Mitigating IoT Security Threats with a Trusted Network Element

Jarkko Kuusijärvi, Reijo Savola, Pekka Savolainen, Antti Evesti
Cybersecurity
VTT Technical Research Centre of Finland Ltd
Kaitoväylä 1, FIN-90570 Oulu, Finland
{jarkko.kuusijarvi, reijo.savola, pekka.savolainen, antti.evesti}@vtt.fi

Abstract—**Securing the growing amount of IoT devices is a challenge for both the end-users bringing IoT devices into their homes, as well as the corporates and industries exposing these devices into the Internet as part of their service or operations. The exposure of these devices, often poorly configured and secured, offers malicious actors an easy access to the private information of their users, or potential to utilize the devices in further activities, e.g., attacks on other devices via Distributed Denial of Service. This paper discusses the current security challenges of IoT devices and proposes a solution to secure these devices via a trusted Network Edge Device. NED offloads the security countermeasures of the individual devices into the trusted network elements. The major benefit of this approach is that the system can protect the IoT devices with user-defined policies, which can be applied to all devices regardless of the constraints of computing resources in the IoT tags. Additional benefit is the possibility to manage the countermeasures of multiple IoT devices/gateways at once, via a shared interface, thus largely avoiding the per-device maintenance operations.**

Keywords-Security offloading; trusted network element; IoT-gateway

I. INTRODUCTION

The IoT (Internet-of-Things) scenarios bring completely new ways of interaction with our world. Already now, the use of IoT devices and emerging applications – which utilise sensors and actuators from our environment – have created several interesting use cases for new business. The possibilities of IoT have been discussed for a long time. Moreover, through the use of IoT devices in an industrial environment, industrial Internet has emerged, which spawns the expansion of use cases with significant advantages: For instance, more efficient production, time savings, and energy efficiency.

Security challenges can be an obstacle for IoT adoption in critical use cases and for the security-aware home users alike. On the other hand, well-designed and effective security for IoT can be a business enabler; high assurance that the particular solution brings IoT advantages without additional security risks. Security issues of IoT have been investigated – e.g., from privacy and legislation [1], integrity and confidentiality [2], and authentication [3] perspectives. These all are essential parts to secure IoT applications. Nevertheless, fast evolution, resource restrictions, and emerging completely new use cases cause constant maintenance and development challenge related to IoT security. Difficulty to patch and update devices is often mentioned as a challenge of IoT security. For example, SANS Institute asked “What do you think the greatest threat to the Internet of Things will be over the next 5 years?”, and 31.0% (the biggest group) answered “Difficulty patching Things, leaving them vulnerable” [4]. Simultaneously, in the same study it appeared that the most of the respondents thought that an IT security group has to take responsibility to manage risks appearing from IoT. The IoT threats are categorised below, in Section 2, giving an IoT architectural view to the IoT-threat landscape.

Because the utilisation opportunities for IoT are clearly visible, and already proven in various cases, it is vital to offer additional and uniform security to assure users with demanding security needs. Beside the accustomary user-and-action-specific control also the IoT-specific control needs have to be served; these are discussed below in Section 3. In this paper, we concentrate on a problem related to the generic implementation of security countermeasures for small and resource-restricted IoT devices in a uniform and scalable way. As mentioned above, it is often assumed that an IT security group takes responsibility to secure IoT, e.g., install and update proper countermeasures. Naturally, it is not possible to implement all required countermeasures into each IoT device, e.g., temperature sensor vs. fridge, which causes that various ad-hoc countermeasures might appear that makes maintenance burden even worse.

In this paper, we present how a NED (Network Edge Device) – developed in the EU project SECURED (SECURity at the network EDge [5]) – can be applied to implement an effective security solution for IoT applications. The NED is a local network or a cloud-based solution to collect an extensive set of security countermeasures into one place, where these mechanisms can be selected for networked devices, based on user needs and policies. Thus, NED offers countermeasures for IoT devices by acting as a proxy service for IoT communication. In addition, we analyse IoT security threats and present an architecture that mitigates them by the means of a NED when applicable. Furthermore, currently implemented countermeasures are presented and future countermeasures are

978-1-908320/73/5/$31.00 © 2016 IEEE

envisioned that would further improve the security posture of IoT devices.

Two most common communication modes of IoT devices are direct and gateway-based communication. In the direct communication, an IoT device sends and receives data directly to/from network, whereas in the gateway-based communication, the IoT devices are connected to a gateway that sends data into a database where requiring parties retrieve it when needed. These two communication modes have the same security requirements; however, threats and attack methods against the models differ. In general, our proposed solution can improve the security of both solutions, though our proposal could be included in a more resource capable gateway directly if needed.

The rest of paper is organised as follows. Background and current challenges are described in Section 2. Section 3 presents threat analysis and risk mitigation utilizing the trusted network element, NED. Demonstration use case is presented in Section 4. Finally, results and shortcomings are discussed in Section 5 and Section 6 concludes the paper.

II. Background

A. *IoT Security Challenges*

Farooq introduces in [6] a four-layer IoT security architecture. In essence, this architecture aggregates the layered interfaces of Functional Decomposition view of ARM (Architectural Reference Model for IoT) to attack surfaces [7]. ARM is the main model of this architecture developed in FP7 research project IoT-A. The four-layer architecture is applicable for NED benefit analysis in IoT protection. For each layer, the open cybersecurity challenges – that is, the challenges not solved in the of-the-shelf IoT solutions – are introduced. The architectural layers are defined as follows [6]:

- **Perception layer**: Comprises of the tags, the physical sensor and actuator devices, with RF connection
- **Network layer**: Forms the communication network, commonly wireless sensor network, connecting the tags to the information processing (back-office) system
- **Middleware layer**: Consists of the information processing systems, the databases providing storage capabilities; service oriented with the goal to provide similar services to all the connected nodes
- **Application layer**: Comprises of the various business-logic applications, creating the added-value IoT applications to implement a smart space, smart logistic, or even smart grid.

Selected IoT attack types in different architectural layers are listed in Table 1.

There are remarkable challenges for security in IoT applications due to the *system characteristics*. First, information is highly distributed in the component systems [8]. This makes it possible for an attacker to choose various strategies, utilizing this physical and logical ubiquity. Scalability of countermeasures is a particular challenge. Limited system resources can limit utilization of some countermeasures. Especially, efficient encryption schemes, with frequent computation, cannot be often used in connection with low-energy and low-memory IoT devices. IoT devices are often quite heterogeneous. High quality configuration management and updating procedures can be difficult. Heterogenuity introduces easily more vulnerabilities to the system as a whole, too.

TABLE I. IoT Security Attack Types In Different Architectural Layers

Perception layer	**Network layer**	**Middleware layer**	**Application layer**
Unauthorised access	Sybil attack	Unauthorised access	Code injection
Tag cloning	Sinkhole attack	DoS	DoS
Eavesdropping	Sleep deprivation	Insider attack	Spear-Phishing
Spoofing	DoS		Sniffing
RF jamming	Code injection		
	MitM		

a. DoS = Denial of Service, MitM = Man-in-the-Middle

The emerging and completely new business applications are posing yet new requirements for IoT-tag fleet management, e.g., from the authorisation and IoT tag identity management viewpoint [9]: the prevalent all-or-nothing (root) access shall be upgraded to enhance the accustomary *multiple users with differing grants* (distinguish between requests from various users) towards *access based on dynamically changing parameters with decisions per user, resource and action*, up until IoT-inherent control needs like *pay-by-use and limited anonymous* grants.

If the IoT application is mobile, threats are even more emphasized. Because access controls are more complicated in this case, they potentially offer more holes for the attackers. In particular, in the mobile environments, unauthorised access by new device introduction, utilizing the holes in access control, becomes possible. In addition, wearable IoT devices record vast amount of information from the users and the access and sharing of this data is a major concern for individual's privacy.

B. *SECURED Platform and NED*

The idea of SECURED [5] is to off-load the security controls (e.g., malware protection, IDS/IPS, network monitoring, etc.) from the individual devices (laptop, tablet, mobile, IoT device) to the closest trusted network element, a network edge device (NED), thereby providing the same security level for each user's device in the SECURED platform, without heavy processing power restrictions on the individual devices. The SECURED platform provides a user-friendly way to define the security policies in a high-level language for the actual end-users without the need of having to be an expert in, e.g., firewall configurations. More detailed information about SECURED's approach and offloading

978-1-908320/73/5/$31.00 © 2016 IEEE

security to the network edge and the relevant components is discussed in previous work [10].

The NED (see Fig. 1), a trusted network node (attested by a trusted 3rd party node, Verifier), enables uniform protection independent from the used terminal by handling the user's traffic according to the security policies defined by the user. The user's security policies are enforced by Personal Security Application(s) (PSAs) running in the NED. The PSAs are the security controls required for enforcing confidentiality, integrity and availability. The PSAs are fetched by the NED from a PSA repository. The user can define his/her security requirements via a high-level or medium-level policy language, depending on whether he/she is a normal user or an expert user in the area of the security control to be used. The SECURED platform incorporates a multi-layered security policy definition, in which the same connection may be subject to constraints from different tenants. The policies are applied in a hierarchical way, taking into account, e.g., company or government enforced policies, which are applied to all relevant users. The policies defined for a user are fetched from a policy repository.

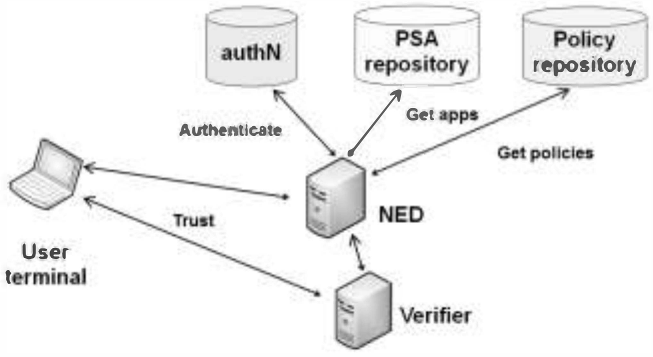

Figure 1. SECURED logical architecture

The NED offers multitenancy and traffic isolation between users with the use of virtual LANs and Open vSwitch. The SECURED platform provides a proof of trust of the used NED, where the user is connected, by a trusted third party attesting the NED machine – NED is equipped with a hardware Trusted Platform Module (TPM) cryptographic chip – at defined intervals, in addition to the NED machine being attested at connection start phase, to verify that the NED machine is not compromised and is running the correct software without any tampering. This attestation proof requires an additional SECURED application (implementing IPsec VPN connection to the NED) to be installed to the user terminal, that can contact the trusted third party before connecting to the NED and also to periodically receive attestation status during active connection. An IoT device (node or gateway) can also be connected to the NED without the use of this specific application, e.g., in case the device is connected through LAN.

III. Current and Proposed Countermeasures

The proposed NED-hosted countermeasures help in mitigating security threats in the typical situation, where terminal nodes have only limited communication and computation resources. Concentrating the countermeasures on the network edge, where more resources are available, makes it possible to select targeted and strong countermeasures, depending on the requirements and situations in the IoT application.

Authentication is a major class of IoT security countermeasures. The ubiquity of IoT applications calls for versatile – that is, complex – authentication solutions, at terminal nodes, too. Constraining factors are the limited communication and computing resources in the terminal end. Therefore, light-weight yet strong authentication schemes are needed. This is a major challenge still. The countermeasures proposed here generally apply to Network Layer, Middleware layer, and Application layer architectural layer types presented in Table 1. The Perception layer is out of the scope of this work, as our proposed solution is the closest network edge to the nodes. Of course, partially the network edge can also detect, e.g., if there exist a clone providing same type of data through inference in monitoring the communication via the network edge.

In SECURED, we define a specific countermeasure as a Personal Security Application (PSA) that can be either one individual security control or a combination of security controls to provide a certain capability they can offer in terms of enforcing some specific security feature. The PSAs are also able to be migrated from a NED to another NED in case of a mobile scenario. Some examples of the PSA capabilities are: access control (filter and restrict traffic), malware (detection and eradication of malicious traffic), privacy (offer privacy, e.g., by VPN), network and monitoring (e.g., intrusion detection system or general logging of connections to and from a targets).

The PSAs are essentially virtualized Network Functions (VNF), which can be executed in the hosting NED as a lightweight VM, a Linux container, a Docker container, or a fully-fledged VM. The implementation strategy of a PSA depends on the wanted level of isolation, efficiency and time required for a PSA to be implemented/ported from existing software to be compatible with a NED. The most isolated and fastest to developed PSA is porting an existing security control into a fully-fledged Virtual Machine. On the other hand, a VM requires more resources from the NED machine in terms of processing power and memory consumption.

Every implementation strategy accompanies a PSA API to allow the control of the PSA by the NED (e.g., configuration, starting, stopping, checking the status of the security control, etc.). The current implementations of PSAs are minimum footprint fully-fledged VMs with a disk size of 512-1024 MB.

Relevant example PSAs for IoT (that are already implemented in the SECURED project) are listed in Table 2, along with a discussion of their benefits to IoT applications. As can be seen from these examples, the set of defences will be very strong, compared to security solutions at terminal nodes (especially, if compared to low-resource IoT devices and/or IoT gateways). Table 2 describes the existing PSAs and list possible benefits that each PSA can offer for IoT usage; in general, multiple PSAs can be used in combination to create a security policy/configuration that allows achieving all the necessary goals on securing an IoT device(s).

TABLE II. CURRENTLY AVAILABLE PSAS PROPOSED FOR IOT CASES

PSA Description	Benefits for IoT
Bandwidth control	Due to resource restrictions of IoT devices, a bandwidth control facilitates to save available resources, i.e., send/receive capability and batteries. Thus, bandwidth control directly supports availability. However, it is notable that bandwidth control is not able to mitigate all threats pertaining to availability, e.g., DDoS.
Bro-logging	Logging can be seen as an enabler to recognise and actively prevent attacks, e.g., data leakage. In an IoT context logging, and recognition of suspicious traffic, can be achieved more easily when compared to traditional IT systems because traffic profiles are more static changes are mostly user driven. Logging supports data confidentiality and system integrity.
Bro-malware	Malware for IoT devices already exist [11]. However, it can be assumed that the peak of IoT malware is not yet visible, even though it is said that "IoT is the new Windows XP -malware's favourite target" [12]. Thus, it is clear that malware detection is needed in IoT devices and environments. Malware detection can pertain to all security objectives, i.e., Confidentiality, Integrity, and Availability (CIA) triad.
iptables	iptables can be applied as a firewall solution for IoT devices. In other words, incoming and outgoing traffic can be analysed based on predefined rule set in order to identify traffic types and / or destinations that are not acceptable.
Re-encrypt	Re-encrypt feature ensures that the best possible encryption is applied for network payload (with a man-in-the-middle proxy). In other words, if IoT device sends data without encryption and receiving device supports, e.g., TLS, then TLS is automatically used. This supports communication confidentiality.
VPN	Offering VPN connections is a way to offer a secure communication for IoT devices over an untrusted network. Applying VPN connection is able to reduce man-in-the-middle attacks, support privacy, and communication confidentiality.

A. Analysis of countermeasure off-loading possibilities

Countermeasures are technical or non-technical, and some set of technical countermeasures can be implemented outside of IoT device. When the countermeasures are located at the network edge, through which the IoT devices are communicating to the Internet, they can be easily updated in case a vulnerability is discovered in the IoT devices and/or the countermeasures can be used to mitigate the impacts of a successful exploit in one of the IoT devices. The defined policies for individual users (IoT gateways, for instance) are fetched from the policy repository, so the configuration of the policies for a general type user IoT gateway can be updated from one place to multiple devices. A typical IoT system can be protected by one or multiple NEDs depending on the network deployment.

B. Vision of required PSA to further enhance IoT Security

In the following we discuss and present a set of countermeasures currently developed and vision new countermeasures in order to fully support the growing security needs of an IoT gateway.

From the list of current countermeasures, the most important ones for IoT gateway-solutions are iptables (set allowed connections), re-encrypt/VPN (secure communication, if possible), and Bro-based (network monitoring / Intrusion Detection System). With these available countermeasures, the end-user or the admin can easily enable security features for an IoT gateway and also enable logging of the traffic, to see if there are any interesting communications.

The enforcement of communication encryption is a solid solution for the confidentiality and integrity, and network monitoring can be used to assess the availability. Still, a compromised IoT node or a gateway can send fraudulent data that cannot be easily detected; or the data can be stale, in case an attacker can exploit vulnerabilities on those entities.

An IoT node can send faked information, if the gateway does not enforce secure connection between the node and the gateway. A countermeasure that could detect the fraudulent packets, or even packets that are not generated at a defined rate, could detect a fraudulent node or a node not functioning correctly. The Bro Network Security Monitor [13] can be used to detect such events, and a PSA that detects and blocks any packets violating the set standard / learned standard of communication would benefit the IoT end-users and admins. This kind of PSA would be specifically tailored to fit the needs of a specific IoT gateway protocol, since it needs to detect and infer information from the packages sent from the IoT node/gateway into Internet. A PSA can inform the end-user/admin that a node is not functioning correctly thus ensuring the functionality of the whole IoT system. For example, a sensor reporting humidity, temperature, etc., can be used in a control loop to control the air conditioning or the heating system, and if the sensors providing the information either malfunction or are compromised, the controlling of the actuators could have serious implications. Additionally, a gateway allowing control messages from the Internet should have a PSA checking the packages for known malware and/or source and also to protect the gateway from DoS attacks. The NED is expected to have more processing power than a typical IoT gateway, thus allowing some level of protection to DoS attacks as well.

In [14] we discussed how the NED (the trusted network element) can be utilized to make trust measurements for a trustee and provide a trust metric value for the trustor – this idea can be implemented as a PSA that can measure the trust level of each connected IoT node / gateway, in order the make a decision whether the information provided by the node can be used. This information can then be used by the admin to disallow compromised nodes or the IoT service that uses the information of individual nodes to make decisions of the whole system / actuator controls. This kind of PSA can be used to detect malicious IoT devices and thereby block access to them or from them to the private network in which they are connected to, thus protecting possible data leakage or further malware distribution, for instance.

IV. A Case Example Of Securing an IoT Gateway with The NED

The case study takes place in a corporate environment, in which the users are connected to the Internet via the NED. In addition to the users, the NED is used to secure the IoT platform offering various sensors and actuators providing information of the surroundings.

A. *Experimentation setup and results*

In this case study (see Fig. 2) we used a NED to secure an IoT gateway for various sensors and actuators in a closed corporate scenario, where the gateway exposed an interface to control the enabled services, apply commands to actuators. The IoT gateway was connected to the NED via a LAN cable (also Wi-Fi could have been used) and the gateway was then registered as an user for the NED. The IT admin defined a set of security policies for the gateway(s). In case of multiple IoT gateways, all the gateways can be configured individually, or all the gateway clients could share a user group, in which case the admin can apply the same policies to be used for all the gateways, which allows for a quick configuration and also a quick detection of the state of the network.

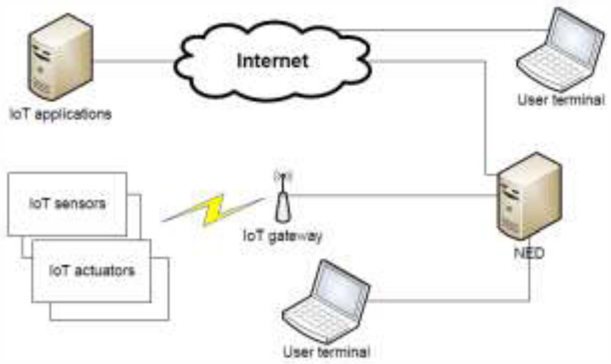

Figure 2. Case study logical setup

The example user scenario is that an employee of the company can read the sensor values and also control the actuators available in the administrator interface. This is controlled by the NED enforcing the policies set for the IoT gateway and the IoT applications server. The IoT gateway processes the messages from IoT nodes and forwards them to the IoT applications and the NED monitors restricts this communication to be allowed only to the defined cloud node that handles storing the IoT data. The admin defined a policy that the IoT gateway could only connected to a predefined address, and also defined a logging of connection to the IoT gateway to its communication to the application server, where the actual data was stored. This information was available in the logs of the PSA in charge of this functionality. The high-level policies defined for this case were “IoT, allow access, traffic target: target“ and “IoT, enable logging, traffic target: target”. The purpose of high-level policies is to allow normal end-users to configure security easily. In addition to this high-level policy, the admin can define a more detailed configuration, e.g., for logging connections by defining how many connections to a target causes a log/event to be generated based on the traffic. This experiment was conducted in VTT Oulu premises as a part of the trial testbed of the SECURED platform.

V. Discussion

We have discussed the security challenges of current and future IoT applications, and proposed a cloud-based solution for mitigating the security threats. This solution uses NEDs (Network Edge Devices) to collect the needed set of security countermeasures. This kind of approach helps especially conquer scalability and limited computation resource problems in case of a resource-constrained IoT device or gateway. Remarkable challenges of the solution are the ubiquity of IoT applications, and mobility of them.

In the example case study, we utilized a NED machine capable of running multiple VMs per user and supporting users up to 100s with small-footprint VM PSAs. In the future, we can further modify the PSAs to be executed as Docker containers and/or combine multiple PSAs into one VM, thus enabling more focused PSAs that can handle all the required capabilities for an IoT node. Another possibility would be to install the PSAs and a minimum NED setup to the actual IoT gateway, thus allowing the pros of SECURED without the need of an additional gateway. The cons of this setup are, of course, that the gateway still has less resources in terms of computation and storage compared to a normal server acting as the network edge gateway. This kind of setup would still utilize the decentralized features of SECURED to provide the user-centric security by components controlled by the company or provided by an ISP or service provider in an outside cloud.

VI. Conclusions and Future Work

The proposed solution facilitates both the IoT end-users and the IT security group, who is often responsible of IoT security. Firstly, the end-users get a better assurance that IoT security is developed in a consistent way, without ad-hoc countermeasures. Secondly, security administrators, i.e., the IT security group, can concentrate on the maintenance activities in one central place. The proposed solution offers a uniform way to update and add security countermeasures for an IoT environment. Therefore, emerging threats can be mitigated by developing a new countermeasure into the NED device. In other words, there is no need to modify dozens of different IoT device types with varying programming interfaces. As an additional benefit, the proposed solution doesn’t consume resources from the IoT devices, which is vital in order to get the full benefit of each IoT sensor and actuator.

Our future work includes a more detailed analysis of IoT risks, and mapping them to the potential countermeasures in NEDs. Additionally, a PSA for measuring the level of trust to individual nodes (be that a user or an IoT node/gateway) is to be studied and implemented to protect, or at the minimum mitigate the effects of a compromised node. In order to be able to infer more detailed information from the communications of IoT gateway, the developed countermeasure will have to understand the messages produced/consumed by the gateway.

Acknowledgment

The work presented in this paper was partly funded by the European Commission under the ICT theme of FP7 (grant agreement no. 611458) related to the SECURED project and Tekes – the Finnish Funding Agency for Technology and Innovation – in Celtic-Plus Flagship project Sendate (Dnro 2783/31/2015).

References

[1] R. H. Weber, "Internet of Things – New security and privacy challenges," Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, Jan. 2010.

[2] O. R. Merad Boudia, S. M. Senouci, and M. Feham, "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography," Ad Hoc Networks, vol. 32, pp. 98–113, 2015.

[3] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Networks, vol. 20, pp. 96–112, 2014.

[4] J. Pescatore, "Securing the 'Internet of Things' Survey," 2014.

[5] "SECURity at the network EDge," [Online]. Available: https://www.secured-fp7.eu/. [Accessed: 10-Nov-2016].

[6] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Int. J. Comput. Appl., vol. 111, no. 7, pp. 1–6, 2015.

[7] Nettsträter, A. ed., 2012. Internet-of-Things Architecture IoT-A Deliverable D1.3 – Updated reference model for IoT v1.5.

[8] M. J. Covington and R. Carskadden, "Threat Implications of the Internet of Things," in 2013 5th International Conference on Cyber Conflict, 2013, pp. 1–12.

[9] Seitz, L., Selander, G. & Gehrmann, C., 2013. Authorization framework for the Internet-of-Things. In 2013 IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2013.

[10] D. Montero, M. Yannuzzi, A. Shaw, L. Jacquin, A. Pastor, R. Serral-Graciá, A. Lioy, F. Risso, C. Basile, R. Sassu, M. Nemirovsky, F. Ciaccia, M. Georgiades, S. Charalambides, J. Kuusijarvi, and F. Bosco, "Virtualized Security at the Network Edge : A User-centric Approach," Communications Magazine, pp. 1–10, 2015.

[11] "IoT devices being increasingly used for DDoS attacks," Symantec Connect Community, 2016. [Online]. Available: http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks. [Accessed: 28-Sep-2016].

[12] "'Internet of Things' is the new Windows XP—malware's favorite target," Ars Technica, 2014. [Online]. Available: http://arstechnica.com/security/2014/04/how-new-malware-is-making-the-internet-of-things-the-windows-xp-of-2014/. [Accessed: 28-Sep-2016].

[13] "The Bro Network Security Monitor," [Online]. Available: https://www.bro.org/. [Accessed: 10-Nov-2016].

[14] J. Hiltunen and J. Kuusijärvi, "Trust Metrics Based on a Trusted Network Element," *Trustcom/BigDataSE/ISPA, 2015 IEEE*, Helsinki, 2015, pp. 660-667.