Cyber Security Cartographies

RISCS
Research Institute in Science of Cyber Security

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 leads blends humanities and technology and includes visual artist and human-computer interaction researcher Makayla Lewis as well as the security engineers and researchers 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 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.

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 is generating new technologies and strategies, it is an open-ended inductive project that began with some fundamental research questions and in-depth interviews with security practitioners to elicit how social and technical security controls are commonly used.

"We had no hypothesis initially," Coles-Kemp says. Instead, "We have a problem space we're looking at and we derive our hypothesis from researching that space. We 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 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 combination of social and visual methods and host and network analysis is 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?

A senior lecturer in information governance and security management at Royal Holloway's Information Security Group, Coles-Kemp's own background is mixed, beginning with a degree in Scandinavian Studies and Linguistics before moving into security work with jobs in industry, auditing, and, latterly, academia. Over the project's first two years, the group learned the importance of pluralistic tools and also that each network - human and data - requires a different type of abstraction.

"What we hadn't appreciated and what's come out is the asymmetry of these networks," she says. "We have to have a visual form that understands the relationships from the perspectives of the different participants in the networks group - what is a close tie to one is not to another."

The human side of the project uses cartoons created by Makayla Lewis (User Experience PostDoc and Visual Narrative Practitioner) as a way of capturing the information given in lengthy, semi-structured interviews studying how security practitioners build relationships and influence practice. Research had previously shown that social interactions, values, and goals influence what people do with their data, but existing security tools fail to incorporate them. The cartoons, which illustrate the relationships and postures the participants describe, were then given to the participants themselves to spark a feedback loop of further discussion. Finally, removing the visual narrative leaves a skeleton suitable for social network analysis showing clusters of people, how they cluster, and what their sharing networks are.

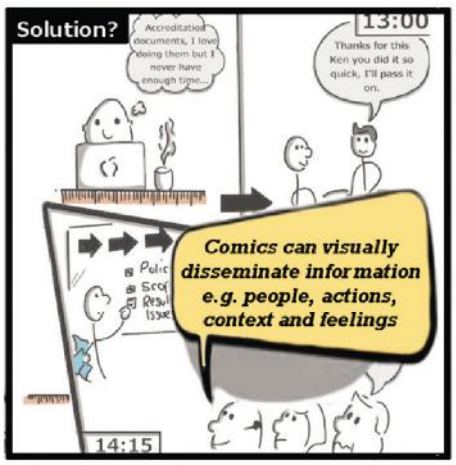
The VOME project

A suggestion of what the eventual shape of CySeCa might look like comes from an earlier Coles-Kemp project, Visualisation and Other Methods of Expression (VOME), which concluded in 2011. In this three-year interdisciplinary project, researchers from Royal Holloway's Information Security Group worked with others from the University of London, Salford University, Cranfield University, Consult Hyperion, and Sunderland City Council to study how people engage with the concepts of online privacy and consent. Both these areas pose challenges for researchers seeking to comprehend user behaviour: consumers struggle to understand the decisions they're being asked to make and to assess risk, and the nuances of the decisions they make are often lost.

"We used various techniques including participatory theatre to engage with users who are not normally consulted about privacy design and who may not be able to respond to normal kinds of engagement," says Coles-Kemp. The variety of techniques they used, which also included family workshops, card trading games, and community art collages, aimed to expose not only the users' engagement with particular technologies but the social context. "We did a lot of work with families and their use of technologies to look at how public services are delivered within the home," she says.

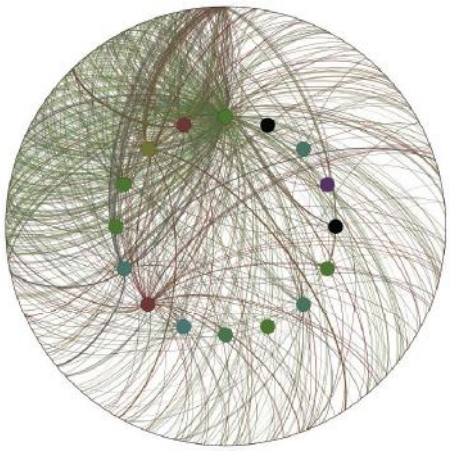
Coles-Kemp doesn't expect CySeCa to go as far as participatory theatre, but some of the other techniques used in VOME, such as card trading games, are a more likely fit for security practitioners. "We sense there's a real interest in alternative methods," she says. Like CySeCa, the VOME was open-ended; at the end, besides a privacy card game, the project produced a participatory music video and developed participatory engagement techniques and design principles that are used in a number of public sector contexts today.

"Yet when we started we had no idea that was where we'd go," says Coles-Kemp.



An example from one of Makayla's cartoons

Separately, network visualisations created by postdoc Davide Papini and co-investigator Lorenzo Cavallaro, capture quantitatively how data moves across the same participants' technology network: the more traditional type of network analysis of audit logs and other computer records of user activity using machine learning techniques.



One of Davide's visualisations of network traffic between 20 nodes

"They were separated initially because paradigmatically if you want to look at people and people networks the unit of analysis is people, and if you're looking at communications networks the unit of analysis is the technology and the data," Coles-Kemp explains.

In the project's third phase, the two analyses must be connected to give the full picture; the first step in this process is to identify the touch points. "Social geographers talk about space and place," says Coles-Kemp. "Space is the physical environment we're talking about; place is the values and meaning we attach to that space. Different groups within one SME may associate different meanings and assume different values and different goals." And then, she adds, "Sitting in among all this you have a policy about what you can and can't share, what you have to protect, and how different groups interpret that policy. If you interpret the rules differently would that make a better environment?"

A crucial element of the work is bridging the gap between the technical and visual sides of the project. What makes this aspect difficult is its cross-disciplinary nature. For technical specialists in particular, the hardest part is getting to grips with visualising organisational data. A background in software engineering isn't enough by itself; traditional methods of surveying security issues such as written reports won't suffice because of the struggle to get those read and understood. This was one of the project's early lessons: security work requires looking at a very diverse, large space and often requires a very small team - say, one security manager and few others - to try 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. Although words might seem the more logical choice, most people find pictures an easier way to understand what's going on. Bringing these different approaches together to find one that is acceptable to both sides has proved to be 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 emerged 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.

The project team 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.

The open-ended nature of the work makes sense when you understand that 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.

Cyber Security Cartographies is one of four main themes of the Research Institute in 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**, **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.

Wendy M. Grossman, freelance journalist

This work is funded by EPSRC Grant Number EP/K006266/1