ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks

Shujun Li
University of Kent

18th September 2018
Basic information

- **Acronym:** ACCEPT
- **Title:** Addressing Cybersecurity and Cybercrime via a co-Evolutionary approach to reducing human-related risks
- **Funder:** EPSRC
- **Call:** Human Dimensions of Cyber Security (HDoCS) 2016
- **Budget:** £~1.1m (funding amount £881k)
- **Duration:** 04/2017 – 03/2019 (extension to be requested due to late starts of RAs)
- **Website:** https://accept.cyber.kent.ac.uk/
Basic information

- **Acronym:** ACCEPT
- **Title:** Addressing Cybersecurity and Cybercrime via a co-Evolutionary approach to reducing human-related risks
- **Funder:**
- **Call:** Human Dimensions of Cyber Security (HDoCS) 2016
- **Budget:** £~1.1m (funding amount £881k)
- **Duration:** 04/2017 – 03/2019 (extension to be requested due to late starts of RAs)
- **Website:** https://accept.cyber.kent.ac.uk/

1. Computer Science
2. Crime Science
3. Business
4. Engineering
5. Behavioural Science
Project team
Stakeholders Group

Wider Stakeholders
Aim and approaches

- Overall aim
  - To reduce human-related risks via developing a **socio-technical framework and corresponding software tools** through which we can
    a) analyse the behavioural co-evolution of cybersecurity/cybercrime ecosystems
    b) effectively influence behaviours of a range of actors in the ecosystems

- Approaches
  - Theory-informed, evidence-based, user-centric, real world-facing
Methodology

- Theories
  - Criminology, evolution (biology), behavioural economics, business, …
  - Computational ontology
  - Knowledge base
  - Crime cases and security incidents
  - Data from interviews, focus groups, surveys, lab-based studies and software tools, …

Top-down ➞ Co-Evolutionary Socio-Technical Framework ➞ Bottom-up
- Computational cyber crime/security ontology
Technical framework

Passively Observable Cyber-Physical Spaces (criminals, insiders, hostile nations, ...)

Active (human-in-the-loop) sensors

Actively Observable Environments (end users, employees, IT Services + computers, servers, IoT devices, ...)

HOC (e.g. visualizer) for human users to adapt behaviors

(Semi-)Automated Communicators/Reporters

(Semi-)Automated Tools for Knowledge Discovery and Backward Communication

Law Enforcement Agencies

IT Service Providers

Other Governmental and Non-Governmental Bodies

Industrial Associations (e.g. UIC's Cyber Security Team)

Expert Knowledge + Experience of Front-Line Officers/Professionals
Who are beneficiaries?

- Designers and developers of solutions
- Cyber security educators, trainers, awareness campaigners, etc.
- Law enforcement agencies
- Businesses managers
- Citizens / Employees (⇒ Human-related risks)
- ...

- Humans need incentives to collaborate!
- ⇒ Make the software tools and information provided useful to them (value)!
Incentivising users

- Valuing user’s input
- Offering values to users who have contributed
- Offering more values to users who have contributes more and who are more active
- Potential use of a cryptocurrency-based approach
  - User ⇒ Our Project (Trusted Centre) / Organisations / Communities: Proof of Value (PoV)
  - Our Project (Trusted Centre) / Organisations / Communities ⇒ Contributing Users: tokens / coins (reputation)
  - Contributing Users can exchange tokens/coins for information or services.
Two use cases

- **Use Case 1: Location Privacy**
  - Human-related *privacy* risks in the *cyber-physical* world *across multiple services*

- **Use Case 2: Human-as-a-Security-Sensor**
  - Human-related *security* risks to semantic attacks in the *cyber-physical* world
  - Based on work of George Loukas’s group (University Greenwich) \(\Rightarrow\) They are joining the project team.

- **Use Case 3: cyber fraud**
  - Human-related *security* risks to cyber scam in the *cyber(-physical)* world

- We will focus on the first two use cases in future.
Work plan

- **WP1: Socio-Technical Framework**
  - Task 1.1 Evidence collection & analysis
  - Task 1.2 Knowledge base & theoretical concepts
  - Task 1.3 Ethnographic study & use cases
  - Task 1.4 Business models & behavioural modelling
  - Task 1.5 Developing socio-technical framework

- **WP2: Design and Development of Software Tools**
  - Task 2.1 Development of ontology & tools
  - Task 2.2 Data management tools & interfaces
  - Task 2.3 Tools for user & community profiling
  - Task 2.4 Tools for risk evaluation & communications

- **WP3: Validation through Use Cases**
  - Task 3.1 Use Case 1
  - Task 3.2 Use Case 2
  - Task 3.3 Comparative analysis of both use cases
  - Task 3.4 Impact evaluation
  - Task 3.5 New business opportunities
  - Task 3.6 Technical support & refinement of software tools

- **WP4: Project Management & Stakeholder Engagement**
  - Task 4.1 Project management
  - Task 4.2 Stakeholder engagement
  - Task 4.3 Dissemination and exploitation
Progress so far

- UCL (FT) RA started in 01/2018.
- Kent (FT) RA started in 06/2018.
- WP1 work has been partly done.
- WP2 work is being done.
- WP4 work
  - Interview with Surrey & Sussex Police (hosted by University of Surrey): 3rd October 2017
  - Workshop on Cyber Crime in Finance: 16th October 2017 @ Lloyds Banking Group in London
  - Workshop on Cyber(-Physical) Crime in Transport: 26th October 2017 @ British Transport Police in London
  - Engagement of stakeholders has been suspended since 10/2018.
- Project meetings
  - Over 10 project technical meetings
  - First AB meeting (hosted by University of Surrey): 8th June 2017
  - Second AB meeting (hosted by TU-Delft): 18th September 2018
Call for help

- Expert opinions
- Crime cases (not limited to cyber crime)
- Cyber security incidents
- Statistical data
- Access to relevant people (cyber criminals, victims and their families, etc.)
- Participation of interviews, surveys, focus groups, workshops, lab-based user studies
- Helping to run field studies in real world
- Helping to disseminate our results
- …
Thanks for your attention!

Questions?