Choice Architecture

RISCS
Research Institute in Science of Cyber Security

Security by design

In supermarkets, food manufacturers fight – even pay – to get the best locations for their products: at eye level, or at the ends of aisles, where they better attract the attention of questing shoppers and therefore are more likely to be bought. In software, designers have long known that most users do not change default settings. This is most easily seen in disputes about whether default privacy settings should opt users in or out. In 2008, the popular book *Nudge*, written by Richard R. Thaler and Cass R. Sunstein, focused mainstream attention on the years of this type of research, and dubbed the design of systems to nudge people toward particular behaviours that benefit both them and society in general "choice architecture" and the designers who make these apparently tiny but vastly influential decisions "choice architects".

The idea of using nudging to influence decision-making in the context of information security is the focus of Choice Architecture for Information Security (ChAISe), led by Aad van Moorsel, a professor at Newcastle University, and co-investigator Thomas Gross, lecturer and director of the Centre for Cyber Crime and Computer Security at Newcastle University. Unlike the rather casual examples above, in the set of tools it finally produces ChAISe aims to implement rigorous assessment and decision-making techniques. ChAISe is Newcastle University's contribution to the Research Institute in the Science of Cyber Security, funded by ESPRC, GCHQ, and BIS, a group of four linked projects intended to provide a scientific basis for making decisions about information security policies and system design.

"We want to find practical solutions to nudge people to do the right thing in terms of security," says van Moorsel. In particular, the project aims to promote secure behaviour without hindering users' productivity and to explore the issues raised by today's trend toward "bring your own device" (BYOD). "We are looking at the consumerisation of the work place. People are going to use devices in ways that we didn't expect."

How long do mobile phone users dwell on different security information?

Besides finding practical solutions, there is a deeper research purpose based on the principle that influencing information security decisions requires a mix of disciplines: technology development, human factors, and economics. Accordingly, ChAISe's four stages began with a study of the psychological factors that dictate human security behaviour and have gone on to develop rigorous foundations for a choice architecture, design and implement the set of tools, and finally evaluate the improvements those tools enable.

Building mathematical models

"The art of modelling is identifying the elements you consider," says van Moorsel, who was a mathematician by training before he got into computer science and has spent his career moving through a series of successively harder problems. Security, he says, is much more challenging than his earlier work quantifying system performance and system availability, simply because of the presence of an attacker.

"You have to take into account the unknown attacks by malicious outsiders and insiders, as opposed to availability interruptions due to software bugs, power failures, and so on, which may be hard to estimate but at least are not inflicted by anybody. Security is about people who are purposely trying to attack you and how you deal with that – making decisions, trading off against productivity."

"To derive a model you need to be a modeller," he says. "Finding the right level of abstraction is also part of the modeller's art.

"If you put in too much detail, you'll be struggling to make the model and to reach a result. Once the model has been built, it then has to be tested to answer two questions. First, how good is the model? And second, are the decisions made using the model better than those made without it? In earlier work, van Moorsel has tended to find that the biggest difference is in the quality of the process by which a decision is reached.

The psychological aspect of the project is the specialty of Lynne Coventry and Pam Briggs at Northumbria University, asking questions such as, "Do people do things differently because it's their own device as opposed to one that belongs to the company?"

In an literature review, Coventry found very little real evidence regarding how people behave with respect to security in real-life situations: there is some work on intentions, but little on actual behaviours other than password use. The surveys that do exist rarely match the problems people have with viruses and insecurities to specific behaviours.

Because SMEs have a particular security problem and rarely having a technical person on staff, a goal of the project has been to understand their needs better. The project has developed a process to allow them and their staff to become involved in identifying security behaviours they may wish to change within their company. Merely involving staff in discussions about security behaviours in itself, Coventry says, could start a change process.

After identifying potentially problematic scenarios, the researchers use their knowledge of how behaviour is influenced to explore why people behave the way they do and to identify ways by which that behaviour could be changed. The ideas thus generated are then evaluated and prioritised with a view to designing appropriate nudges. Once an approach has been agreed, it can be prototyped and evaluated. Those that look promising are completed and deployed for evaluation within the company.

"In the second year," says Coventry," we are looking at different behaviours such as acceptance of cookies and getting people to report a suspected threat, and also the role of personality in behaviour. We are particularly interested in impulsivity, and our work suggests that more impulsive individuals are less likely to behave securely – going with the first, most convenient option rather than the most secure. This means that they are more likely to need to be 'nudged'. We have found that the appropriate redesign - choice architecture - can ensure that their automatic impulsive behaviour still results in secure outcomes."

"With BYOD," adds Briggs, "we don't know that much about the context in which it will be used." User-centred design requires context: where do people work on these devices? What work do they take home? Which apps are on the device? What sort of protection does the device have? What are the psychological differences that derive from the fact that the device belongs to the person and not the company? What impact do the user's level and length of commitment to the organisation have? "We want that rich context before we can understand the way people use them, then the nudges will develop."

Says Coventry, "Users might not necessarily be able to express the problems they're having. If there's no one there who acts in a security capacity with any depth of knowledge, you have to find slightly different language to get people to talk about the issues."

Iryna Yevseyeva, one of the project researchers, presenting at a RISCS meeting

The understanding they develop, along with the scenarios they are working on, feed into van Moorsel's mathematical models (see box, overleaf), both as an attempt to understand the problems and as an eventual guide to developing nudges. An example scenario: a user uploads company data onto a personal device because it's easier to carry home than a laptop, leaves it where it can be played with by a child, who in turn accesses or changes the data, which might then be synced back onto company servers or sent elsewhere.

Ultimately, ChAISe develops tools – for example, apps to run on users' devices – that will help people to make better decisions without dictating to them: "a nudge in the right direction".

Papers the project has published study extracting user preferences; the ownership and management of devices in use; and the dynamics of influence and the allocation of control between an influencer and a user faced with many uncertainties. These variables may include context in a dynamic situation, changing user preferences, and changes in the surrounding environment, as well as tradeoffs between security and productivity. There might also be limitations - for example, ethical or financial - to what can be modified to influence users within their context.

Monitoring users over time gives the influencer the chance to adapt and target nudges. Says research associate Iryna Yevseyeva, "We want to study the level of influence needed to change choice. By being able to evaluate whether it makes sense to influence a particular user in a particular situation, we want to aid the influencer to provide an adaptive influence, which should be better than influencing always or never. Our models are helpful for deciding when to influence, how, and how much."

Choice Architecture for Information Security is one of four main themes of the Research Institute in Science of Cyber Security, funded by EPSRC, GCHQ, and BIS, a collaboration between government and a group of universities to consolidate existing research and build upon it in new directions in order to create a science of information security. ChAISe is led by **Aad van Moorsel** at Newcastle University. The other three themes are Cyber Security Cartographies, led by **Lizzie Coles-Kemp** at Royal Holloway; Games and Abstraction, led by **Chris Hankin** at Imperial College London; and Productive Security, led by **Angela Sasse**, the Research Institute's director, at University College London.

Wendy M. Grossman, freelance journalist

Where do mobile phone users look for information about security?

This work is funded by EPSRC Grant Number EP/K006568/1