3 June 2019

MEMORANDUM FOR: AFIT/ENG
ATTENTION: MAJ CASEY

FROM: 2D LT DAVID CROW (GCS-20M)

SUBJECT: Thesis Prospectus: *Intrusion Detection with Nonlinear Forecasting Methods*

1. In an environment of ever-increasing numbers of malicious actors, the United States Air Force requires a reliable Intrusion Detection System (IDS) in each of its vital systems. This research hopes to determine whether inherent causal relationships of various functions or metrics in a car can be identified and then leveraged as an IDS. Ideally, a successful demonstration of such a capability can generalize to other domains, including aircraft and cyber systems.

2. Previous research concerning nonlinear forecasting methods forms the inspiration for this research. Dr. George Sugihara's empirical dynamic modeling (EDM) toolset, specifically, will likely help with the identification of causal relationships. Captain Brent Stone, a recent AFIT graduate, explored the possibility of using EDM to identify relationships in vehicular systems. However, there are currently no examples in the literature of EDM – or any other nonlinear forecasting method – being used in the construction of an IDS.

3. AFIT already possesses a large amount of data extracted from various cars. If necessary, I can extract further data with the help of Steve Dunlap's data collection devices. Captain Stone's reverse engineering pipeline can convert the data into usable time-series plots. Unsupervised and supervised machine learning toolkits will then cluster the plots and label those that can be labeled (using the SAE J1979 protocol). EDM and other nonlinear forecasting methods will then be used to identify relationships between the various metrics. Finally, the relationships can be used to inform intrusion detection decisions. Ideally, the entire process can be bundled into an automatic IDS pipeline for a given vehicle. Completion of each step in the process (e.g., reverse engineering pipeline, relationship identification) will indicate progress. This research will be deemed successful if I can demonstrate that already-present relationships can be identified, quantified, and leveraged as an intrusion detection system.

4. I expect that the relationships in the vehicle's data can be identified and exploited. The quantified relationships will be documented in the thesis. Additionally, I will evaluate the intrusion detection system's accuracy by utilizing unseen data, some of which is poisoned. In doing so, I can determine whether the IDS can successfully identify faults or intruders in the vehicle.

5. Although this research is not sponsored, it can certainly provide lasting benefits to cybersecurity efforts within the Air Force. If I can successfully devise a car-based process with which one can construct an intrusion detection system, future research can attempt to apply the process to various aircraft. Such a system would add another layer of cybersecurity to our planes, and, if correctly tuned, it could also predict system errors and miscalibrations.

6. Proposed thesis committee:

a. Dr. Scott Graham, Chair / Thesis advisor

GRAHAM.SCOTT.R.1158436376 Digitally signed by GRAHAM.SCOTT.R.1158436376 Date: 2019.05.30 15:19:41 -04'00'

b. Dr. Brett Borghetti, Committee member

BORGHETTI.BRETT.J.1009082820 Digitally signed by BORGHETTI.BRETT.J.1009082820 Date: 2019.06.05 07:46:10 -04'00'

c. Lt Col Patrick Sweeney, Committee member

SWEENEY.PATRICK.JOHN.1169114443 Digitally signed by SWEENEY.PATRICK.JOHN.1169114443 Date: 2019.05.30 15:46:06 -04'00'

7. Machine learning, software engineering, and algorithm design techniques encompass the fundamental research areas for the projected thesis. Therefore, my course plan includes the following courses to prepare me to successfully complete this research:

- CSCE 586 Design and Analysis of Algorithms
- CSCE 593 Introduction to Software Engineering
- CSCE 623 Statistical Machine Learning
- CSCE 723 Advanced Topics in Statistical Machine Learning

CROW.DAVID.
R.1511541502

Digitally signed by
CROW.DAVID.R.1511541502
Date: 2019.05.30 14:58:16
-04'00'

DAVID CROW, 2D LT, USAF
GCS-20M

1st Ind, AFIT/ENG

MEMORANDUM FOR AFIT/ENG

I acknowledge receipt of the above thesis prospectus and thesis committee. This prospectus will be maintained in the department files for students graduating between Sept 2019 and Jun 2020. The thesis should be prepared in accordance with the AFIT Thesis Guide. Good luck!

DANIEL J. CASEY, MAJ, USAF
Chief, Computer Science Division
Department of Electrical and Computer Engineering