Behavioural Science for Usable Security

18 May, 1 – 5pm

Workshop Report

Behavioural Science for Useable Security was a half day workshop held virtually by the University of Surrey. The event was co-organised by Professor Steve Schneider (Director of the Surrey Centre for Cyber Security), Professor Helen Treharne (Department of Computer Science), Dr Adrian Banks (School of Psychology) and Dr Irina Cojuharenco (Director of the University of Surrey Business and Economic Experiments Laboratory). The event was attended by 50 participants including invited speakers and technical assistants. The workshop consisted of plenary key note speakers followed by panel discussion, small group break out room discussions and feedback presentations.

Workshop Aims

The aim of the workshop was to explore how systems can be better designed to engender secure user behaviour by applying insights from behavioural science into how users are likely to actually behave in practice. The workshop used online electronic voting as a context and exemplar of systems with challenging security requirements, though participants were invited to consider wider security contexts. The workshop was interdisciplinary with behavioural and computer scientists joining forces to tackle the challenges of usable cyber security, which requires a blend of technical requirements and understanding of human behaviour.

Key questions were: What determines users' security decisions and behaviour? How may a better understanding of users' behaviour benefit the design of security systems? How can we nudge users to take up important but inconvenient security procedures?

Feedback from participants and positive interactions during the meeting suggests we were successful in meeting these aims.

Summary of Proceedings

Please find our programme here

After a brief introduction to the afternoon from Professor Steve Schneider, the first session of the workshop consisted of four speakers to provide context and frame the group discussions to come.

Karen Renaud from University of Strathclyde opened the proceedings with her presentation about accessibility within security, ensuring that people are capable of acting securely drawing on her experience in Human Centred Security and Privacy. Renaud also discussed nudging and manipulating the architecture where people are making their choice to encourage them to choose a certain way. This was followed by Professor Daniel Reed from Warwick Business School, who's talk titled 'observations from an unsecure human' highlighted how easy and quickly it can be to become unsecure and at risk.

Next Edward Flahavan, Policy Advisor at The Behavioural Insights Team built on this concept of user susceptibility as well as sharing some examples of when they have tested interventions to evaluate whether it improves resilience. Finally, Peter Y A Ryan, Professor of Applied Security at the University of Luxembourg circled back to focus on electronic voting and verifiability. In his presentation he underlined the main challenges involved in designing a secure voting system whilst giving a high-level explanation of how this might work.

These talks were followed by a panel discussion with the four speakers led by Steve Schneider who raised questions from the participants.

The second session formed the heart of the workshop: group discussions within multidisciplinary groups to consider specific security challenges (chosen by the groups based on their interests and expertise) from the point of view of applying insights from behavioural science to propose solutions that might be worthy of research investigation. The challenge was considered both from a behavioural and a security point of view, and then potential solutions considered. The intention was to bring together these two communities to understand each others' modes of discourse and approaches. There were 6 groups, with 5-8 participants in each.

The final session consisted of a plenary where each group fed back to the workshop the main ideas that had been generated, followed in each case by a brief discussion and Q&A.

Key Themes from Presentations and Discussions

Theme 1: Keeping users motivated to exercise good security practices

1. **Considerations**
    a. Age – difficulty and hassle; disabilities
    b. (mis)-using behavioural sciences to motivate users
        i. e.g. advertising vs user privacy
    c. May be aware of good practice but not always apply it
    d. Need to convince user that it is worthwhile
        i. Not always as difficult as they expect
        ii. Consistency across services?
        iii. Disincentives for bad guys (e.g. phishing mitigation through webAuthn)
2. **What solutions do we expect to work?**
    a. Defaults enforced by organisation (cf organ donation opt-in vs opt-out)
    b. Penalise users taking shortcuts
        i. Not a good option
        ii. Shock them? to break the illusion of being safe and secure
        iii. Make bad practice more time-consuming to pursue
    c. Unity (e.g. collective identity, social influence)
        i. Nudges may not work if few are doing the correct thing
3. **Under what additional conditions?**
    a. Enforcement of best practice
    b. Hot/cold empathy gap
4. **What remains unknown?**
    a. Education: how to teach
        i. Backfire effect, more you know, less you trust
        ii. Media coverage, confirmation bias
    b. What to do when opinions and experts disagree?

Theme 2: Electronic Voting

1. **Behavioural Issues:**
    a. Need to use behavioural insights to improve what to convey and what not to convey to voters
    b. Need to understand how to trigger the motivation of users
    c. Need to understand why users need to challenge a system?
2. **Security Issues:**
    a. Perceived risks are lower than benefits of voting and verifying a vote are greater
    b. Taking the human factor into account in the security analysis
3. **What solutions do you expect to work?**
    a. How to explain that one cannot trust the code like in most of the other contexts?
    b. Metaphors?
    c. Make voters think of how to hack the system? And would they detect it?
4. **What remains to be explored?**
    a. Whether being able to see everyone's vote in any way cause feelings that votes are less secure
    b. Whether trust will decrease in e-voting in general after having understood that one cannot trust the source code like in other context
    c. What is the best voter training to improve motivation? Do they need to really know about the underlying security?
5. **Other insight:** Much bigger challenge of understanding the large motivational gap of verifying your vote compared to the trust of the devices

Theme 3: Data Protection

1. **Behavioural Issues:**
    a. Protection comes from owners of the data (responsibility for data)/ This becomes a burden for the user
    b. Responsibility (when things go wrong)
    c. Perception of the vulnerability by the user (I'm too small to be targeted)
    d. Churn - drop off of engagement with security
2. **Security Issues:**
    a. Ease of use vs. maximum protection of data
    b. Contextual situations determine the ease/pain of the deployment of the security process
3. **What solutions do you expect to work?**
    a. Methods to nudge people to proactively defend themselves
    b. Ethical compliance on the corporate level
    c. Cultural change - making the processes easy in a contextual sense
4. **What remains unknown?**
    a. How people will change their behaviour
    b. How to build confidence in security - balance between security/risk

Theme 4: Trust in payment systems

1. **Behavioural Issues:**
    a. Misuse of Identity (accidental or deliberate)
        i. Children or those unfamiliar with technology

ii. One-click payments (bypass MFA)

b. Accessibility of enforced biometrics

c. Trust in Multi-Factor Authentication (MFA)

i. Do users afford too much trust in MFA?

ii. Misunderstanding of MFA guarantees

2. **Security Issues:**

a. Sensitivity of biometric identity verification

b. Adequately conveying the risk of payment systems

c. Spoofing Multi-Factor Authentication (MFA)

i. Lack of accountability (who is responsible?)

ii. Strength of each factor (weakest link)

3. **What solutions do you expect to work?**

a. User adaptability

b. Risk tolerance

c. Positive approach to the adoption of digital systems

i. increase usability

d. Awareness through education

4. **What remains unknown?**

a. Legal considerations, absence of laws/regulations

b. Who is responsible for technology

c. MFA spoofing

Theme 5: Roadmap to usable security

1. **Behavioural Issues:**

a. Ease of use and security defaults are desirable

b. User trust is important

c. Users need to be aware of and react in an agile manner in a fast-paced environment of technology/security updates (e.g., who has access to data and under what assumptions?)

2. **Security Issues:**

a. Systems are constantly updated, including on security features (e.g., producers will update their offerings)

b. Systems need to learn/change in response to security challenges (Zoom example)

c. Systems seek removal of single points of failure

3. **What solutions do you expect to work?**

a. Secure by design (user can turn off)

b. Private by design (user can turn off)

c. Visibility of design criteria of system (transparency)

d. Build up a repository of recovery mechanisms as a result of scenario planning for possible threats (targeting trust in the system)

e. Use champions to help users (targeting greater availability of user support by leveraging communities and social connection)

f. Governance (both decentralised and centralised)

4. **What remains unknown?**

a. Role of emotion

b. How to enable user alertness to changes, including in security requirements?

Theme 6: Interacting with Security Technology

1. **Behavioural Issues:**
    a. Users need to understand "some" security (e.g. public-key certificates like they understand websites) vs. complete transparency (hiding)
    b. In the case of e-voting people "need" security but when they see it, they get completely lost
2. **Security Issues:**
    a. Security solutions have improved considerably, but there are some potential drawbacks on usability due to these security solutions
    b. Do we force users to "engage" with security or do we allow them to check (in e-voting, you would force them to verify)
    c. E-voting is much harder (both technically and socially/psychologically, e.g. people arguing against it - it is a political problem)
3. **What solutions do you expect to work?**
    a. Hardware underpins trust
    b. Vendors removing themselves from responsibility chain
    c. Browsers preventing access to malicious sites
    d. Systems need to be simple and transparent
4. **Under what additional conditions?**
    a. Variable trust and trustworthiness influences behaviour
    b. Increased security can reduce usability
5. **What remains unknown?**
    a. How do different user groups and ages respond?
    b. Will complex systems ever be comprehensible?
    c. How does a lack of comprehensibility influence behaviour?

Next Steps

Several future activities are planned which involve the dissemination of the ideas generated within the workshop, bidding for funding to continue the network that has been created, and exploring future opportunities for funding with collaborators that have been identified through the workshop.

1) SPRITE+ is an EPSRC funded hub for academic and non-academic communities involved in security. We plan on applying to it for funding for the next workshop in this field, in particular linking to one of their main themes of digital vulnerabilities.

2) Several valuable insights in behavioural science arose from the workshop, and we will explore submitting these in response to the recent call for a special issue on 'Security, Privacy, and Surveillance in Cyberspace: Organizational Science Concerns and Contributions' in the Journal of Business and Psychology.

3) All of the key note talks were recorded and are available here as a record and a resource for workshop attendees.

4) Finally, several new contacts have been established and some existing contacts have been deepened in both the cyber security and behavioural science fields. This will allow focused ideas for routes to collaboration to be explored.

Acknowledgements

The organisers are grateful to the Institute of Advanced Studies for financial support. We are particularly thankful to Vicki Blamey for support and advice in organising the workshop. Special thanks go to Ele Pucci for all her hard work in organising the event. We would like to thank all our chairs, participants and presenters for the intellectual and social contributions to the workshop. We would also like to thank the PhD students who provided technical support for the workshop breakout groups.

Adrian Banks, Irina Cojuharenco, Helen Treharne, Steve Schneider

Email: SCCS@surrey.ac.uk