iot

Sponge-Based Control-Flow Protection for IoT Devices

Embedded devices in the Internet of Things (IoT) face a wide variety of security challenges. For example, software attackers perform code injection and code-reuse attacks on their remote interfaces, and physical access to IoT devices allows to tamper with code in memory, steal confidential Intellectual Property (IP), or mount fault attacks to manipulate a CPU's control flow. In this work, we present Sponge-based Control Flow Protection (SCFP). SCFP is a stateful, sponge-based scheme to ensure the confidentiality of software IP and its authentic execution on IoT devices. At compile time, SCFP encrypts and authenticates software with instruction-level granularity. During execution, an SCFP hardware extension between the CPU's fetch and decode stage continuously decrypts and authenticates instructions. Sponge-based authenticated encryption in SCFP yields fine-grained control-flow integrity and thus prevents code-reuse, code-injection, and fault attacks on the code and the control flow. In addition, SCFP withstands any modification of software in memory. For evaluation, we extended a RISC-V core with SCFP and fabricated a real System on Chip (SoC). The average overhead in code size and execution time of SCFP on this design is 19.8% and 9.1%, respectively, and thus meets the requirements of embedded IoT devices.  
 **main\_author: Stefan Mangard**  
 **published\_date: 2018-02-19 16:28:48+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.06691v1*

Machine learning for Internet of Things data analysis: A survey

Rapid developments in hardware, software, and communication technologies have allowed the emergence of Internet-connected sensory devices that provide observation and data measurement from the physical world. By 2020, it is estimated that the total number of Internet-connected devices being used will be between 25 and 50 billion. As the numbers grow and technologies become more mature, the volume of data published will increase. Internet-connected devices technology, referred to as Internet of Things (IoT), continues to extend the current Internet by providing connectivity and interaction between the physical and cyber worlds. In addition to increased volume, the IoT generates Big Data characterized by velocity in terms of time and location dependency, with a variety of multiple modalities and varying data quality. Intelligent processing and analysis of this Big Data is the key to developing smart IoT applications. This article assesses the different machine learning methods that deal with the challenges in IoT data by considering smart cities as the main use case. The key contribution of this study is presentation of a taxonomy of machine learning algorithms explaining how different techniques are applied to the data in order to extract higher level information. The potential and challenges of machine learning for IoT data analytics will also be discussed. A use case of applying Support Vector Machine (SVM) on Aarhus Smart City traffic data is presented for a more detailed exploration.  
 **main\_author: Amit P. Sheth**  
 **published\_date: 2018-02-17 22:37:17+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.06305v1*

Smart Asset Management for Electric Utilities: Big Data and Future

This paper discusses about future challenges in terms of big data and new technologies. Utilities have been collecting data in large amounts but they are hardly utilized because they are huge in amount and also there is uncertainty associated with it. Condition monitoring of assets collects large amounts of data during daily operations. The question arises "How to extract information from large chunk of data?" The concept of "rich data and poor information" is being challenged by big data analytics with advent of machine learning techniques. Along with technological advancements like Internet of Things (IoT), big data analytics will play an important role for electric utilities. In this paper, challenges are answered by pathways and guidelines to make the current asset management practices smarter for the future.  
 **main\_author: Mart A. M. M. van der Meijden**  
 **published\_date: 2017-06-18 14:59:06+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1706.09711v2*

High Speed SRT Divider for Intelligent Embedded System

Increasing development in embedded systems, VLSI and processor design have given rise to increased demands from the system in terms of power, speed, area, throughput etc. Most of the sophisticated embedded system applications consist of processors, which now need an arithmetic unit with the ability to execute complex division operations with maximum efficiency. Hence the speed of the arithmetic unit is critically dependent on division operation. Most of the dividers use the SRT division algorithm for division. In IoT and other embedded applications, typically radix 2 and radix 4 division algorithms are used. The proposed algorithm lies on parallel execution of various steps so as to reduce time critical path, use fuzzy logic to solve the overlap problem in quotient selection, hence reducing maximum delay and increasing the accuracy. Every logical circuit has a maximum delay on which the timing of the circuit is dependent and the path, causing the maximum delay is known as the critical path. Our approach uses the previous SRT algorithm methods to make a highly parallel pipelined design and use Mamdani model to determine a solution to the overlapping problem to reduce the overall execution time of radix 4 SRT division on 64 bits double precision floating point numbers to 281ns. The design is made using Bluespec System Verilog, synthesized and simulated using Vivado v.2016.1 and implemented on Xilinx Virtex UltraScale FPGA board.  
 **main\_author: Sachin Gajjar**  
 **published\_date: 2018-02-17 05:20:34+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.06195v1*

A Reputation-based Stackelberg Game Model to Enhance Secrecy Rate in Spectrum Leasing to Selfish IoT Devices

The problem of cooperative spectrum leasing to unlicensed Internet of Things (IoT) devices is studied to account for potential selfish behavior of these devices. A distributed game theoretic framework for spectrum leasing is proposed where the licensed users can willingly lease a portion of their spectrum access to unlicensed IoT devices, and in return the IoT devices provide cooperative services, firstly to enhance information secrecy of licensed users via adding intentional jamming to protect them from potential eavesdroppers, and secondly to enhance the quality of communication through cooperative relaying. The cooperative behavior of the potentially selfish IoT devices is monitored using a reputation-based mechanism to enable the primary users to only interact with the reliable IoT devices. The simulation results show that using the proposed reputation-based method enhances the secrecy rate of the primary users by reducing the possibility of attacks from selfish IoT devices. Hence, this model can offer a practical solution for spectrum leasing with mobile IoT devices when assuring the required quality of communication and information secrecy for the spectrum owners.  
 **main\_author: Charles Kamhoua**  
 **published\_date: 2018-02-16 04:21:17+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.05832v1*

Security and Privacy Approaches in Mixed Reality: A Literature Survey

Mixed reality (MR) technology is now gaining ground due to advances in computer vision, sensor fusion, and realistic display technologies. With most of the research and development focused on delivering the promise of MR, there is only barely a few working on the privacy and security implications of this technology. This survey paper aims to put in to light these risks, and to look into the latest security and privacy work on MR. Specifically, we list and review the different protection approaches that have been proposed to ensure user and data security and privacy in MR. We extend the scope to include work on related technologies such as augmented reality (AR), virtual reality (VR), and human-computer interaction (HCI) as crucial components, if not the origins, of MR, as well as a number of work from the larger area of mobile devices, wearables, and Internet-of-Things (IoT). We highlight the lack of investigation, implementation, and evaluation of data protection approaches in MR. Further challenges and directions on MR security and privacy are also discussed.  
 **main\_author: Aruna Seneviratne**  
 **published\_date: 2018-02-15 23:33:45+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.05797v1*

ICN enabling CoAP Extensions for IP based IoT devices

The Constrained Application Protocol (CoAP) and its extensions, such as observe and group communication, offer the potential for developing novel IoT applications. However, a full-fledged CoAP-based application requires delay-tolerant communication and support for multicast: since these properties cannot be easily provided by existing IP networks, developers cannot take full advantage of CoAP, preferring to use HTTP instead. In this demo we show how proxying CoAP traffic over an ICN network can unleash the full potential of CoAP, simultaneously shifting overhead and complexity from the (constrained) endpoints to the network.  
 **main\_author: Eero Hakala**  
 **published\_date: 2018-02-14 16:44:01+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.05198v1*

Virtualized Control over Fog: Interplay Between Reliability and Latency

This paper introduces an analytical framework to investigate optimal design choices for the placement of virtual controllers along the cloud-to-things continuum. The main application scenarios include low-latency cyber-physical systems in which real-time control actions are required in response to the changes in states of an IoT node. In such cases, deploying controller software on a cloud server is often not tolerable due to delay from the network edge to the cloud. Hence, it is desirable to trade reliability with latency by moving controller logic closer to the network edge. Modeling the IoT node as a dynamical system that evolves linearly in time with quadratic penalty for state deviations, recursive expressions for the optimum control policy and the resulting minimum cost value are obtained by taking virtual fog controller reliability and response time latency into account. Our results indicate that latency is more critical than reliability in provisoning virtualized control services over fog endpoints, as it determines the swiftness of the fog control system as well as the timeliness of state measurements. Based on a realistic drone trajectory tracking model, an extensive simulation study is also performed to illustrate the influence of reliability and latency on the control of autonomous vehicles over fog.  
 **main\_author: Mung Chiang**  
 **published\_date: 2017-11-30 22:02:14+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1712.00100v2*

Smart Contract-Based Access Control for the Internet of Things

This paper investigates a critical access control issue in the Internet of Things (IoT). In particular, we propose a smart contract-based framework, which consists of multiple access control contracts (ACCs), one judge contract (JC) and one register contract (RC), to achieve distributed and trustworthy access control for IoT systems. Each ACC provides one access control method for a subject-object pair, and implements both static access right validation based on predefined policies and dynamic access right validation by checking the behavior of the subject. The JC implements a misbehavior-judging method to facilitate the dynamic validation of the ACCs by receiving misbehavior reports from the ACCs, judging the misbehavior and returning the corresponding penalty. The RC registers the information of the access control and misbehavior-judging methods as well as their smart contracts, and also provides functions (e.g., register, update and delete) to manage these methods. To demonstrate the application of the framework, we provide a case study in an IoT system with one desktop computer, one laptop and two Raspberry Pi single-board computers, where the ACCs, JC and RC are implemented based on the Ethereum smart contract platform to achieve the access control.  
 **main\_author: Jianxiong Wan**  
 **published\_date: 2018-02-13 00:42:31+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.04410v1*

Musical Chair: Efficient Real-Time Recognition Using Collaborative IoT Devices

The prevalence of Internet of things (IoT) devices and abundance of sensor data has created an increase in real-time data processing such as recognition of speech, image, and video. While currently such processes are offloaded to the computationally powerful cloud system, a localized and distributed approach is desirable because (i) it preserves the privacy of users and (ii) it omits the dependency on cloud services. However, IoT networks are usually composed of resource-constrained devices, and a single device is not powerful enough to process real-time data. To overcome this challenge, we examine data and model parallelism for such devices in the context of deep neural networks. We propose Musical Chair to enable efficient, localized, and dynamic real-time recognition by harvesting the aggregated computational power from the resource-constrained devices in the same IoT network as input sensors. Musical chair adapts to the availability of computing devices at runtime and adjusts to the inherit dynamics of IoT networks. To demonstrate Musical Chair, on a network of Raspberry PIs (up to 12) each connected to a camera, we implement a state-of-the-art action recognition model for videos and two recognition models for images. Compared to the Tegra TX2, an embedded low-power platform with a quad-core CPU and a GPU, our distributed action recognition system achieves not only similar energy consumption but also twice the performance of the TX2. Furthermore, in image recognition, Musical Chair achieves similar performance and saves dynamic energy.  
 **main\_author: Hyesoon Kim**  
 **published\_date: 2018-02-05 19:32:35+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1802.02138v2*