Deliverable for WP 5.2

1. INTRODUCTION

This work package was optional and it was co-led by SMU and UoS. The main aim was to provide insights on how the research outcomes from the project can be generalized to other cyber security or even wider computing systems beyond user authentication.

2. EXAMPLE SYSTEMS

The CogTool+ software tools and the general framework we developed in the project are designed for supporting general user interfaces so it can be applied to wider computing systems naturally without any changes.

Among all cyber security systems that can potentially benefit from the tools we developed, this report lists a number of examples, for many of which we have other ongoing projects or planned future research proposals. Note that for many such systems we expect new modules are needed for extending CogTool+ (see the deliverable report of WP5.1 for some of such modules).

Human behaviour sensors for cyber security and cyber crime prevention: In another ongoing EPSRC project "ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks" (EP/P011896/1, see https://accept.cyber.kent.ac.uk/), human behaviour sensors will be developed to help gather useful information about how victims of cybercrime are targeted by criminals. Such systems have user interfaces to engage users for awareness and privacy control purposes, and cognitive modelling tools like CogTool+ can find applications in helping evaluate different designs of the user interfaces without running too many lab-based user studies.

Privacy protection systems: In a newly funded EPSRC project "PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers (PriVELT)" (EP/R033749/1), we will look at privacy enhancing and value evaluation tools for leisure travellers. Such tools will have rich user interfaces (mostly on mobile devices), which can be modelled using CogTool+ for automatic usability evaluation. Data collected from real-world user behaviours can help build new behavioural templates to enrich the models in CogTool+. In addition, the project PI Shujun Li has a PhD student working on mobile privacy. One of his ongoing work is about a mobile app with a new pervasive user interface for nudging users to install apps with better privacy ratings. We can also use CogTool+ to model the app's user interface to evaluate its usability, which can be cross-validated using data from lab-based studies. We expect more future research project proposals of UoS and SMU on privacy related topics, and most will involve user interfaces that can be studied using CogTool+. Similarly, for other privacy protection systems including privacy settings of online social networks, cognitive modelling tools like CogTool+ can be useful to evaluate both usability and settings that can be more easily misunderstood or missed therefore leading to unexpected privacy risks.

Data loss prevention (DLP) systems: The project PI Shujun Li has another Innovate UK funded project "H-DLP: Human-assisted machine learning for bootstrapping DLP (data loss prevention) systems" (see http://gtr.ukri.org/projects?ref=509895), which will involve user interfaces for sensing human behaviours and those for DLP administrators. Such user interfaces can be evaluated using

cognitive modelling tools like CogTool+ to help the design process without conducting a lot of lab-based studies.

Cyber security control rooms: In many industrial systems, human operators in control rooms need to interact with many user interfaces to do their work properly. For a recently granted Dstl UK-France PhD studentship, the project PI Shujun Li will investigate how human-machine teaming can help improve performance of both machines and human operators. Cognitive modelling tools like CogTool+ can potentially help the design and development of any user interfaces to be tested in this project.

Digital forensics systems: The project PI Shujun Li has been working on digital forensics for many years (e.g. in an Innovate UK funded project "POLARBEAR - Pattern Of Life ANPR Behaviour Extraction Analysis and Recognition", see http://gtr.ukri.org/projects?ref=101949). For such systems police staff and officers often need to work with a lot of user interfaces in order to identify useful information for different purposes (e.g., crime investigation, intelligence gathering, and crime prevention campaigns). As far as we know, cognitive modelling tools like CogTool+ can obviously help evaluate usability of such systems and provide insights on how their user interfaces can be improved.

Online banking systems: Such systems have many security-sensitive user interfaces not just for user authentication, but also for transaction verification, foreign currency exchange and other trading features. Cognitive modelling tools like CogTool+ can help evaluate usability and potential security problems related to human behaviours, providing insights for banks to improve both aspects of their systems.

Online exchange platforms of cryptocurrencies/digital assets: Such systems have become popular due to the increased activities of cryptocurrencies in the market. While they mimic currency exchange and trading features of online banking systems and traditional exchange platforms, the special characteristics such as the use of cryptography and the different way to make transactions mean that their user interfaces may be harder to use and more error-prone. It is clearly not easy to conduct lab-based user studies of such systems and some operations may be untestable if the systems do not support a testing feature. Such problems can be solved by using cognitive modelling tools like CogTool+ to conduct non-intrusive testing of usability and also potential attack vectors.

Firewalls: Software and hardware firewalls have been widely used by end users and network administrators to improve security of end user devices and networks. Such systems also have user interfaces that can potentially be mis-used (e.g. complicated rules may be configured wrongly) thus leading to unexpected security risks. Cognitive modelling tools like CogTool+ can help simulate such human errors and estimate how those errors can be reduced by redesigning the user interfaces.

Anti-virus software: Similar to firewalls, AV software also often depend on end users to configure things and react to alerts properly. How usable their user interfaces is and how unexpected security risks may be caused by human behaviours are less explored by researchers. Cognitive modelling tools like CogTool+ can help to simulate complicated scenarios and human behaviours in those scenarios and the consequences in terms of security.