Map quest

“It’s important to us that we use eyes and ears that don’t have a specialist security background,” says Lizzie Coles-Kemp, by way of explaining why the Cyber Security Cartographies (CySeCa) project she is leading is inspired by work from the arts and humanities world and includes social media and human-computer interaction researcher Makayla Lewis as well as the security engineers and researchers Gerhard Hancke, Lorenzo Cavallaro, Allan Tomlinson, Davide Papini and Geraint Price. CySeCa is Royal Holloway’s contribution to the Research Institute in the Science of Cyber Security, funded by EPSRC, 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.

Most research into security starts with an expected outcome: a new or improved technology, an innovative set of tools, or novel strategies for countering a new and growing problem. While CySeCa hopes to generate new technologies and strategies, its starting point is different. CySeCa is an open-ended project that starts with some fundamental research questions and in-depth interviews with security practitioners to elicit how social and technical security controls are commonly used. In an inductive project, the researchers build their theories from the results of analysis rather than beginning with a theory and looking for evidence to support or refute it. The research is expected to continue with a combination of visual methods and host and network analysis that together are intended to expose how different user communities engage with technologies, handle information, and influence behaviour. The key questions the researchers are trying to answer: what stops security practitioners from being as effective as they would like to be? Is my organisation secure?

“We have no hypothesis initially,” says Coles-Kemp. Instead, “We have a problem space we’re looking at and we derive our hypothesis from researching that space. We will look at the user experience in the broadest sense - why users exchange information the way they do and the value they put on it: sociology in design. We will likewise look at inferring the behaviour of devices, computers, and systems, their interactions and dependencies, and whether such low-level technical “maps” can be fruitfully enriched by the user experience we’ve uncovered (and vice-versa).”

The open-ended nature of the work makes sense when you understand what they’re looking for is the “unknown unknowns” - that is, the gaps in our knowledge and understanding that we don’t know exist. Maps are a logical approach: once you’ve located the things you know and the things you know you don’t know it’s easier to see where the empty spaces are.

A senior lecturer in information governance and security management at Royal Holloway’s Information Security Group, Coles-Kemp herself has a mixed background: she began with a degree in Scandinavian Studies and Linguistics before moving into security work with jobs in industry, auditing, and, latterly, academia.

The organisational research starts with a series of semi-structured, lengthy interviews with security practitioners “to find out how they build relationships and influence practice”. The interviews ask, for example, what the practitioners do all day, what their significant relationships are and how those were built, the kinds of issues they face in dealing with people, and the importance to them of the information security community. Once the project team has a baseline understanding of these questions, the research will continue as a combination of organisational research and network and host analysis via audit logs and other computer records of user activity.

“What we expected from this initial activity,” says Coles-Kemp, “and what is coming out, is that security practitioners see themselves as slightly separate to the organisation they work in. However loyal or embedded they are, or however long they’ve been there, they all put themselves as security practitioners first and organisation members second,” says Coles-Kemp. “Whether it’s a big distance or a close-run thing they’re all coming out with that perspective. Identity-wise,
being a security practitioner is clearly a very important thing to them, though the organisation may be important to them, too.”

Feeding back to the research participants and seeking their input on findings is an important aspect of the organisational research. The material gathered in this initial baselining activity will be used to build a visualisation – “probably a large, rich picture”; all the participants will have the opportunity to reflect on and add to the narrative that’s begun to form. Later stages are likely to include participatory workshops and rapid prototyping of visualisation ideas to see how people interact with different tools.

“We want to critically map the information security community and get them to take part in a self-reflective process so we can think about who we are in the cyber era and see what kinds of novel intervention will help them get where they want to be,” says Coles-Kemp. “What’s exciting for us is that we get to combine the inductive, innovative theme with the classic deductive (network and host) analysis that builds on machine learning research.”

Gerhard Hancke, a Fellow with the Information Security Group and one of several principal co-investigators on the project, is working on bridging the gap between the technical side of the project and the “softer” work being done by the project’s visual artists, who are more used to working in psychology and human-computer interaction. For him, the hardest part is getting to grips with visualising organisational data. Despite his background in software engineering, it’s clear to him that more traditional methods of surveying security issues such as written reports won’t suffice because of the struggle to get those read and understood.

“The problem is that in security you’re looking at a very diverse, large space,” he says. “One security manager and a small team of people are trying to get a handle on a very large company with a dynamic IT estate.” The security team may in fact have very little control - and they have to communicate their concerns to upper level management who have an entirely different vocabulary for discussing business issues.

“Words might be better,” he says, “but pictures are the way to get most people to understand what’s going on.” Bringing these different approaches together to find one that is acceptable to both sides is, he says, a genuinely hard problem.

Yet both sides are necessary: security involves many aspects of a complex system of humans and technology. Just studying audit logs risks inferring patterns and traits that are not really true. Just asking humans risks being led astray: people do not always behave the way they say – or think – they do.

One of the first themes that’s emerging from the project’s earliest interviews with a range of security practitioners from various sectors, is that many struggle to know how best to relate to the security issues of other user communities within an organisation and to communicate the connection between the issues and standard security approaches. This is where visualisation may help. Mapping their influence throughout the organisation may make it easier for security practitioners to understand who’s listening to them and also to demonstrate to managers what they do and how it can be improved. A glue layer might be a geographical or organisational map; over it may be layers based on technical and organisational data that together help define a narrative that leads to designing new layers. Two very diverse approaches to mapping are being used initially. Makayla Lewis (User Experience PostDoc and Visual Narrative Practitioner) has been using cartoons in the first year of the project to draw out the social networks that form around security practitioners:

At the network level, PostDoc Davide Papini and co-I Lorenzo Cavallaro have spent the first year working on the visualisation of network traffic to better support activity analysis:

Both Coles-Kemp and Hancke hope that the eventual result of their work will be interventions that are tangible enough to be used and applied effectively. Both stress, that their opening approach is just a first idea: they talk as though the less conventional and more technologically disruptive the approach they wind up with the happier they’ll be.

“All bets are off at this stage,” says Coles-Kemp. Cyber Security Cartographies is one of four main themes of the Research Institute in the Science of Cyber Security, funded by EPSRC and GCHQ, 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. CySeCa is led by Lizzie Coles-Kemp at Royal Holloway and supported by co-investigators Lorenzo Cavallaro, Gerhard Hancke, Geraint Price, and Allan Tomlinson. The other three themes are Games and Abstraction, led by Chris Hankin at Imperial College; Choice Architectures, led by Aad van Moorsel at Newcastle; and Productive Security, led by Research Institute director Angela Sasse at UCL. The overall goal of the Research Institute is to create good science and also to have an impact on the world of security management.