102609-ITN-47s-E-2019
IoT / OT Security Team Lead

Holds a B. Sc. in Communications & Electronics Engineering and has about 10 years of experience in cyber security for IoT/OT, Hardware and RF security in Electricity, Oil & Gas and Railway.

PERSONAL DATA

Nationality	:	Egyptian
Birth Date	:	11/10/1992
Gender	:	Male
Residence	:	New Cairo

EDUCATION

: B. Sc. in Communications & Electronics Engineering, Cairo University, 2019

LANGUAGES

Arabic	:	Native Language
English	:	Good

COMPUTER SKILLS

: Windows, MS Office, Internet

CHRONOLOGICAL EXPERIENCE RECORD

Dates : From Oct. 2021 till now

Employer : The Egyptian Computer Emergency Readiness Team (EG-CERT)

Job title : IoT / OT Security Team Lead

Job Description :

- Leading the team through penetration testing and vulnerability assessment of critical IoT/OT infrastructure applications according to IEC62443 - TS50701 - NIST 7628 - NIST SP800-82 - ENISA - IoT Security Foundation.
- Cybersecurity architecture review and risk assessment for massive national projects including railway (LRT - Monorail - Siemens high speed rail), Oil & Gas (Pipelines control and security, and main control centers cybersecurity) and Electricity (Smart meters and smart grid cybersecurity) and water treatment facilities, in addition to huge steel factories and many other industries.
- Experience with security architecture for OT and selecting the suitable security solutions for the use cases. For example, SEIM solution, EDR, Firewall, NGF, WAF, Authentication…etc.
- Leading IEC 62443 Security architecture review and IEC certification process with SGS and UL.

- PSA Level 1, Level 2, and Level 3 software and hardware assessments and Common Criteria EAL3+ - EAL4 assessments.
- Managing communications with IoT/OT OEMs and stake holders about the current projects' security status and required vulnerability fixes.
- Writing complete penetration testing and vulnerability assessment reports for the critical infrastructure tests.
- Conducting risk assessment and threat analysis, and review risk plans for the IoT/OT projects.
- Leading code security reviews and fuzzing.
- Conducting trainings for the team in Cryptography, Fault injections, Side channel, Fuzzing, and other firmware and hardware security related topics**.**

Dates : From Jan. 2018 till Oct. 2021

Employer : The Egyptian Computer Emergency Readiness Team (EG-CERT)

Job title : Senior IoT, RF & Hardware Security Engineer

Job Description :

- Hardware security and penetration testing including side channel analysis and fault injection attacks (Voltage – EMI – Clock – Temperature) using both DIY and professional lab tools.
- Using DPA, CPA, DCA methods for side channel analysis. Using the reverse CPA and T-Test for leakage detection. Experience with Chip Whisper, eShard tools, and Daredevil, Tracergrind.
- Using Deep learning for side channel analysis including MLP and CNN.
- Analysis and fuzzing of encryption protocols to find and fix cryptographic vulnerabilities, this includes analysis if the white box cryptography implementations, and using the side channel analysis and fault injection attacks Including using Differential Fault Analysis tools.
- Firmware analysis using fuzzing, symbolic execution, reverse engineering.
- Penetration testing wireless protocols and devices including Wi-Fi – Bluetooth – Zigbee – RFID – GNSS (GPS/Glonass) – LoRA. Using state of the art tools including SDR, spectrum analyzer, vector signal transceiver, and protocol analyzers.
- Developing intrusion prevention and detection systems for Wi-Fi networks, GNSS receivers and CAN bus networks.
- Expert knowledge with many cyber security frameworks and guidelines including: NIST7628 – IoT Security Foundation – ENISA – ISO 21434 – NIST SP800-174 – NIST SP800-53 – NIST SP800-193.
- Machine learning and deep learning experience in cyber security including Attack detection, Attack analysis, Anomaly detection, Network traffic analysis, etc.
- Expert knowledge in cryptography including symmetric, asymmetric, hybrid algorithms, digital certificates, key exchange, key encapsulation, key derivation...etc.
- Penetration testing industrial and critical infrastructure devices including smart meters, train signaling and control devices, modems, wireless transceivers...etc.
- Secure C/C++ source code review based on CERT C/C++, CWE, OWASP.

Dates : From Sep. 2021 till now
Employer : Iskraemeco
Job title : OT Security Consultant
Job Description :

- White box penetration testing on secured smart meters firmware and hardware. Including reviews on cryptographic algorithms, authentication, CWE coverage, code review based on CERT C/C++ secure coding standard, and assessments on the effectiveness of attack counter measures.
- Hardware security analysis regarding side channel, and fault injection attacks.
- Assessments on DLMS/COSEM and the communication protocols used by smart meters, including IEC1107, Power Line Communication, and Wireless Communication.
- Security assessment on one of the big smart meter projects in compliance with the NIST 7628 standard.

Dates : From Sep. 2022 till now
Employer : DXC Technology, Outsourced to BMW
Job title : Senior Automotive Security & Cryptography Expert
Job Description :

- Responsible for the security architecture of the secure boot and secure firmware update concepts in BMW IPNext ECUs.
- Responsible for the hardware security of the Qualcomm chipset and the ECU.
- Responsible for the architecture of the BMW cryptography stack based on the adaptive AUTOSAR.
- Working on QNX QCrypto, OpenSSL, Botan.
- Code reviews based on the CERT C++ Secure coding standard, and the AUTOSAR standard.

Dates : From Sep. 2021 till Sep. 2022
Employer : ElektroBit - Full time, remote contract with the Sub-contractor AveLabs LLC
Job title : Senior Automotive Security & Cryptography Expert
Job Description :

- Developing the Adaptive AUTOSAR Cryptography stack for Ford.
- Developing the architecture of the Cryptographic Daemons based on the Public Key Infrastructure (PKI) and the PKCS#11 to secure hardware and secure the SW transactions. Including Daemon interface with Identity and Access Management, Communication stack, and Crypto API.
- Working on SoftHSM2 and Botan cryptographic libraries and modifying their source code to be AUTOSAR compliant.
- Secure code reviews based on the CERT C++ Secure coding standard, and the AUTOSAR standard.
- Using static analysis tools for inheritance relation, code coverage, and code reviews. This includes using tools like Axivion and Bullseye.
- Expert in cryptography including symmetric (AES, DES, 3DES), Asymmetric (RSA, ECC) cryptography, Hashing algorithms, Message authentication, digital signatures. In addition to Secure Boot, chain of trust and Hardware Security Modules (TPM and SE).
- Participating in the Security Architecture PI planning meetings with Ford

and Elektobit as per the SAFe methodology.
- Planning trainings for AveLabs team on Cryptography, PKCS#11, and Secure coding.
- Following ISO SAE 21434 standard including managing cyber security threats using TARA.

Dates : From Jan. 2021 till Jun. 2021
Employer : Remote – Part-time, PhD Project, King Abdulaziz University – KSA – Network attacks classification based on CNN Auto-Encoder
Job title : Deep Learning Engineer
Job Description :
- Developed a novel CNN Auto-Encoder architecture.
- Used a novel approach for CNN weights initialization before training achieving 99% F1 score with 99.7% AUC on the CICDDOS2019 Dataset.

Dates : From Oct. 2019 till Jan. 2021
Employer : Part-time, PhD Project, Helwan University - CtuNet: A Deep Learning-based Framework for Fast CTU Partitioning of H265/HEVC Intra-coding
Job title : Deep Learning Engineer
Job Description :
- Developed the CNN Model and tuned it for the problem needs.
- Integrated the Deep learning Python code into the H265 complex C++ code to replace the H265 Codec's complex math predictions with a fast CNN prediction. This resulted in 70% time saving and improving FPS rate.
- Published in "Ain-Shams Engineering Journal" - an Elsevier Journal.

Dates : From Jun. 2017 till Jan. 2018
Employer : Full time, The Design Lab for Electronics & Communication Systems (DLECS), Cairo University
Job title : Embedded FW Engineer
Job Description :
- Implemented AES-128bit encryption algorithm for the smart power meter national project.
- Implemented OTA Bootloader for the railway national project.
- Railway sensor interface logic for the railway national project.
- Worked on TI CC1350 Dual-Band RF for IoT applications.
- Worked on TI MSP430 mixed signal processor.
- Used TI RTOS on CC1350.

Dates : 2017
Job title : Embedded FW Engineer (Freelancer)
Job Description :
- Implemented one-way communication system for transmitting encrypted audio signals to a receiver.
- Implemented PCM encoding/decoding for an uncompressed audio processing.

Dates : From Jan. 2017 till Feb. 2017
Employer : Freelancer, Bartech-Egypt
Job title : Embedded FW Engineer

Job Description : Developed an NFC student registration system for Schools and Busses.

Dates : From Aug. 2016 till Sep. 2016
Employer : Freelancer, EBike Egypt
Job title : Embedded FW Engineer
Job Description : Developed the FW and HW to enable smart phones to have full control over electric bikes for tourism industry.

Dates : From Jun. 2016 till Feb. 2017
Employer : Full time, Telekord
Job title : Embedded FW Engineer
Job Description :

- Implemented BLE Beacons protocol on nRF52 and CC2640 ICs.
- Implementing Bootloader for OTA updates.
- Worked on the HW&FW HLDs.
- Worked on socket programming TCP/IP communication for TI TM4C Devices.
- Implemented MQTT protocol on TM4C devices for iot application.

Dates : From Feb. 2016 till Jan. 2017
Employer : Full time, Smartec-Group
Job title : Hardware Developer
Job Description :

- Designed 3-channel sliding gates motor control board for home automation.
- Completed HW design for the tire pressure monitoring system using energy harvesting.
- Collaborated in the design of 3-channel Smart Power Switch (SPS).
- Designed PCBs for the ESP8266 2.4GHz WIFI modules.
- Designed PCB for 433MHz communication in Automotive.
- Home Automation systems installations.

Dates : From Jan. 2016 till Oct. 2016
Employer : Remote – Part time, Neo-Dronics GmbH, Bremen, Germany
Job title : Embedded Control Engineer
Job Description :

- Designed and implemented Control algorithms for using DGPS signals in precise navigation.
- Designed and implemented a complete Adaptive Extended Kalman Filter sensor fusion algorithm for 1000Hz INS/DGPS precise navigation solution for Quad-Copters.
- Designed and implemented a non-linear UHF RF Positioning algorithm on DWM1000 Modules.

Dates : From Jul. 2015 till Dec. 2015
Employer : Remote – Part time, RECCE UNMANNED SYSTEMS CORP (RUSC), Calgary, Canada
Job title : Embedded Control Engineer
Job Description :

- Implemented DGPS algorithm for quad-copter precise navigation in Survey industry.

- Enhanced IMU sensor fusion performance by 41% using a sensor array solution.

Dates : From May 2015 till Dec. 2016
Employer : Remote – Part time, ATAN2 Corp, California, USA
Job title : Embedded Control Engineer
Job Description :
- Designed and implemented AHRS algorithm for the MOTUS Camera project.
- Designed Hard and Soft Iron calibration algorithms for Magnetometer sensors on MOTUS sensor boards.
- Collaborated in the RF Positioning algorithm using DWM1000 UHF Modules.
- Designed and implemented 3-axis brushless motor gimbal for camera stabilization.
- Project listed on Kickstarter.

Dates : From Feb. 2015 till Feb. 2017
Employer : Remote – Part time, Visus VR, California, USA
Job title : Embedded Control Engineer
Job Description :
- Designed and implemented a complete head tracking system for Visus VR.
- Designed and implemented sensor calibration algorithms against fixed offset errors, scale errors, and temperature errors.
- HW & FW Design for a 2.4GHz communication system using nRF24L01 ICs.
- Implemented a secure AES-128Bit encrypted Bootloader for OTA updates on Visus VR.
- Designed 9W LED Driver PCB for imaging applications.

Dates : 2015
Job title : Embedded FW Engineer (Freelancer)
Job Description :
- Implemented a CAN transceiver for Nissan motors ECUs to perform read/write Flash memory and motor calibration parameters.
- Implemented an OBD2 diagnostic module for car maintenance.

Dates : 2015
Job title : Embedded FW Engineer (Freelancer)
Job Description :
- Implemented a basic 14-bit digital signal oscilloscope using TI TM4C Series.
- Programmed a basic GUI to display the scope input signals on PC and perform signal conditioning using C# and USB HID protocol.

Dates : 2014
Employer : Full time, ArabTech
Job title : Embedded Systems Instructor
Job Description : Worked for the following courses:
- NI LabView Diploma.

- Micro-Controller Diploma.
- Quad-Copter Autopilot courses.
- Solar charging.

Dates : From 2013 till 2014

Employer : Cairo University

Job title : Embedded Control Engineer

Job Description : Worked on developing a quad-copter autopilot with Dr. Ahmed Abu-elseoud, Control Professor, for navigation and imaging applications.

Publications:

- Lecturer: Wireless Security and Penetration Testing Course (Feb. 2022), Ottawa University master's degree in cyber security - DEBI program.
- Author: Wireless Networks Penetration Testing Professional Course (Jan. 2022), Information Technology Institute (ITI).
- Research Paper: CtuNet: A Deep Learning-based Framework for Fast CTU Partitioning of H265/HEVC Intra-coding (vol. 12, issue 2) (Jun. 2021, pages 1859-1866).

Field of experience :

- Versatile ICS, OT, Embedded systems, Hardware, and Wireless systems security professional.
- Expert skills in ICS/OT Security, IEC 62443, TS 50701, NIST 7628, NIST SP800-82, Risk assessment, Penetration Testing, Vulnerability Assessment, threat analysis, Cryptography, Public Key Infrastructure, Wireless Network Security, Hardware Security including side channel analysis and fault injections, IoT security.