Notice of the Final Oral Examination
for the Degree of Master of Applied Science

of

AASHNA AHLUWALIA

BEng (University of Mumbai, 2015)

" Impact Study of Length in Detecting Algorithmically Generated Domains"

Department of Electrical and Computer Engineering

Tuesday, April 17, 2018
2:15 P.M.
Engineering Office Wing
Room

Abstract

Domain generation algorithm (DGA) is a popular technique for evading detection used by many sophisticated malware families. Since the DGA domains are randomly generated, they tend to exhibit properties that are different from legitimate domain names. It is observed that shorter DGA domains used in emerging malware are more difficult to detect, in contrast to regular DGA domains that are unusually long. While length was considered as a contributing feature in earlier approaches, there has not been a systematic focus on how to leverage its impact on DGA domains detection accuracy. Through our study, we present a new detection model based on semantic and information theory features. The research applies concept of domain length threshold to detect DGA domains regardless of their lengths. The experimental evaluation of the proposed approach, using public datasets, yield a detection rate (DR) of 98.96% and a false positive rate (FPR) of 2.1%, when using random forests classification technique