COLLEGE OF ENGINEERING
AND COMPUTER SCIENCE

FINAL ORAL EXAMINATION

OF

Roy Laurens
BS, Sekolah Tinggi Teknik Surabaya, Indonesia, 1996
MS, Carnegie Mellon University, 1998

for the degree of

DOCTOR OF PHILOSOPHY
IN COMPUTER SCIENCE

November 29, 2022, 11:00 AM
Virtual
https://ucf.zoom.us/j/98669091110?pwd=NkxCamg1RVVpMXJWM080K1FUNzlMdz09

Dissertation Committee:
Dr. Cliff Zou, Chairman changchun.zou@ucf.edu
Dr. Kien Hua kien.hua@ucf.edu
Dr. Chung-Ching Wang chung-ching.wang@ucf.edu
Dr. Xinwen Fu xinwenfu@ucf.edu

DISSERTATION RESEARCH IMPACT

The prevalent use of credit/debit cards our online transactions makes it easy for fraudster to use a stolen card, since online merchants cannot physically verify the supposed buyer/cardholder. And in the payment card processing scheme, merchants are held responsible for any fraud claims by the cardholder, yet there is virtually all fraud research focus on the card processor and not on the merchant. In contrast, our research presents a practical framework that can be implemented by online merchants to defend against transaction frauds by combining three synergistic components: 1. automated detection of known fraud patterns; 2. anomaly detection to catch new/unknown fraud patterns; 3. an automated system to 'challenge' the buyer if the transaction is suspected to be fraudulent. This allows the framework to be scalable with minimal human supervision, and it also reduce customers dissatisfaction as they can proof that they are the legitimate cardholder if their transactions are incorrectly flagged.

Our framework can be readily implemented and we have deployed several aspects of our framework at a real-world e-commerce Merchant website, with the real testing results explained in this dissertation.

SELECTED PUBLICATIONS & PATENTS

Secure Smart Card Signing with Time-based Digital Signature, Hossein Rezaeighaleh, Roy Laurens, Cliff C. Zou, in IEEE ICNC, 2018.

Using DNS Client Information to Detect Transaction Fraud, Roy Laurens, Hossein Rezaeighaleh, Cliff Zou, Jusak Jusak, in IEEE ICC, 2019.

The Evolution of Online Credit/Debit Card Fraud Used by Indonesian Perpetrator: a Case Study, Roy Laurens, in The Inaugural I-4 International Conference on Science, Technology and Humanities, 2020.

Side-Channel VoIP Profiling Attack against Customer Service Automated Phone System , Roy Laurens, Edo Christianto, Bruce Caulkins, Cliff Zou, in IEEE Globecom, 2022.

A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Testbed, Jusak Jusak, Seedahmed S. Mahmoud, Roy Laurens, Musleh Alsulami, Qiang Fang, in IEEE Access, 2022.

Applying the Mission Model Canvas to LVC Network Defects, Rebecca Cebulka,Jordan Dauble, Roy Laurens, Ethan Whaley, Brandon Lima, Erik Bates, Luke Milbocker, in Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop, 2022.

Patents:

2002, Network layer support to enhance the transport layer performance in mobile and wireless environments, 6,947,451

2003, Network Layer Support To Enhance The Transport Layer Performance In Mobile And Wireless Environments, 6,510,144

DISSERTATION

A SEMI-AUTONOMOUS CREDIT/DEBIT CARD TRANSACTION FRAUD DEFENSE FRAMEWORK FOR ONLINE MERCHANTS

The majority of online credit/debit card fraud research focuses on the defense by back-end entities, such as card issuer or processor (i.e., payment processing company), and overlooks the fraud defense initiated by online merchants. This is problematic because the merchants - especially online merchants - are the ones generally held responsible for covering any loss due to transaction fraud. Thus they have a great incentive to detect and defend against card fraud. But at the same time, compared with card issuers, they also lack access to large samples needed for data mining (such as existing purchase data of a cardholder).

This dissertation presents a novel semi-autonomous framework for online merchants to defend against such fraud by utilizing three interrelated components: a supervised classifier based on existing fraud pattern and our newly developed DNS fingerprinting, an unsupervised anomaly detection method using diversity index, and a novel soft descriptor based verification system. The classifier and the anomaly detection work together to allow our framework to detect known fraud patterns and adapt to the previously undetected patterns. Afterward, suspicious transactions can be autonomously verified by requesting the customer to provide a unique identifier that was previously embedded in the soft descriptor during the card transaction processing. This verification process greatly improves fraud detection accuracy without adding a burden on most legitimate customers. Our framework can be readily implemented and we have deployed several aspects of our framework at a real-world e-commerce Merchant website, with the real testing results explained in this dissertation.

ROY LAURENS

2018, Kennesaw State University Cybersecurity Research Workshop

SELECTED AWARDS & HONORS:

2018, Graduate Travel or Presentation Fellowship