principles and design of a deep learning-based approach using dense random neural networks (RNN) for the online detection of network attacks. Empirical validation results on packet captures in which attacks are inserted show that the Dense RNN correctly detects attacks. However our experiments show that a simple threshold detector also provides results of comparable accuracy on the same data set. |  |  | Detection of abnormal behavior in smart-home environments *G. Spathoulas, S. Evangelatos, M. Anagnostopoulos, G. Mema, S. K. Katsikas*  Without a doubt, the security of Internet of Things (IoT) systems is of crucial importance. The use of such systems has significantly increased in the recent year, where in every aspect of our daily life we interact with IoT environments and devices of any type. Therefore, it comes with no surprise that the relevant security concerns have attracted the focus of the security community and there is a rising need for security solutions in the IoT domain. GHOST is an EU Horizon 2020 Research and Innovation funded project, aiming at developing a reference architecture for securing smart-home IoT ecosystems. One of the approaches employed in GHOST project is to model the behavior of the IoT devices with regard to the network activity with the aim to detect and following mitigating cyber-security events. This functionality is mainly provided by two GHOST system modules, that is the Network and Data Flow Analysis (NDFA) and the Profile Builder (PB).  The multi-layer solution integrates traditional cyber-security countermeasures, while it introduces new mechanisms for the efficient defence of common to IoT threats. The architecture of GHOST system is based on multiple distinct concepts and modules. The main idea is that the network activity of the smart-home environment is monitored and fed to the various components which in turn notify the Risk Engine (RE) component about observed cyber-security events. RE then takes action, if required, in order to mitigate the identified risk. This paper presents, the part of the GHOST system related with the detection of the behavioral changes in the context of the smart-home devices' network activity. |  |
|  | Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users *Kulyk, O., Gerber, P., Marky, K., Beckmann, C., Volkamer, M.*  Over the years, the wide-spread usage of smartphones leads to large amounts of personal data being stored by them. These data, in turn, can be accessed by the apps installed on the smartphones, and potentially misused, jeopardizing the privacy of smartphone users. While the app stores provide indicators that allow an estimation of the privacy risks of individual apps, these indicators have repeatedly been shown as too confusing for the lay users without technical expertise. We have developed an information flyer with the goal of providing decision support for these users and enabling them make more informed decisions regarding their privacy upon choosing and installing smartphone apps. Our flyer is based on previous research in mental models of smartphone privacy and security and includes heuristics for choosing privacy-friendlier apps used by IT-Security experts. It also addresses common misconceptions of users regarding smartphones. The flyer was evaluated in a user study. The results of the study show, that the users who read the flyer tend to take privacy-relevant factors into account by relying on the heuristics in the flyer more often. Hence, the flyer succeeds in supporting users in making more informed privacy-related decisions. |  |  | From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes *Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K.M., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E., Nijdam, N.A.*  The H2020 European research project GHOST - Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control - aims to deploy a highly effective security framework for IoT smart home residents through a novel reference architecture for user-centric cyber security in smart homes providing an unobtrusive and user-comprehensible solution. The aforementioned security framework leads to a transparent cyber security environment by increasing the effectiveness of the existing cyber security services and enhancing system's self-defence through disruptive software-enabled network security solutions. In this paper, GHOST security framework for IoT-based smart homes is presented. It is aiming to address the security challenges posed by several types of attacks, such as network, device and software. The effective design of the overall multi-layered architecture is analysed, with particular emphasis given to the integration aspects through dynamic and re-configurable solutions and the features provided by each one of the architectural layers. Additionally, real-life trials and the associated use cases are described showcasing the competences and potential of the proposed framework. |  |
|  | GHOST - Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control *Collen, A., Nijdam, N.A., Augusto-Gonzalez, J., Katsikas, S.K., Giannoutakis, K.M., Spathoulas, G., Gelenbe, E., Votis, K., Tzovaras, D., Ghavami, N., Volkamer, M., Haller, P., Sanchez, A., Dimas, M.*  We present the European research project GHOST, (Safe-guarding home IoT environments with personalised real-time risk control), which challenges the traditional cyber security solutions for the IoT by proposing a novel reference architecture that is embedded in an adequately adapted smart home network gateway and designed to be vendor-independent. GHOST proposes to lead a paradigm shift in consumer cyber security by coupling usable security with transparency and behavioural engineering. Usability studies have been defined with the aim to establish mental models of the end users. This allows systematical and effective addressing of the human factor with the aim to facilitate end-users’ proper decision making in relation to security and privacy issues and adequate usage of the GHOST solution. GHOST's conceptual design involves advanced data flow analysis on a packet basis to build the context of communication. From this context, data are classified into user and device profiles, which in turn are used in the automated real-time risk assessment. The assessment is based on evaluation, comparison and matching with safe data flow patterns, utilising a self-learning approach. Data analytics and visualisation techniques are deployed to ensure enhanced user awareness and understanding of the security status, potential threats, risks, associated impacts and mitigation guidelines. |  |  | Home Sweet Home? Investigating Users’ Awareness of Smart Home Privacy Threats *Gerber, N., Reinheimer, B., Volkamer, M.*  Albeit providing many benefits, smart homes collect and process large amounts of sensitive data. In order to successfully cope with the resulting risks for their privacy, users have to be aware of potential privacy threats and consequences in the first place. Since research in other contexts has shown that users often lack this awareness even when it comes to well-known technologies, e.g., Online Social Networks (OSN), it is crucial to investigate users' awareness of threats related to the use of unfamiliar technologies like smart homes. To this end, we conducted a survey study with 1052 lay users. By prompting participants to state all consequences that could potentially result from using smart home and smart health devices as well as OSN, we find that most participants were unable to state a single privacy consequence. Instead, most referred to general privacy issues (e.g., profiling, data collection) or threats related to non-privacy topics, such as security problems resulting from defect smart home devices. Since our participants were least aware of potential privacy consequences resulting from the use of smart home devices, further effort is necessary to inform lay users about possible privacy threats, e.g., by launching public campaigns or conducting trainings and interventions directly implemented in the UIs of smart home systems. |  |
|  | Implementing a Forms of Consent Smart Contract on an IoT-based Blockchain to promote user trust *Kouzinopoulos, C.S., Giannoutakis, K.M., Votis, K., Tzovaras, D., Collen, A., Nijdam, N.A., Konstantas, D., Spathoulas, G., Pandey, P., Katsikas, S.*  The H2020 European research project Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST) aims to develop a cyber-security layer on IoT smart home installations. The proposed system analyses packet-level data flows for building patterns of communications between IoT devices and external entities. To ensure non-repudiation, integrity and authentication of the data captured, they are stored in a Blockchain, a distributed ledger network, as digitally-signed transactions. Since the data can potentially include sensitive user information, it is imperative to promote trust by informing users about the operating principles of the network as well as to request the acceptance of a consent form by them. This paper presents the design and implementation of a Forms of Consent application, a Distributed Application that interacts with a set of Smart Contracts deployed on a private Ethereum network. The application is being developed as part of the GHOST project. |  |  | Investigating People's Privacy Risk Perception *Gerber, N., Reinheimer, B., Volkamer, M.*  Although media reports often warn about risks associated with using privacy-threatening technologies, most lay users lack awareness of particular adverse consequences that could result from this usage. Since this might lead them to underestimate the risks of data collection, we investigate how lay users perceive different abstract and specific privacy risks. To this end, we conducted a survey with 942 participants in which we asked them to rate nine different privacy risk scenarios in terms of probability and severity. The survey included abstract risk scenarios as well as specific risk scenarios, which describe specifically how collected data can be abused, e.g., to stalk someone or to plan burglaries. To gain broad insights into people’s risk perception, we considered three use cases: Online Social Networks (OSN), smart home, and smart health devices. Our results suggest that abstract and specific risk scenarios are perceived differently, with abstract risk scenarios being evaluated as likely, but only moderately severe, whereas specific risk scenarios are considered to be rather severe, but only moderately likely. People, thus, do not seem to be aware of specific privacy risks when confronted with an abstract risk scenario. Hence, privacy researchers or activists should make people aware of what collected and analyzed data can be used for when abused (by the service or even an unauthorized third party). |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Non-negative Autoencoder with Simplified Random Neural Network *Yin, Y., Gelenbe, E.*  A new shallow multi-layer auto-encoder that combines the spiking Random Neural Network (RNN) with the network architecture typically used in deep-learning, is proposed with a learning algorithm inspired b non-negative matrix factorization which satisfies the non-negative probability constraints of the RNN. Auto-encoders equipped with this learning algorithm are tested on typical images including the MNIST, Yale face and CIFAR-10 datasets, and also using 16 real-world datasets from different areas., exhibiting the desired high learning and recognition accuracy. Montecarlo simulations of the stochastic spiking behaviour of this RNN auto encoder have also been carried out, showing that it can be implemented in a highly parallel manner to achieve substantial speed improvements. |  |  | Random Neural Networks and Deep Learning for Attack Detection at the Edge *Brun, O.,* *Yin, Y.*  In this paper, we analyze the network attacks that can be launched against Internet of Things (IoT) gateways, identify the relevant metrics to detect them, and explain how they can be computed from packet captures. We then present the principles and design of a deep learning-based approach using dense random neural networks (RNN) for the online detection of network attacks. Empirical validation results on packet captures in which attacks are inserted show that the Dense RNN correctly detects attacks. |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Smart Home Security – How safe is your data? *Milanovic, K.*  It is estimated that there are 59.3 million Smart Homes globally. Smart homes are defined as homes where there are smart appliances present. These can be coffee machines, vacuum cleaners or voice activated digital assistants. They are designed to be easy to use and reviews of these devices are centred around their interaction aspects. This division of security and convenience makes it difficult for the average user to determine the security of their device before purchase, but it is just as important to know how secure a device is as it is whether it’s easy to use. Fundamentally, there are two primary issues with the introduction of smart devices into the home. The first issue is that the device has ineffective security, for example the device is easily hackable. The GHOST system addresses this issue. The second issue is that the device is sufficiently secure, but users are manipulated into allowing manufacturers access to more data than they want. Overall what is required is more stringent regulation on the part of device manufacturers to combat both of these. |  |  | Towards Automated Threat-Based Risk Assessment for Cyber Security in Smarthomes *P. Pandey, A. Collen, N. Nijdam, M. Anagnostopoulos, S. K. Katsikas, D. Konstantas*  Cyber security is a concern of each citizen, especially when it comes to novel technologies surrounding us in our daily lives. A multitude of the cyber security solutions are currently under development to satisfy the increasing demand on threats and vulnerabilities identification and private data leakage detection tools. Within this domain, ubiquitous decision making to facilitate the life of the regular end-users is a key feature here. In this paper we present a Risk Assessment Model (RAM), originating from Negative to Positive approach, to automate the threat-based Risk Assessment (RA) process, tailored specifically to the smart home environments. The calculation model application is demonstrated on derived threat-triggered evaluation scenarios, which were established from analysing the historical evidence of data communication within the smarthome context. The main features of the proposed RAM are the identification of the existing risks, estimation of the consequences on possible positive and negative actions and embedding of the mitigation strategies. Through the proposed RAM, common factors and variables are extracted and integrated into a quantified risk model before being embedded in the automated decision making process. This research falls within the GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control) project, aiming to provide a cyber security solution targeted at the regular citizens. |  |
|  | Towards Reliable Integrity in Blacklisting: Facing Malicious IPs in GHOST Smart Contracts *G. Spathoulas, A. Collen, P. Pandey, N. A. Nijdam, S. K. Katsikas, C. S. Kouzinopoulos, M. B. Moussa, K. M. Giannoutakis, K. Votis, D. Tzovaras*  When it comes to novel cyber security solutions for extremely heterogeneous environments like IoT and smart homes, the key focus is typically given to the understanding of network activities and elimination of suspicious traffic. The GHOST project adds an extra dimension to this approach by integrating blockchain technology at its core decision mechanism. GHOST's Smart Contracts (SC) are designed to tackle in an easy, yet productive way, the reporting on suspicious IP addresses which the IoT devices in a smart home are trying to communicate with. Two variations of blacklisting smart contracts are presented in this paper, covering a diverse spectrum of possible attack vectors while closely following the Privacy by Design (PbD) principles. This paper presents a novel SC use case that aims to provide decentralised security for the protection against data exchange with malicious nodes external to the smart home. Each GHOST smart home installation collaboratively creates and maintains a blacklist of malicious IP addresses, by sharing *Risk Engine (RE)* produced data from the evaluation of the risks imposed by specific connections between the external IPs and the gateway, an external IP and the IoT devices in the smart home, and the actual behaviour of the IoT devices and their network communication profiles. Blacklisted IPs are stored on the private blockchain with the help of SCs. The implementation of the blacklist implies operation with data of different levels of sensitivity and trustworthiness and, therefore, can be split into two scenarios: public and private. The main contribution is the integration of a SC with reputation scoring method, further exploited by the RE to perform dynamic risk metric calculations in order to characterise the likelihood of an external IP being malicious. |  |  | Using blockchains to strengthen the security of internet of things *Kouzinopoulos, C.S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., Katsikas, S. K., Collen, A., Nijdam, N.A., In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D.* (eds.)  Blockchain is a distributed ledger technology that became popular as the foundational block of the Bitcoin cryptocurrency. Over the past few years it has seen a rapid growth, both in terms of research and commercial usage. Due to its decentralized nature and its inherent use of cryptography, Blockchain provides an elegant solution to the Byzantine Generals Problem and is thus a good candidate for use in areas that require a decentralized consensus among untrusted peers, eliminating the need for a central authority. Internet of Things is a technology paradigm where a multitude of small devices, including sensors, actuators and RFID tags, are interconnected via a common communications medium to enable a whole new range of tasks and applications. However, existing IoT installations are often vulnerable and prone to security and privacy concerns. This paper studies the use of Blockchain to strengthen the security of IoT networks through a resilient, decentralized mechanism for the connected home that enhances the network self-defense by safeguarding critical security-related data. This mechanism is developed as part of the Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control (GHOST) project. |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |
|  |