CIS-TC Newsletter

Communications and Information Security Technical Committee

http://cis.committees.comsoc.org/

Issue 5 – December 2019

cistc@comsoc.org

http://cis.committees.comsoc.org/newsletters

Contents

Message from The Chair

Welcome to the December issue of CIS-TC Newsletter!

This is the third issue of our newsletter. It is established as a mean to share important information with the members of CIS Technical Committee and to have some brief contact approximately every semester. We hope that it is a useful communication tool.

Contributions are open for everybody. Please feel free to send us any piece of news that you believe can be of interest to our technical committee.

During 2019, we started three Interest groups: - IoT cyber security, - Security in 5G and - Security in blockchains. You are welcome to participate to these groups and contribute to the topics.

Christmas is approaching and hence, holidays is coming. While you enjoy your time with family and friends, I hope you will be able to spend some time in reading our December Issue. It is an entirely fresh perspective and a new look and really exciting when reading through it. Thanks to our newsletter Editor-in-Chief, Dr. Francesco Chiti, for his effort and dedicated time to realize this issue. Also, you may notice that many parts of our newsletter are waiting for more input and updates from you to make our newsletter look better. On behalf of CIS-TC officers, best wishes to you, your families and friends for a healthy and joyful holiday season and a prosperous.

Sincerely,
Abderrahim Benslimane
Chair of CIS-TC

Technical Recognition Award 2019

The Committee decided to give the CIS-TC Technical Recognition Award 2019 to Professor for Prof. Bhavani Thuraisingham at the University of Texas at Dallas, (USA), for her contributions in data mining for network security.

Prof. Thuraisingham has been awarded and will receive her plaque at the CIS-TC meeting held at IEEE Global Communications Conference on December 12,2019 in Waikoloa, HI, USA.

Prof. Bhavani Thuraisingham is the Founders Chair Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at The University of Texas at Dallas (UTD). She is an elected Fellow of several prestigious organizations including ACM, IEEE, the AAAS, National Academy of Inventors and the British Computer Society. She has received prestigious awards in

cybersecurity including the IEEE Computer Society's 1997 Technical Achievement Award for "outstanding and innovative contributions to secure data management", the 2010 ACM SIGSAC Outstanding Contributions Award for "seminal research contributions and leadership in data and applications security", and a 2013 IBM Faculty Award in Cyber Security. She has a unique experience working in the commercial industry (Honeywell), a federal research laboratory (MITRE), US government (NSF) and academia and her 38-year career includes research and product development, technology transfer, program management, and consulting. Her work has resulted in 120+ journal and 300+ conference papers, 130+ keynote and featured addresses, and 6 US patents. She has authored 15 books and edited 12 more. She was educated in the United Kingdom and received the prestigious earned a higher doctorate (Doctor of Engineering) from the University of Bristol, England for her published research in data security since her Ph.D. She is a STEM mentor to women and minorities and has given talks at SWE, WITI, WiDS, WiCyS, and CRA-W. She serves on multiple advisory boards and has been a software consultant to the US Dept. of Treasury since 1999.

Featured Topics

"Secure Data Science: Integrating Cyber Security and Data Science"

Bhavani Thuraisingham [1]

[1]University of Texas at Dallas, (USA),

My research over the past 34 years has been on integrating cyber security and data science including applying data mining/data science for cyber security problems such as network intrusion detection and securing data science techniques such as adversarial machine learning.

With respect to data mining for cyber security, together with my team we designed and developed new data mining algorithms and demonstrated that the novel class detection technique that we developed can be effectively utilized for finding brand new or emerging class/patterns in streaming data and applied it to intrusion detection, insider threat detection, and website fingerprinting. This work has provided the directions for handling the zero-day attacks.

With respect to securing the data mining techniques we developed Adversarial Machine Learning techniques since the stream data mining techniques themselves may be attacked. Our goal is to thwart the adversary since the adversary is trying to figure out the data mining models, we are using, and we adapt our models. Over time the adversary learns our adapted data mining approaches and eventually it becomes a game played between us and the adversary.

In addition to applying data mining/machine learning for network security problems and securing the data mining techniques, we have also focused on analyzing and securing social networks. In particular, we designed and developed access control models for social networks based on semantic web technologies as well as designed and developed a machine learning system called InXite that analyzes social network data to determine cyber-attacks on the social networks as well as determine suspicious events.

I believe that as more progress is made on analyzing massive amounts of data and we learn more about the types of attacks on networks, we have the opportunity to solve challenging problems in secure data science.

Forthcoming Meeting

The next IEEE ComSoc's Communication & Information Security TC (CISTC) meeting will be held at IEEE ICC 2020, 7-11 June 2020, Dublin, Ireland.

CIS-TC Newsletter
Communications and Information Security Technical Committee
http://cis.committees.comsoc.org/

SCANNING THE WORLD

"Securing IoT: Benefits and Challenges of SDN Approach"

Luca Barletti, Michele Bonanni, Francesco Chiti, Tommaso Pecorella, Roberto Picchi, Adnan Rashid, Federico Raspini[1]

[1]University of Florence, Italy

IoT Features

Internet of Things (IoT) also known as the Internet of *Objects* is a system of interrelated computing devices, mechanical and digital machines, animals or people, directly or indirectly connected to the human daily life, as shown in Figure 1. They provide unique identification and ability to generate and transfer data over the Internet, without requiring human-to-human or human-to-computer interaction. Above all, their use in industry represents a shift that increase the productivity, which is directly connected to the economy of the state.

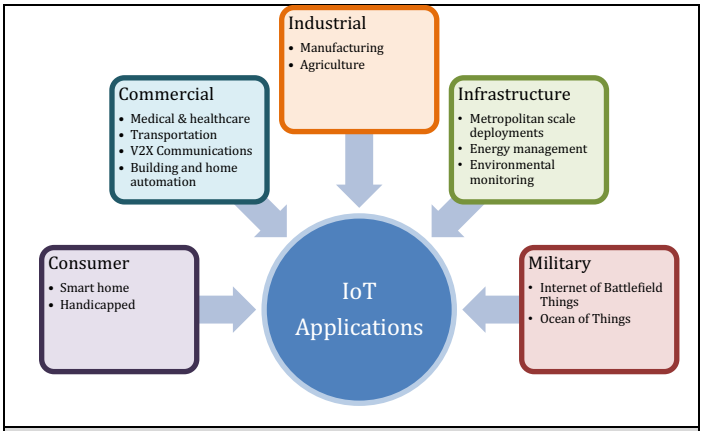

Figure-1: IoT Applications

Connectivity of these heterogeneous devices is considered to be the next big opportunity, and challenge, for the Internet engineering community, users of technology, companies, and society. IoT is primarily driven by deeply embedded devices, which are usually low-bandwidth, low-repetition data capture and low-bandwidth data-usage appliances that communicate with each other and provide data via user interfaces. Connecting things to the Internet yields many problems like scalability, manageability, controllability, flexibility, availability and, above all, security. However, ITU-T Y.2060 reference model introduced new dimensions on IoT in terms of any time/place/thing connections, where security considerations became the focus of consumers.

Securing these objects and their data in large scale and distributive way is very challenging and preserving information security on the shared data is an important issue that cannot be neglected. Like conventional networks, the essential security requirements (confidentiality, authenticity, integrity, accountability, and availability) are also mandatory for the IoT systems. Figure 2 shows the main elements of interest for IoT security and several typical scenarios for interconnection and the inclusion of security features.

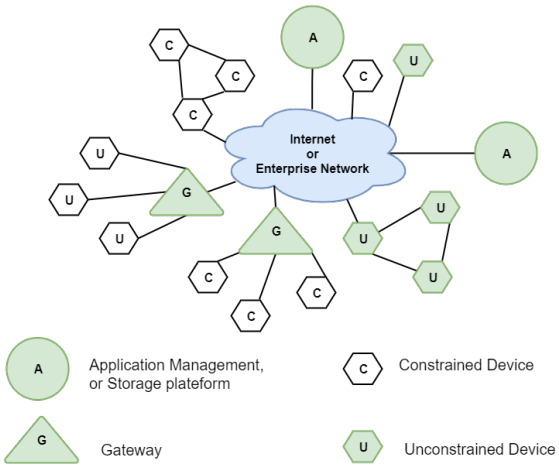

Figure-2: Elements of Interest in The Contexts of IoT Security

Application platforms, data storage servers, and network and security management systems are shown at the core of the network topology. These central systems gather data from sensors, send control signals to actuators, and are responsible for managing the IoT devices and their communication networks. At the network edge IoT-enabled devices are present, usually quite simple *constrained* devices, while some of which are more intelligent *unconstrained* devices. Protocol conversion and other networking services on behalf of IoT devices are the conventional jobs of *gateways*. Shading devices indicates the systems is secure, Typically, gateways implement secure functions, such as TLS and IPsec. Unconstrained devices may or may not implement some security capability. Constrained devices generally have limited or no security features. However, any constrained or unconstrained device attached to the gateway are outside the secured zone established between the gateway and the central systems. Unconstrained devices can communicate directly with the center and support security functions. However, constrained devices that are not connected to gateways have no secure communications with central devices.

IoT is perhaps the most complex and unexplored area of network security. The reason is that the chip manufacturers have incentives to produce their products with firmware and software as quickly and cheaply as possible. Their focus is on the functionality of the device itself, not the security features because it increases the cost of the device. The end-user may have no or limited means of patching the system. The result is that the hundreds of millions of Internet-connected

devices in the IoT are *vulnerable* to attack. This is certainly a problem with sensors, allowing attackers to insert false data into the network. It is potentially a graver threat with actuators, where the attacker can affect the operation of machinery and other devices.

IoT Attacks

A standard architecture design for IoT is still an open issue, but, several international organizations, such as the International Telecommunication Union, IEEE, to name a few, are actively engaged in the development and standardization of IoT. In a general perspective, a layered architecture compromised on four layers is commonly assumed, as shown in Figure 3.

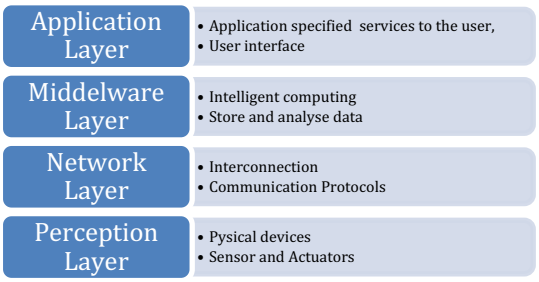

Figure-3: General IoT Architecture

If we compare this layered architecture with TCP/IP stack, we can point out the similarities between them, thus same traditional security threats are also possible to IoT. Conventional threats especially to the perception layer (Physical layer of TCP/IP stack) can exploit the whole IoT network due to the insecure installation of sensors and actuators, moreover the lack of security provided to such devices by the manufacturers.

IoT Layers	Security Issues/Attacks
Application Layer	Data access and security authentication issues, data protection and recovery problems, spear-phishing attack, software vulnerabilities, attacks on reliability and clone attack.
Middleware Layer	Making intelligent decision processing huge data, malicious-code attacks, multi-party authentication, handling suspicious information.
Network Layer	Cluster security problems, dos attacks, spoofed, altered or replayed routing information.
Perception Layer	Node capture, fake node, mass node authentication, cryptographic algorithm, and key management mechanism.

SDN Security

Software-defined networking (SDN) is one of the main research area in recent years, allowing network administrators to control and manage the network routers remotely through specific commands and programming. SDN has been typically applied to infrastructure-based networks, where controlling is generally easy due to the static positioning of network nodes. In the case of the Internet of Things (IoT), devices have multiple interfaces, low energy of devices, Interference, security and ubiquity of diver's networks are very challenging.

The decoupling of the Control Plane (CP) from the Data Plane (DP) represents the foundation of the Software-Defined Networking (SDNing). Moreover, the concept of the SDN is more suited for stable and fixed networks, instead of intermittent networking. The interface between the DP and CP are developed by different organizations and research groups, provided only over well-known transport security, while typical *Wireless* Sensor Networks devices rely on IEEE 802.15.4 MAC layer security. Although SDN gives privileges to network administrators to solve top-level security problems it also opens two types of threats; e.g., to Application Plane (AP), CP and DP or to interfaces between layers, i.e., *north*, *south*, and *east*/*west*-bound ones.

Although there is an ongoing arms race between attackers and defenders, it is possible to build a powerful security facility for traditional networks and for SDN/NFV networks. The sudden explosion of IoT networks with millions to billions of devices poses an unprecedented security challenge. Different models and frameworks produced by different standard organizations can serve as a foundation for the design and implementation of an IoT security facility.

University of Florence is presently involved in several projects related to the above-mentioned technologies and protocols, among which a couple is particularly relevant, as below described.

HYDROCONTROLLER Project

This project funded by the Tuscany Region, aims at the design and develop of an automated secure IT platform for the real-time monitoring and prediction of water resources on hydrologic basins for electrical power generation in a dam. The platform is made up of heterogeneous networks as well as heterogeneous input data, e.g., integrating satellite observation data, forecasting data, and data coming from a wide area ad-hoc network.

Currently, different systems are available in the market, but they are specialized in specific functions with certain operative conditions, for example, to prevent hydrological risks, or to optimize the use of the water resource timely. In addition, they are not interoperable: for instance, systems for monitoring a river basin do not usually take account of the weather conditions; similarly, systems to prevent environmental risk are not aware of the soil structure. Moreover, they are not scalable and reliable. Therefore, the proposed approach aims at automatically and on-demand integrating these components into a flexible framework.

There are three major components involved in the HYDROCONTROLLER platform: (i) Sensor Monitoring Equipment in situ, (ii) Satellite and

weather data assimilation models and (iii) The automated management telecommunication module.

In this perspective, the application of SDN principles over Cloud/Fog domains presents a great potential for the information service innovation, and, accordingly, HYDROCONTROLLER project adopted this vision to achieve the main goals are summarized below:

- the overall system can be locally and remotely accessed and controlled through public IP (LAN and WAN)
- the common Wireless Personal Area Network (WPAN), functionalities (routing, management, and security) are empowered
- the security requirements for the entire network, from sensors/actuators in IEEE 802.15.4 based WPAN, within the water basin area, up to the server in Cloud/Fog domains are better defined and real-time managed, without while providing effective security mechanisms at the device level as well as network level
- the robustness and the availability of the HYDROCONTROLLER IT platform are increased.

Slide-Sense Project:

In this project, the design, development, and testing of an integrated IoT platform is addressed, to environmental monitoring application, with a special focus on emergency situations involving ground subsidence, and landslides in urban and sub-urban scenarios. This pose the foundation of the so called *Internet of Geology* (IoG), where we adopted the SDN and Network Function Virtualization (NFV) approaches in a Fog/Edge processing architecture over an *in situ* WSN to achieve (1) adaptability and reconfigurability of the overall topology (2) interoperability with classic satellite synthetic aperture radar (SAR) monitoring to prevent hydrogeological risks.

Specifically, we rely on a distributed group position processing and refinement oriented to a P2P paradigm, where each differential GPS sensor is able to communicate with a subset of nodes, dynamically selected basing on a network assigned *reputation*, which allows to cope with device outage, fault and even unavailability due to attacks.