EVERYDAY SECURITY: A MANIFESTO FOR NEW APPROACHES TO SECURITY MODELLING

RENÉ RYDHOF HANSEN
AND LIZZIE COLES-KEMP

THE IMPORTANCE OF EVERYDAY SECURITY

'Everyday security' describes the ability of an individual to go about their digital activities with confidence and trust. The importance of everyday security in the delivery of government services has greatly increased over the last decade. For example, the UK government's *'digital by default'* agenda sets online service delivery as the primary mechanism for implementing essential civic services, including housing, employment, education, healthcare, welfare, transport, food and criminal justice services. These are provided by central government departments that support the *digital by default* agenda. Consequently, the majority of UK households digitally access essential civic services, with some of the largest increases in digital access occurring in low income households. The everyday security needs of such a diverse user community are highly varied but the design of service security is often unresponsive to this variety. This results in parts of society being unable to comply with the security requirements of the service.

One example is the use of passwords to access essential services. Whilst much focus in internet safety is on 'one user-one password', the reality is that many service users rely on 'social proxies' (other people such as carers, family and friends) to help them login and administer, for example, health, welfare, employment and housing services. So, the digital service security question is not so much one of secure passwords but more one of enabling the individual to manage their social proxy and to be able to detect if that social proxy begins to work against their interests.

MANIFESTO FOR EVERYDAY SECURITY MODELLING

In order to respond to these challenges, the underpinning models and philosophy of service security need to be re-designed. We need to understand what needs to be secured, and then what security means in this context. We also need to design for the conflicts that emerge between service stakeholders. This requires techniques for modelling that accommodate the goals of security whilst acknowledging that these may change over time.

Such modelling would be in contrast to traditional models that rarely scale well and usually do not have effective means of modelling implicit, inconsistent, or contradictory goals. Whilst we're good at designing the possible and necessary security features of a system, our traditional approaches do not typically respond to the needs of everyday security. This is, in part, because traditional models focus on capturing and reasoning about protection of information and computing assets.

The security philosophy of everyday security also differs to the security philosophy that informs traditional security. This is because the focus of traditional security design stems from the security concerns voiced by the technological and policy security communities. As the social proxy example shows, these concerns are at times misaligned with the concerns related to the everyday security experience of citizens.

INTRODUCING A FAMILY OF MODELS

Recent research suggests that a family of security models (and modelling processes) are needed to respond to both system and everyday security concerns, starting with exploratory models and moving to more classic, mathematical models once the goals, conflicts and inconsistencies are defined. At the same time a transformation in security management practice is required. This means that together with the more traditional, mathematically-informed approaches to risk assessment and audit, approaches from design and the humanities that encourage active and reflective end-user participation and engagement are needed. Including such participation in security management approaches will help stakeholders identify conflicts and ambiguities in the service design. Such a family of modelling techniques provides a landscape in which interdisciplinary teams can work together—both in academia and in practice—to leverage the strengths of each discipline and respond to the complex problem of everyday security.

ABOUT THE AUTHORS

René Rydhof Hansen is a computer scientist and an associate professor at the University of Aalborg. Lizzie Coles-Kemp is a professor whose work focuses on the social aspects of information security at the Information Security Group, Royal Holloway University of London.