View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Bournemouth University Research Online

ERCIM NEWS

www.ercim.eu

Special theme:

Cyber-Security

Also in this issue:

Keynote:

Cybersecurity: A Key Pillar of the European Digital Single Market

by Afonso Ferreira and Paul Timmers
DG CONNECT, European Commission

Research and Society:

On the Occasion of Aad van Wijngaarden's 100th Birthday

International Informatics

by Gerard Alberts

Research and Innovation:

High-Density Data Storage in Phase-Change Memory

by Haralampos Pozidis, Nikolaos Papandreou, Thomas Mittelholzer and Evangelos Eleftheriou

proof-of-concept of this architecture is partly supported by the SECSi French PIA (Programme Investissement Avenir) project.

Important scientific, technological, societal and legal issues are raised by such Secure Personal Cloud architecture. Notably, our objective is to enable the execution of distributed queries linking the personal data of several individuals with the guarantee that neither the result of the query, nor the observation of all intermediate steps of the execution discloses any information about a particular individual [4]. In other words, Privacy-by-Design big data treatments can be implemented on personal data. Another important challenge is to ease the declaration and administration of access control policies by the individuals. Our hope is that the Secure Personal Cloud approach will provide a credible alternative to the systematic centralisation of personal data on servers and will pave the way for new privacy-by-design architectures.

Links:
[L1] https://cozy.io/fr/
[L2] https://project.inria.fr/plugdb/

References:
[1] S. Abiteboul, B. André, D. Kaplan: "Manage your digital life in your personal info management system", Communications of the ACM, 2015, 58 (5), pp.32-35.
[2] N. Anciaux, S. Lallali, I. Sandu Popa, P. Pucheral: "A Scalable Search Engine for Mass Storage Smart Objects", Proc. of the 41th International Conference on Very Large Data Bases (VLDB), Hawaï, PVLDB 8(9): pp 910-921, September 2015.
[3] N. Anciaux, et al.: "MILo-DB: A Personal, Secure and Portable Database Machine", Distributed and Parallel Database Journal (DAPD), 32(1), 2014.
[4] C. To, B. Nguyen, P. Pucheral. 'Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture', ACM Transaction on Database Systems (TODS), to appear (http://tods.acm.org/).

Please contact:
Benjamin André
Cozy Cloud, France
benjamin@cozycloud.cc

Philippe Pucheral
University of Versailles & Inria, France
Philippe.Pucheral@inria.fr

VirtuWind – Security in a Virtual and Programmable Industrial Network Prototype Deployed in an Operational Wind Park

by Ioannis Askoxylakis, Nikolaos Petroulakis, (FORTH), Vivek Kulkami and Florian Zeiger (Siemens)

The wind power industry is a good example of an industrial network with strict performance, security, and reliability requirements. The VirtuWind project aims to develop and demonstrate a software defined network (SDN) and network function virtualisation (NFV) ecosystem, based on an open, modular and secure framework.

Applications are becoming increasingly networked and distributed, especially in industrial domains, such as smart grid, factory automation, process automation, transportation and logistics. Many of these applications have very stringent requirements on the underlying communication network(s). This is currently addressed by using complex and proprietary network protocols and mechanisms, but this approach has major drawbacks: substantial engineering, operations and maintenance efforts; complex configuration of devices and services; and significant (planned) down times during system upgrades. Thus, there is a trend in industrial networks to move away from closed, implementation-specific solutions towards more open solutions. Open, standardised solutions come with their own problems, however: increased openness makes intra-domain operation and security more critical than ever before and different network providers may implement the same functionality differently, with interoperability and inter-domain operation becoming a huge concern.

VirtuWind will develop and demonstrate a software defined networking (SDN) and network function virtualization (NFV) ecosystem, based on an open, modular and secure framework [1]. The project showcases a representative use case of an industrial network by demonstrating a prototype of an industrial control network for wind park operations. It also addresses the challenges in intra-domain and inter-domain scenarios of real wind parks, and validates the economic viability of the demonstrated solution. The wind park control network has been chosen as a professional application in VirtuWind as wind energy has now established itself as a mainstay of sustainable energy generation. By envisioning lower capital expenditure and operational expenditure costs in control network infrastructure, VirtuWind will play an important role in assisting the wind energy sector to reduce costs. The VirtuWind solution also has the potential to offer multiple benefits to the communication networks of other industrial domains.

Introducing revolutionary concepts, such as SDN and NFV, to the communication networks of critical infrastructures, requires a careful investigation of the new security risks, since new threats – not encountered in legacy systems – will occur [2]. More specifically, SDN is currently only used in closed environments, such as data centres. However, the use of SDN in cross-domain setups and the absence of multi-operator col-

laborative incident detection mechanisms introduces new threats. The nature of software increasingly used in SDN and NFV environments comes with additional security threats, such as data forging, application programming interface (API), controller and management exploitation which need to be avoided by means of suitable mechanisms, e.g., strong authentication, access control, application isolation and sandboxing, flow integrity and conflict resolution as well as threat detection and encrypted interfaces.

One of the core objectives of VirtuWind is to assure security-by-design for the SDN and NFV ecosystem. To this end, VirtuWind aims to establish comprehensive threat and risk frameworks for industry-grade SDN networks. Suitable mechanisms will be developed for network monitoring and intrusion detection for SDN networks. More specifically, VirtuWind aims to address the following requirements:

Authentication, Authorization and Accounting (AAA)

The presence of mechanisms ensuring AAA functions, distributed horizontally and vertically on the SDN, if needed, are necessary for validating identities and requests, and for providing logging of the associated events. Authorisation (access control) and other control plane elements, along with the associated interfaces, will provide isolation and QoS-awareness to the overlaying applications. Mechanisms for ensuring accountability of controller actions affecting cyber-physical systems will be enabled. In addition, north bound interfaces (interfaces to the business applications) should allow applications to express their requirements in terms of network policies, e.g., flow isolation and QoS profiles. Based on the information exchanged through this interface, authentication and authorisation of stakeholders could be realised via access and role-based lists for different levels of function granularities.

Secure Interfaces

The SDN infrastructure will be reachable from beyond a network services platform's domain and needs protection from misuse and abuse. More precisely, security mechanisms for the protection of controller and inter-controller interfaces should be established. In addition, the definition of security mechanisms

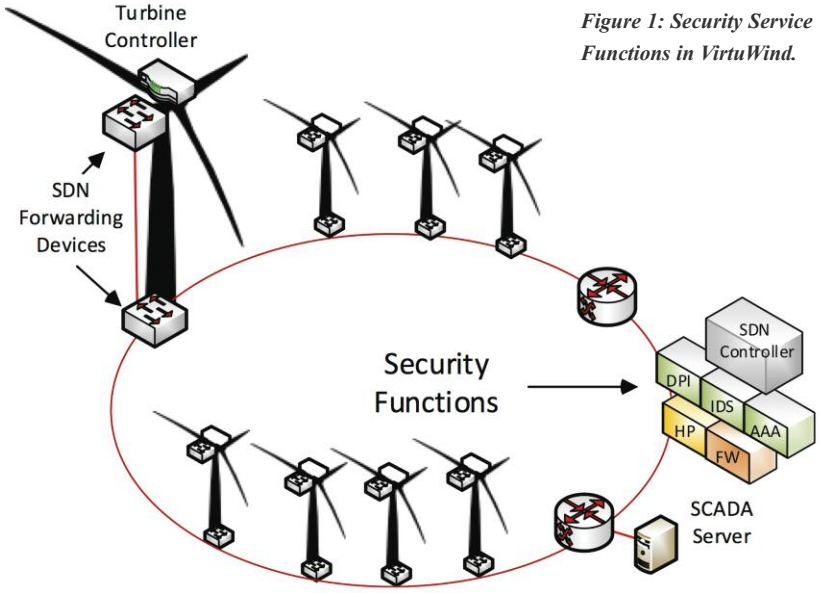

Figure 1: Security Service Functions in VirtuWind.

for north-/southbound and inter-controller interfaces, securing the controller can prevent adversaries from applying Denial of Service (DoS) attacks. Design principles followed by VirtuWind will guarantee that secure communication for all interfaces (north-/south-/east-/west-/bound) is possible. The communication channel between each SDN layer will be well protected (e.g., OpenFlow protocol is protected by Transport Layer Security (TLS)). Security measure techniques such as secure coding, deployment of integrity checks, and most importantly, application digital signing, will be used. Moreover, all communication channels can be hardened using TLS security.

Incident Detection Analysis and Prevention

The development of intra- and inter-domain incident detection mechanisms including real-time detection, analysis and prevention is necessary for the trace-backs and audits enhancing root cause analysis during incident response, and failure analysis mechanisms. To achieve this objective, VirtuWind will deploy network monitoring and intrusion detection for identification of attacks and run-time network adaptation for attack response and mitigation mechanisms. Mechanisms such as firewalls (FW), intrusion detection systems (IDS) and deep packet inspection systems (DPI) should be in place to detect malicious activity on the SDN, assess its impact, and evaluate the system's response and attack mitigation effectiveness. The intrusion detection mechanism will be also based on 'honeypot' (HP) technology that can visualise and show in real-time the attacks in the inter-domain SDN. Application, control and data plane should feature the appropriate elements (e.g., dummy devices) and interfaces (e.g., supporting mirroring and redirect traffic) to enable the deployment of data and/or control plane SDN honeypots and the backend assessment of the information they aggregate.

VirtuWind project is one of the 5G-PPP phase-1 Innovation Action projects under the Horizon 2020 framework. This three-year project commences on 1st July, 2016. The VirtuWind consortium consists of strong industry (Siemens, NEC, Deutsche Telecom, Intel, Intracom, WorldSensing) and academic partners (FORTH (ERCIM member), Kings College London, Technical University Munich) covering the whole value chain of programmable networks. The consortium is striving for a common vision of creating industrial capability of SDN/NFV in Europe.

Link:
http://www.virtuwind.eu

References:
[1] N. Petroulakis et al.: "VirtuWind: Virtual and Programmable Industrial Network Prototype Deployed in Operational Wind Park", EUCNC 2016
[2] Threat Landscape and Good Practice Guide for Software Defined Networks/5G, ENISA 2016

Please contact:
Ioannis Askoxylakis
ICS-FORTH, Greece
asko@ics.forth.gr