Khaled Serag

1109 Windsor Dr. West Lafayette, Indiana, USA, 47906

+1 (347) 766-1152 | kserag@purdue.edu | khaled-alsharif.github.io/ | linkedin.com/in/khaledserag | Khaled Serag

Education

Purdue University *West Lafayette, Indiana, USA*

Ph.D. in Computer Science *August 2017 - August 2023*

- **Thesis:** Proactive Vulnerability Identification and Defense Construction – The Case For CAN
- **Advisor:** Dongyan Xu
- **Co-advisor:** Z. Berkay Celik

State University of New York at Binghamton *Binghamton, New York, USA*

M.S. in Electrical and Computer Engineering *December 2015*

- **Specialization:** Information Assurance
- **GPA:** 3.91

Ain Shams University *Cairo, Egypt*

B.S. in Electrical Engineering *September 2012*

- **General Grade:** G.
- **Major Grade:** V.G.

Publications and Patents

Academic Papers

ZBCAN: A Zero-Byte CAN Defense System. *Khaled Serag*, Rohit Bhatia, Akram Faqih, Muslum Ozgur Ozmen, Vireshwar Kumar, Z. Berkay Celik, Dongyan Xu. In Proceedings of the 32^{nd} USENIX Security Symposium, 2023.

Attacks on CAN Error Handling Mechanism. *Khaled Serag*, Vireshwar Kumar, Z. Berkay Celik, Rohit Bhatia, Mathias Payer, Dongyan Xu. In Proceedings of the NDSS' Fourth International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2022

Exposing New Vulnerabilities of Error Handling Mechanism in CAN. *Khaled Serag*, Rohit Bhatia, Vireshwar Kumar, Z. Berkay Celik, Dongyan Xu. In Proceedings of the 30^{th} USENIX Security Symposium, 2021

Evading Voltage-Based Intrusion Detection on Automotive CAN. Rohit Bhatia, Vireshwar Kumar, *Khaled Serag*, Z. Berkay Celik, Mathias Payer, and Dongyan Xu. In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2021

Patents

Multiple Security Level Monitor for Monitoring a Plurality of MIL-STD-1553 Buses with Multiple Independent Levels of Security. Josh D Eckhardt, Thomas E Donofrio, *Khaled Serag*. United States Patent No.: US10685125B2, 2020

Bus data monitor. Josh D Eckhardt, Thomas E Donofrio, *Khaled Serag*. United States Patent No.: US10691573B2, 2020

System and Method of Monitoring Data Traffic on a MIL-STD-1553 Data Bus. Josh D Eckhardt, Thomas E Donofrio, *Khaled Serag*. United States Patent No.: US10467174B2, 2019

Research Experience

Purdue University *West Lafayette, Indiana, USA*

Research Assistant *August 2017 - Present*

Versatile and Performance-Friendly CAN Defense Construction (Paper Published) *January 2021-Present*

- Design a CAN defense system that protects against the most common CAN attacks
- The system should have prevention and detection abilities
- The system should not use high-overhead operations such as encryption
- The system should not cause significant delays or significant busload increase and should not use message fields

CAN Error Handling Mechanism Vulnerability Identification (Multiple Papers Published) *August 2017-January 2021*

- Identify vulnerabilities in CAN's error handling and fault confinement mechanism
- Showcase the different attack vectors that could take advantage of the discovered vulnerabilities
- Suggest ways to mitigate the discovered vulnerabilities
- Formalize and automate the vulnerability identification process
- Design a vulnerability scanning tool to test the protocol's error handling and fault confinement mechanism

Boeing
Huntsville, Alabama, USA

Cyber Security Researcher (Summer Only) *August 2017 - January 2022*

Key Management for a Mesh-Networked Satellite System *May 2021 - June 2021*

- Design a key management mechanism for a satellite network that uses mesh networking
- Provide forward and backward secrecy for nodes that join or leave the network
- Account for and differentiate between nodes that are joining and leaving the network and nodes that are being temporarily disconnected

Avionic CAN Bus Intrusion Detection System *May 2020-August 2020*

- Make a list of the most common attack vectors for avionic CAN bus systems
- Elaborate on the pros on cons of different attack detection approaches, whether ML-based, Rule-based or hybrid
- Recommend features and rules to be watched for or enforced by any defense system

Vulnerability Assessment for a Mesh Network Using the Thread Protocol *May 2019 - August 2019*

- Assess the security posture of the Thread protocol if implemented on cargo airplanes
- Assess the performance impact of Thread given a cargo airplane scenario
- Write a white paper listing the security and performance pros and cons if such implementation takes place

AFDX Switch Design and Analysis *May 2018 - August 2018*

- Analyze current security threats to AFDX Systems
- Collaborate with team to design an AFDX switch with security measures to overcome the current security threats

Boeing
Huntsville, Alabama, USA

Cyber Security Researcher (Full Time) *February 2016 - August 2017*

MIL-STD-1553 Guard/Monitor Design (Two Patents Published) *February 2016 - August 2017*

- Collaborate with team to design a guard for MIL-STD-1553 systems using off-the-shelf components
- Investigate the impact of installing a guard between the protected payload and the bus on the system's latency
- Investigate the impact of installing a guard between the protected payload and the bus on the electrical characteristics of the system
- Study the different approaches to minimize the negative consequences of the guard installation on the system's latency

Multiple Independent Layers of Security for MIL-STD-1553 Systems (Patent Published) *September 2016 - August 2017*

- Collaborate with team to secure multiple 1553 buses with different security levels running on a shared hardware
- Work with team to design an interface that maintains the separation between different security levels of each bus

Common Open Research Emulator (CORE) API Development *September 2016 - August 2017*

- Collaborate with team to Develop CORE's API to incorporate more protocols/standards
- Investigate ways to develop a complete framework for wireless communications
- Develop CORE's software to facilitate the interaction between CORE and EMANE (Extendable Mobile Ad-hoc Network Emulator)

Threat Analysis for an Avionic System *January 2017 - July 2017*

- Threat-analyze a system of TTTech Deterministic Ethernet, AFDX, and Windriver VxWorks
- Identify system assets, threat agents and system vulnerabilities
- Write a white paper containing a descriptive list of the possible attack vectors in addition to an attack tree

Network Monitoring Web Interface for Commercial Airplanes *April 2017 - July 2017*

- Design a system to monitor real-time network performance metrics using Sflow
- Identify the relevant network metrics
- Collaborate with team to design a GUI web interface to show the network components and real-time metrics

Dynamic Network Resource Allocation for DARPA *June 2017 - July 2017*

- Make a list of the specifications to adopt based on the Dynamic Link Exchange Protocol (DLEP)
- Update the Common Open Research Emulator's (CORE) source code to include Open vSwitch as a network element

State University of New York at Binghamton
Binghamton, New York, USA

Graduate Student *January 2014 - December 2015*

Distributed Web Crawling System *September 2015 - December 2015*

- Use Python to control Google Chrome browser, interface with pages, and gather data in real time
- Write a Crawling algorithm that allows for the specification of the crawling depth and the number of crawlers
- Create a database that collects the data gathered from running crawlers and keeps track of the visited URLs

Privacy Assurance on Facebook *January 2015 - May 2015*

- Collaborate with my professor to find better ways to protect personal information on Facebook
- Collaborate with two students to use Steganography to embed secret pictures in cover pictures
- Investigate whether Partially Homomorphic Encryption (Additive, Multiplicative) could be beneficial if used to encrypt keys in the database

Dual Core Processor Design Using Verilog *April 2014 - May 2014*

- Collaborate with two team-mates to design a simple dual core processor
- Write the code for the Caches, ALU's, and buffers, then synthesized the code using Synopsys

Other Professional Experience

Deloitte *New York City, New York, USA*

Cyber Risk Intern *June 2015 - July 2015*

- Collaborated with team to develop SIEM content for The State of Connecticut
- Created 8 Qradar reports based on 6 use cases
- Concluded with a final presentation during the Weekly Status Meeting

Security Meter *Giza, Egypt*

Information Security Intern *September 2013 - December 2013*

- Applied (SIEM) solutions for both Linux and windows computers of Banque Misr Using Qradar and Tenable
- Collaborated with 2 Engineers to apply Freeradius server authentication on the computers of Banque Misr
- Participated in multiple projects to develop two factor authentication (using Entrust) plans for several organizations

Talks and Presentations

ZBCAN: A Zero-Byte CAN Defense System *August 2023*

The 32^{nd} USENIX Security Symposium *Anaheim, California*

Vulnerability Identification and Defense Construction in Cyber-Physical Systems *March 2023*

Presented to the School of Electrical and Computer Engineering *University of Ottawa*

Vulnerability Identification and Defense Construction in Cyber-Physical Systems *February 2023*

Presented to the School of Electrical Engineering and Computer Science *American Uni. of Beirut*

Protecting Against The Most Common CAN Bus Attacks *October 2022*

Presented to the Office of Naval Research (ONR) *Purdue University*

Demo: Attacks on CAN Error Handling Mechanism *April 2022*

Automotive and Autonomous Vehicle Security (AutoSec) Workshop

Exposing New Vulnerabilities of Error Handling Mechanism in CAN *August 2021*

The 30^{th} USENIX Security Symposium

Evading Voltage-Based Intrusion Detection on Automotive CAN *February 2021*

The Network and Distributed System Security Symposium (NDSS)

A Highly Portable CAN Bus Testbed *January 2020*

Presented to the Office of Naval Research (ONR) *Purdue University*

Exposing New Vulnerabilities of Error Handling Mechanism in CAN *June 2021*

Automotive Information Sharing and Analysis Center (Auto-ISAC)

Academic and Professional Services

Technical Program Committee Member

The 26^{th} International Symposium on Research in Attacks, Intrusions and Defenses (RAID) *2023*

Technical Program Committee Member

The Inaugural ISOC Symposium on Vehicle Security and Privacy (VehicleSec), co-located with NDSS *2023*

Technical Program Committee Member

The Artifact Evaluation Committee of the 18^{th} European Conference on Computer Systems (EuroSys) *2023*

Reviewer

IEEE Transactions on Information Forensics and Security (T-IFS) *2022*

IEEE Transactions on Intelligent Transportation Systems (T-ITS) *2023*

Subreviewer

IEEE Symposium on Security and Privacy (IEEE S&P) *2023*

32^{th} USENIX Security Symposium *2023*

IEEE Transactions on Dependable and Secure Computing (T-DSC) *2022*

30^{th} USENIX Security Symposium *2021*

The Network and Distributed System Security Symposium (NDSS) *2021*

Fellowships

Emil Stefanov Fellowship *2022*

For domestic graduate students who specialize in security and show originality and creative thinking in research *Purdue University*

Certifications

2016	Certified Ethical Hacker (CEH)	*EC-Council*
2013	Cisco Certified Network Associate (CCNA)	*Cisco*

Vulnerability Reports

CERT's Vulnerability Information and Coordination Environment (VINCE) *Case: VU#720158*

Controller Area Network Standard (CAN Bus), ISO-11898 *January 2021*

- *Passive Error Regeneration:* Could be exploited to launch an immediate denial of service (DoS) attack
- *Deterministic Recovery Behavior:* Could be exploited to launch a persistent denial of service (DoS) attack
- *Error State Outspokenness:* Could be exploited to identify message sources, their error states, and to map the network
- Also reported the vulnerabilities to Bosch, ISO, ANSI, and SAE
- Gave a talk to the Automotive Information Sharing and Analysis Center (Auto-ISAC) explaining the vulnerabilities

Technology Transfers

Smart Information Flow Technologies (SIFT) *July 2021*

RAndomized Identifier Defense (RAID)

Provides protection against error-handling attacks on CAN systems

Siege Technologies *September 2021*

DUET Attack

A CAN injection attack that evades detection by voltage-based intrusion detection systems (VIDS)

Academic Teaching Experience

CS 590: IoT/CPS Security *Guest Lecturer*

Invited by Dr. Z. Berkay Celik *Spring 2020*

CS 426: Computer Security *Guest Lecturer*

Invited by Dr. Dave Tian *Fall 2022*

CS 426: Computer Security *Guest Lecturer*

Invited by Dr. Z. Berkay Celik *Spring 2023*

CS 528: Network Security *Guest Lecturer*

Invited by Dr. Dave Tian *Spring 2023*

Languages

Arabic	Full Proficiency
English	Full Proficiency
French	Intermediate Proficiency
Spanish	Elementary Proficiency

Citizenship and Visa Status

Citizen of the United States of America

References available upon request.