Software Tools for Addressing Cybersecurity and Cybercrime via a co-Evolutionary Approach to reduce human-related risks

Tasmina Islam and Shujun Li
School of Computing, University of Kent

The focus on cybersecurity as a dynamic interaction between humans and socio-technic elements within a risk ecosystem raises practical issues of implementation and conventionally these issues are often considered under ‘raising awareness’. Key to make these awareness activities more effective in influencing human behaviour is to properly incentivise people, businesses and organisations to participate and adapt their behaviour. But due to lack of information about dynamically evolving personal preferences (which need collecting dynamically and at individual level) these may still not be effective. While there is isolated research across these areas, there is no holistic framework combining all these theoretical concepts (co-evolution, opportunity management, behavioural and business models, ad hoc technological research on cyber risks and specific types of cybercrime) to allow a more comprehensive understanding of human-related risks within cybersecurity ecosystems and to design more effective approaches for engaging individuals and organisations in the reduction of such risks. Filling this research gap is the aim of this proposed project.

Introduction

A series of software tools is being developed for active engagement of users in cybersecurity ecosystems, including data management for data sharing (collection), user and community profiling based on shared data, cybersecurity risk evaluation and personalised contextualised communications (including risk visualisation tools). Our goal is not to develop such tools from scratch, but base them on mature technologies and software which we will integrate into a user-friendly toolset for each user group and also investigate behavioural models to allow us to incentivise individuals to engage

Two main aspects of the software development:

Human related location privacy and behavioural model analysis
⇒ System reporting risks to human

# A mobile app
# Based on Hub of All Things (HAT)
https://www.hubofallthings.com/

Human as a Security Sensor (HaaSS)
⇒ Human reporting to system with feedback loop

# An Windows app
# Based on CogniSense

Software Development Objective

A series of software tools is being developed for active engagement of users in cybersecurity ecosystems, including data management for data sharing (collection), user and community profiling based on shared data, cybersecurity risk evaluation and personalised contextualised communications (including risk visualisation tools). Our goal is not to develop such tools from scratch, but base them on mature technologies and software which we will integrate into a user-friendly toolset for each user group and also investigate behavioural models to allow us to incentivise individuals to engage

Main Aspects

Human related location privacy and behavioural model analysis
⇒ System reporting risks to human

# A mobile app
# Based on Hub of All Things (HAT)
https://www.hubofallthings.com/

Human as a Security Sensor (HaaSS)
⇒ Human reporting to system with feedback loop

# An Windows app
# Based on CogniSense

Contact:
School of Computing, University of Kent, Canterbury, Kent, CT2 7NF. Email: T.Islam@kent.ac.uk; Website: https://accept.cyber.kent.ac.uk/