정 보 보 호 학 회 지
제26권 제6호, 2016. 12

Cyber Security Approaches for Industrial Control Networks

C. Dillabaugh*, B. Nandy*, N. Seddigh*, K. Wong*, Byoung-Joon (BJ) Lee**

Abstract

Critical infrastructure (CI) such as the electrical grid, transportation systems and water resource systems are controlled by Industrial Control and SCADA (Supervisory Control and Data Acquisition) networks. During the last few years, cyber attackers have increasingly targeted such CI systems. This is of great concern because successful attacks have wide ranging impact and can cause widespread destruction and loss of life. As a result, there is a critical requirement to develop enhanced algorithms and tools to detect cyber threats for SCADA networks. Such tools have key differences with the tools utilized to detect cyber threats in regular IT networks. This paper discusses key factors which differentiate network security for SCADA networks versus regular IT networks. The paper also presents various approaches used for SCADA security and some of the advancements in the area.

Ⅰ. Introduction

The term SCADA (Supervisory Control and Data Acquisition) is used to describe Industrial Control System (ICS) networks. We note that SCADA systems themselves are but one element in a full ICS network. However, since the term is broadly used to reference such networks we will follow the same convention in this paper.

Industrial Control Systems (ICS) refer to the networked equipment and software controlling and monitoring industrial systems. Such systems can be found in a diversity of critical infrastructure industries including gas, chemical, transportation, electrical, water, wastewater and oil. The systems may be localized, as in the case of a manufacturing facility, or highly distributed, as in the case of an oil or gas pipeline or electrical grid.

Historically, proprietary technologies were utilized for SCADA network. This proprietary nature greatly assisted in their security – a factor sometimes referred to as “security by obscurity”. The standardization of various elements of ICS networks in recent years combined with the increased connection of these systems to WAN (Wide Area Networks), Enterprise Networks and the Internet, has opened up access to such networks. While this opening up of ICS networks has many benefits, it has exposed and created a number of security issues which were previously not evident. The specialized protocols used to control ICS devices such as PLCs (Programmable Logic Controllers) were not designed with security in mind, leaving them susceptible to cyber security threats. Further the security tools and network architectures used in SCADA networks have not been subject to the same security design rigour as their counterparts in IT networks. The absence of security design rigour can be attributed to the previous isolation of SCADA networks. This is unlike IT networks which were earlier subjects of malicious cyber threats and which therefore had to develop security solutions early and rapidly.

* Solana Networks ({cdillabaugh, bnandy, nseddigh, kwong}@solananetworks.com)
** Creatrix Design Group (bjlee@creatrix.ca)

While SCADA networks have similarities to IT networks, they also have certain distinctive characteristics. The result is that traditional IT security architectures, products and solutions cannot be used as-is on a SCADA network. Specialized cyber security tools are required which are ICS or SCADA-aware.

This paper is organized as follows. In section 2 we outline differences of SCADA networks from regular IT networks and analyze the related security implications. Section 3 discusses various SCADA network security technologies and associated tools. Section 4 outlines some of the recent advancements in SCADA security technologies.

Ⅱ. Security Issues in SCADA Networks

Industrial control systems consist of specialized hardware and software including for example Programmable Logic Controllers (PLCs), Distributed Control Systems (DCSs), and Supervisory Control and Data Acquisition (SCADA) systems [4], [11]. PLCs are rugged low-cpu/memory computers which control industrial processes and which form the core of ICS networks. DCSs are fully automated systems controlling the operation of processes within an industrial facility, and are sometimes called Process Control Systems (PCS).

Schematic of a SCADA network.

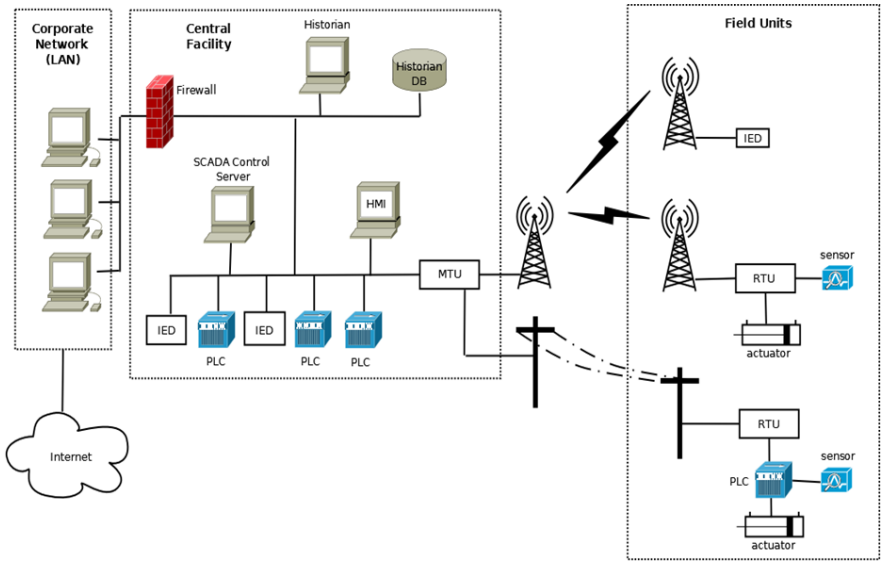
SCADA networks differ from traditional corporate networks in a number of ways. These differences present a number of challenges in the quest to defend the network against cyber threats – malicious, criminal or otherwise.

The specialized communication protocols utilized for ICS networks were designed for closed networks to achieve the goals of speed and reliability needed by these systems. The SCADA protocols were designed with operational considerations, rather than security considerations being the driving force behind their design. To achieve security within ICS networks a key consideration is that the systems should operate, to the degree possible, as closed systems. A standard security practice is to use air gaps to separate control systems from other parts of the network. An air gap refers to a physical disconnection between the control system and the rest of the ICS network [13]. However as show in Figure 1 there are connections between the SCADA subsystem and the control systems, and the SCADA system may be connected to the corporate network, which in turn is connected to the internet.

Air gaps are achieved in practice by the use of firewalls and data diodes. Data diodes restrict the flow of network traffic to one direction (for example from control network to the central SCADA system). However, if the central SCADA system does include control elements there is sometimes a need for traffic to flow in the other direction. Firewalls are also employed, to restrict the types of traffic passing between the supervisory network and the control systems. Improperly configured, or defective data diodes and firewalls both represent a possible security hole.

A number of specialized protocols have been developed, often for historical reasons, which are used exclusively within SCADA networks. Some of the more popular protocols include Modbus, DNP3, Profinet, EtherNet/Ip (not to be confused with either the Ethernet or IP protocols). These protocols, some of which are quite old, have not necessarily been designed with security in mind. Furthermore as they are niche protocols, popular network security tools such as signature-based IDS (Intrusion Detection Systems) such as Snort, Suricata or Bro have limited or no support for many of these protocols.

Another aspect of ICS networks is that equipment, and technologies have a longer life within these networks. Comparatively, operating systems are upgraded and patched more frequently in traditional



〔Fig. 1〕 Schematic of a SCADA network

IT networks and hardware is replaced more often. This situation is to be expected given that the systems involved in ICS networks are controlling complex, operational systems. Knapp [13] reported that the average number of days between the public disclosure of a security vulnerability, and the discovery of the same vulnerability in a control system, was almost a full year. The life cycle of PLCs may be several times longer than that of the computer equipment used to host the SCADA supervisory systems – which are typically standard PCs [4]. Thus even though newer protocols may be developed with greater consideration to security matters, the need to support legacy hardware, which may not understand newer protocols means that vulnerabilities persist. However, even some modern PLCs include documented features that would present serious vulnerabilities should a malicious intruder somehow gain the ability to communicate directly with the device [14].

The traffic characteristics of SCADA networks also differ significantly from traditional IT networks. Most of the traffic in SCADA networks is generated by devices which control and monitor the industrial processes. Such communications are often based on timers and occur at regular intervals, and between the same hosts within the network. Thus the pattern of communications is relatively deterministic and periodic in nature. This is quite different compared to network traffic on an IT network which is generated by human beings and which can be quite noisy and non-deterministic in nature.

One of the key methods to ensure good security in ICS networks, as with regular IT networks, is to use a defense-in-depth approach. In an ICS network this includes such strategies as dividing the network into functional enclaves and minimizing, or eliminating altogether, unnecessary communications between those enclaves[13]. However, this approach also requires careful monitoring of the network and traffic on the network within the network's outer defenses, using tools such as Intrusion Detection Systems.

A final aspect in developing network security tools for SCADA networks is the difficulty in obtaining either real, or realistic, SCADA network traffic. The systems they monitor are large and complex. The operators of these systems are reluctant both for business and security reasons, to share their network traffic data with outside researchers. As a result researchers rely on simulated SCADA traffic, small

scale testbeds or traffic traces for their experimental evaluation. The vast majority of research into SCADA network security has been conducted using simulated or testbed data, although in recent years a few studies have appeared where the authors were able to obtain traffic captures from real SCADA networks including [2],[5] and[6].

We note that the above discussion considers SCADA security issues from cyber-threats, as opposed to physical threats which are certainly a concern, but outside the scope of this paper.

Security risks in ICS network are more than just potentially sensitive data loss and embarrassment for authorities. Any security breach in ICS network could conceivably damage industrial infrastructure or be a threat to human life.

Ⅲ. SCADA Network Security Technologies

In this Section we identify various network security technologies that are commonly used to protect SCADA networks from cyber attacks. Some of these tools are widely used at regular IT networks. These tools have been extended to address security issues in SCADA networks. Some of the categories of tools that are commonly used are:

1) Intrusion Detection System
2) Firewalls
3) Vulnerability scanners
4) Forensic tools
5) Log management software and host-based intrusion detection systems firewalls
6) Security Information and Event Management Systems (SIEMs)

Most of the widely used Intrusion Detection Systems (IDSs) are open source. These systems almost exclusively rely on signature based threat detection in which network packets are examined to find traffic which matches the signature of known threats. Due to the niche market for SCADA protocols, coupled with the reluctance of SCADA operators to share data and information on attacks, IDS support for SCADA protocols lags behind support for more commonly used protocols. Such systems lack both extensive libraries of signatures, and base support for decoding the protocols themselves. Three most widely deployed IDS systems are Snort[8], Suricata[9] and Bro[10]. Snort is the oldest, most proven open source Network Intrusion Detection System (NIDS). It has a user base of nearly 400,000 people and is well documented for Windows, many Linux variants, and the BSDs. Suricata is a relatively new and scales well with faster traffic. The project is partly funded by the Department of Homeland Security's Directorate for Science and Technology and is designed to work with the Snort rule sets. Bro is a passive, open-source network traffic analyzer. It is primarily a security monitor that inspects all traffic on a link in depth for signs of suspicious activity.

Snort currently has built in preprocessors for Modbus, DNP3 and EtherNet/IP. A pre-processor is important for complex protocols like EtherNet/IP. Also, preprocessor is desirable because in the absence of such attackers can use packet fragmentation to defeat the signature matching engines. Snort has signatures available for these three protocols as well since 2012. Suricata has support for Modbus and DNP3 development underway. Very recently Solana Networks [24] has developed preprocessor and other support for Ethernet/IP protocol in Suricata. Bro has support for Modbus and DNP3 protocols. The Quickdraw[12] package provides a large number of Snort rules that can be used by Snort and Suricata. All three IDSs have some SCADA capability and more support are added in recent years.

The purpose of a firewall is to analyze the packet headers of traffic entering a network, or subnet, and applying filtering policies, and possibly restricting traffic based on source or destination IP address, source or destination port, or protocols. Firewalls are

available either as specialized network appliances or wholly in software. There are a number of vendors who develop specialized Firewalls for SCADA networks, these include Tofino Security[15] and Secure Crossing[16]. Devices by these companies support a wide range of SCADA protocols, including Modbus, DNP3, EthernetIP, IEC 61850, Profinet, BACnet and ICCP.

Vulnerability scanners are software that can probe network devices to discover security vulnerabilities of devices attached to the network, such as PLCs. Vulnerability scanners may perform actions such as performing port scans on a system to determine which ports are open. Scanners may also interact directly with the host OSs to extract security information including things such as open ports, password policies, and patch levels for the operating systems. Examples of such tools include the Nessus vulnerability scanner and Passive Vulnerability Scanner (PVS), both commercial products available from Tenable[17]. The later product performs passive network monitoring to build a list of network communication pairs, including protocols used in communication with specific devices on the network. Nessus provides more traditional vulnerability scanning options. Both products include components geared towards SCADA networks. The SCADA plugins were first introduced in 2006, and were added to in 2011 and 2012, so that there are now almost 180 plugins for various SCADA devices and protocols [18].

OpenVAS is an open source vulnerability scanner and management solution. The security scanner is accompanied by a daily updated feed of network vulnerability tests. The number of such tests exceeded 35,000 as of April, 2014 [19]. The core of the OpenVAS system is the OpenVAS Scanner, which executes the vulnerability tests. The OpenVAS Scanner is controlled by a second piece of software, the OpenVAS Manager which provides the system intelligence and backend database management. OpenVAS does not include any specialized SCADA support.

Forensic tools provide the ability to analyze attacks on computer network. The line between anti-virus software, intrusion detection, and forensic tools can be somewhat blurry. Products advertised as forensic tools may fall into the anti-virus or intrusion detection categories. The key distinguishing feature for a forensic tool is that they provide after the fact analysis of attacks. For network forensics, a common tool is to use a packet sniffer such as Wireshark (open source), which includes extensive support for SCADA protocols including Modbus, DNP3, EtherNet/IP and to some level ICCP [20]. Similar products like NetworkMiner (available on MS Windows host) also provides limited SCADA protocol support [21]. However the use of such tools presupposes the existence of network packet captures, which can be a challenge in SCADA networks. Network appliances that perform SCADA analysis for forensics also exist, such as the Norman SCADA Protection device by Norman ASA. A recent study by Ahmed et al. [3] concluded that research on SCADA system forensics has lagged behind research on SCADA security.

Log management/analysis systems are a very important component of an overall security system. The various services that run on a network all generate activity logs, monitoring these logs provides important system information and can be a means of detecting malicious activity on a network. Given the large number of logs generated on a single host alone, having a centralized log management system is essential to allow security personnel to monitor and analyze activity occurring on the network devices. There are many commercial log management products, with Splunk being perhaps the most popular, and many open source log management tools. Typically, these are not SCADA specific products, but can be used within SCADA networks. The OSSEC open source host-based intrusion

detection system includes, among other modules, a log analysis component [6].

Closely related to log management are full fledged Security Information and Event Management systems (SIEMs). SIEMs extend the capabilities of log management systems with specific analytical and contextual features [13]. The IDS and log management systems may be thought of as components of the SIEM, with the SIEM providing a means of managing these components. SIEMS may also provide modules for correlation analysis, which allows security officers to examine related events from the various monitoring systems in order to build a better understanding of a security incident. For example, an attack on the network may generate alerts from the IDS, but also cause events logged by the servers. Firewall logs may also give useful evidence of the exact nature of the attacks, since some of the traffic generated by the attack would never make it beyond the firewall, and therefore would be unavailable to the detection systems located within the network. By examining all these events together, the operator is able to get a more accurate picture of what has taken place, and potentially identify the source of the attack.

In the open source world the most popular SIEM tool is the OSSIM project. This project integrates a number of sensors, including the Snort IDS, OpenVAS vulnerability scanner, and OSSEC host based intrusion detection systems, plugins for popular anti-virus software, in addition to other components. While not geared specifically towards SCADA networks itself OSSIM [22] is part of AlienVault's ICS SIEM, which is a SIEM appliance targeted directly at the SCADA market. AlienVault is also the primary developer behind OSSIM.

Ⅳ. Recent Advancements in Attack Detection in SCADA Network Securities

There are two main approaches to detect cyber threats in IT and SCADA networks – signature/rule –based methods, and anomaly detection methods. The open source IDS systems described in the previous section typically utilize rule-based approaches. Rule based methods use known details about a particular cyber threat/attack to detect specific instances of traffic that match that particular attack. They essentially implement a pattern matching scheme where they maintain a database of known traffic patterns for each threat and examine packet headers/payload to match the patterns/signatures. Anomaly based methods typically utilize machine learning to build a model of normal traffic behaviour on the network and then monitor the traffic continuously, comparing it to the model/baseline. When the monitored traffic patterns deviate sufficiently from the baseline/normal behaviour, the traffic is marked as anomalous and warranting further investigation.

Certain aspects of SCADA network traffic makes such traffic a strong candidate for use in machine learning cyber threat detection. Such aspects include:

- Specialized (and somewhat obscure) protocols, with limited examples of real world traffic available for researchers, mean that signature rule based systems such as Snort and Suricata have limited coverage against the range of cyber threats.
- The deterministic nature of traffic patterns in SCADA networks mean that models characterizing the network traffic can be more easily formed than in traditional networks which have non-deterministic and noisy traffic.

Given the large number of protocols employed in SCADA systems we believed that methods which are independent of specific protocol knowledge (ie. deep packet inspection) would be the most promising for developing a good general purpose anomaly detection tool for SCADA networks.

A number of researchers have studied the use of flow whitelisting to determine valid vs invalid traffic

in SCADA networks. In one example, Barbosa [1] studied flow whitelists to characterize valid traffic in live SCADA networks. The approach used a learning phase and a monitoring phase. During the learning phase one challenge was to identify which host+port constituted the client and which the server. The whitelist contained entries for all flows observed during the learning phase. The anomaly detection method operates under two key assumptions:

- All flows observed during the learning period are legitimate traffic
- Most of the legitimate flows that will appear on the network will be observed during the learning phase.

This technique is more suitable for SCADA networks than traditional networks. In SCADA networks the size of the networks, and the number of flows occurring, is limited relative to corporate networks. Thus the size of the connection matrix is not expected to grow too large. During the detection phase any flow encountered that is not on the whitelist will result in an alarm being raised. It requires the ability of an administrator to add flows to the whitelist – in the event of false positives. For testing purposes data was obtained from a number of real world SCADA facilities

Based on our research Solana Networks developed a functioning prototype to enhance SmartFlow [23] product that detected cyber threats by applying anomaly detection against network flow traffic such as Sflow or Netflow. While anomaly detection methods can be applied to a range of data (including log files, raw packets, flows, active directory data, alerts) we found strong benefits in applying the methods to flow data. With an increasing number of switches and routers supporting xflow (Netflow, Sflow etc) it is more cost effective and operationally easier to enable multiple monitoring points in the network using xflow as opposed to packets.

Ⅴ. Conclusions

Security threats on ICS networks are real and any breach can cause damage to critical infrastructure. However, security tools for ICS networks are evolving and lag behind tools for regular IT networks. In most cases, regular security tools are enhanced or extended to suite ICS networks requirements. However, there is a gap since ICS networks are different from regular IP networks. There are opportunities to build more sophisticated cyber attack detection and prevention tools. For example, sophisticated and accurate IDS systems can be built based on anomaly detection of network traffic. These new class of tools will complement existing set of security tools.

One major roadblock in tool development in ICS networks is the lack of availability of real ICS traffic and threat vectors. This is evident from recent research publications. Most of the research results are based on synthetic network traffic. However, the problem will get addressed when owners of these critical infrastructures participate on these endeavors.

Acknowledgment

We acknowledge the discussions and effort by Frank Turbide and Paul O Brien in completing various aspects of this work. We also acknowledge that this work was carried out as part of a project with Public Safety Canada and Defence R&D Canada.

References

[1] Barbosa, Rafael Ramos Regis, Ramin Sadre, and Aiko Pras. "Flow whitelisting in SCADA networks." International journal of critical infrastructure protection 6, no. 3 (2013): 150-158.

[2] Barbosa, Rafael Ramos Regis, "Anomaly

detection in SCADA systems: a network based approach," University of Twente, 2014.

[3] Ahmed, Irfan, Sebastian Obermeier, Martin Naedele, and Golden G. Richard III. "SCADA systems: Challenges for forensic investigators." Computer 45, no. 12 (2012): 44-51

[4] Galloway, Brendan and Gerhard P. Hancke. "Introduction to industrial control networks." Communications Surveys & Tutorials, IEEE 15, no. 2 (2013): 860-880.

[5] Goldenberg, Niv, and Avishai Wool. "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems." International Journal of Critical Infrastructure Protection 6, no. 2 (2013): 63-75.

[6] Cid, Daniel B. "Log Analysis using OSSEC." Accessed Nov., 21st, 2014. http://www. ossec. net/ossec-docs/auscert-2007-dcid.pdf (2007).

[7] Mantere, Matti, Mirko Sailio, and Sami Noponen. “A module for anomaly detection in ICS networks.” In Proceedings of the 3rd international conference on High confidence networked systems, pp. 49-56. ACM, 2014.

[8] Snort.org, https://www.snort.org, Accessed Nov. 30th, 2016

[9] Suricata.org, https://suricata-ids.org, Accessed Nov. 30th, 2016

[10] Bro.org “https://www.bro.org”, Accessed November 30th,2016

[11] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82.

[12] Quickdraw, http://www.digitalbond.com/tools/quickdraw, Accessed Nov. 30th, 2016

[13] Knapp, Eric. “Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems.” Elsevier, 2011.

[14] Peterson, Dale. Blog. “ICS Protocols Make New GE D20 RTU Still Insecure By Design,” http://www.digitalbond.com/blog/2013/08/22/ics-protocols-make-new-ge-d20-rtu-still-insecure-by-design/, Accessed Nov., 7th, 2014.

[15] Tofino Security. “Tofino Argon Security Appliance.” https://www.tofinosecurity.com/sites/default/files/DS-TSA-ARGON.pdf, Accessed Nov., 29th, 2016.

[16] Secure Crossing. “Zenwall-5,” http://www.securecrossing.com/our-products/zenwall-5/, Accessed Dec., 1st, 2014.

[17] Tenable Network Security “Protecting Critical Infrastructure: SCADA Network Security Monitoring.” http://www.tenable.com/whitepapers, Accessed Dec., 2nd, 2014

[18] Tenable Network Security. “Plugins: SCADA”. . http://www.tenable.com/plugins/index.php?view=all&family=SCADA, Accessed November 29th, 2016

[19] OpenVAS.org “About OpenVAS.” Accessed November., 29th, 2016. http://www.openvas.org/about.html.

[20] wireshark.org “Dissector for ICCP/TASE.2.” https://ask.wireshark.org/questions/19908/dissector-for-iccptase2, Accessed Nov., 29th, 2016.

[21] Netresec “SCADA Network Forensics with IEC-104.” Accessed Dec., 8th, 2014. http://www.netresec.com/?page=Blog&month=2012-08&post=SCADA-Network-Forensics-with-IEC-104

[22] Alien Vault OSSIM, https://www.alienvault.com/products/ossimAccessedNovember30th,2016

[23] SmartFlow Anomaly Detection for SCADA – Solana Networks, “/www.solananetworks.com/products/smartflow”, Accessed November 29th,2016.

[24] Solana enhances Suricata Open Source Intrusion Detection System (IDS), “http://www.solananetworks.com/news/2015/09/03/solana-enhances-suricata-open-source-intrusion-detection-system-ids-support” Accessed November., 29th, 2016.

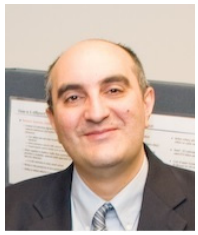
〈저자소개〉

Dr. Craig Dillabaugh

He is a researher/software developer with Solana Networks in Ottawa, Ontario, Canada. He has worked in networking research/development for two years, with a focus on SCADA networks. Prior to his work with Solana Networks, Craig worked as chief technical officer with Changzhou AiSpatial Technologies Inc in China, where he he lead development on Satellite Imaging systems. Craig has also worked with government research labs at the Canada Centre for Remote Sensing and Agriculture Canada where he conducted research in remote sensing and Geographic Information Systems. Mr. Dillabaugh holds a Ph.D. in Computer Science from Carleton University, a Masters degree in Geography from the University of Victoria, and a Bachelors degree in Environmental Studies from the University of Waterloo.

Biswajit Nandy

He has 25 years of experience in the area of data communication and network security. At Solana Networks, as Chief Technology Officer he is focused on technology development for network and security monitoring solutions. He was previously with Nortel Networks and worked extensively in the area of IP-QoS, congestion control and transport protocol performance. He is an Adjunct Research Professor with the Systems and Computer Engineering Department at Carleton University. He has authored more than 50 papers in conferences and journals and holds 22 granted US patents in the area of IP networking. Biswajit holds a PhD degree in Electrical and Computer Engineering from the University of Waterloo, Canada.



Nabil Seddigh

He completed a B.Eng in Computer Engineering from the University of Waterloo in 1993 and a M.A.Sc in Systems and Computer Engineering from Carleton University. He is a co-founder and President of Solana Networks with over 22 years experience in the networking and cyber security industry. Nabil's research interests include network security, network diagnostics, network discovery, Quality of Service and traffic analysis. He is the holder of 20 issued US Patents with over 35 conference and IETF publications.

Kevin Wong

He is a software engineer and developer with 10 years of experience. His projects since 2005 have focused on software development, deployment and support of numbers of network tools using languages such as C/C++, Java, and Python to develop products for Network Monitoring, Network reporting, Network Management, Network Discovery tool, and Multi-Protocol Access Router. In addition to software development, he has extensive knowledge of networking and cybersecurity concepts such as SCADA (Modbus, DNP3, EtherNet/IP, CIP), Deep Packet Inspection, Netflow, sFlow, cryptography, MPLS, SNMP, and Ethernet.

Byoung-Joon (BJ) Lee

He has more than 20 years of industry and academic experience in the area of data networking and communications technology. Since March 2015, he has been running Creatrix Design Group - a web technology company focused on the accessibility and UX innovations. His previous work was with Samsung Electronics Advanced Institute of Technology in Giheung, Korea from 2003 to 2014, and also with Nortel Networks, Cisco Systems, and Tropic Networks from 1996 to 2003 in various technical and managerial capacities, all in Ottawa, Canada. He has more than 30 US patents. BJ holds a PhD in Electrical and Computer Engineering from the University of Waterloo, Canada.