

Khaled Serag

RESEARCH ASSISTANT · DOCTORAL CANDIDATE

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

Ph.D. in Computer Science

West Lafayette, Indiana, USA

August 2017 - Current

- **Thesis:** Securing CAN Bus Through Vulnerability Identification and Defense Construction
- **Advisor:** Dongyan Xu
- **Co-advisor:** Z. Berkay Celik

State University of New York at Binghamton

M.S. in Electrical and Computer Engineering

Binghamton, New York, USA

December 2015

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

Ain Shams University

B.S. in Electrical Engineering

Cairo, Egypt

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 the 32nd 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 30th 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

Graduate Research Assistant

West Lafayette, Indiana, USA

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

Software Engineer (Cyber Security Researcher-Summer Only)

Huntsville, Alabama, USA

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
- Provide forward and backward secrecy for nodes that join or leave the network

Avionic CAN Bus Intrusion Detection System

May 2020-August 2020

- Make a list of the most common attack vectors for avionic CAN bus systems
- Compare and recommend different attack detection approaches

Vulnerability Assessment for a Wireless Mesh Network (Thread)

May 2019 - August 2019

- Assess the security and performance of the Thread protocol if implemented on cargo airplanes
- Write a white paper listing the security and performance pros and cons if such an 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

Software Engineer (Cyber Security Researcher-Full Time)

Huntsville, Alabama, USA

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 on the system's latency and electrical characteristics

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

- 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

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

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

Academic Teaching Experience

CS 590: IoT/CPS Security

Invited by Dr. Z. Berkay Celik

Guest Lecturer

Spring 2020

CS 426: Computer Security

Invited by Dr. Dave Tian

Guest Lecturer

Fall 2022

CS 426: Computer Security

Invited by Dr. Z. Berkay Celik

Guest Lecturer

Spring 2023

CS 528: Network Security

Invited by Dr. Dave Tian

Guest Lecturer

Spring 2023

Talks and Presentations

Protecting Against The Most Common CAN Bus Attacks

Presented to the Office of Naval Research (ONR)

October 2022

Purdue University

Demo: Attacks on CAN Error Handling Mechanism

Automotive and Autonomous Vehicle Security (AutoSec) Workshop

April 2022

Exposing New Vulnerabilities of Error Handling Mechanism in CAN

30th USENIX Security Symposium

August 2021

Evading Voltage-Based Intrusion Detection on Automotive CAN

The Network and Distributed System Security Symposium (NDSS)

February 2021

A Highly Portable CAN Bus Testbed

Presented to the Office of Naval Research (ONR)

January 2020

Purdue University

Exposing New Vulnerabilities of Error Handling Mechanism in CAN

Automotive Information Sharing and Analysis Center (Auto-ISAC)

June 2021

Academic and Professional Services

Technical Program Committee Member

The 26th 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 18th European Conference on Computer Systems (EuroSys)

2023

Reviewer

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

2022

Subreviewer

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

2023

32th USENIX Security Symposium

2023

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

2022

30th USENIX Security Symposium

2021

The Network and Distributed System Security Symposium (NDSS)

2021

Fellowships

Emil Stefanov Fellowship

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

2022

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

Case: VU#720158
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)
RAandomized Identifier Defense (RAID)
Provides protection against error-handling attacks on CAN systems

July 2021

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

September 2021

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.