

Walking the line: The everyday security ties that bind*

Lizzie Coles-Kemp¹ and René Rydhof Hansen²

¹ Royal Holloway University of London, UK

`Lizzie.Coles-Kemp@rhul.ac.uk`

² Aalborg University, Denmark

`rrh@cs.aau.dk`

Abstract. In this paper we argue that in contemporary society a form of security emerges that is qualitatively neither technological nor social but that is truly sociotechnical. We argue that everyday security is a form of sociotechnical security co-constituted of both technological protection mechanisms designed to protect assets and of relational social practices that enable people to build and maintain trust in their daily interactions. We further argue that the complexity of real-world information security problems requires security models that are able to articulate and examine security as a sociotechnical phenomenon and that can articulate and examine the results of interaction between these two security constructions. Security must be modelled to acknowledge, at least, the connection between an individual's security needs and the protection of assets if it is to help design secure services with which citizens can safely engage. We exemplify these attributes from case studies conducted as part of two sociotechnical research projects: the UK government and research council funded Cyber Security Cartographies (CySeCa) project and the EU FP7 funded project TREsPASS. These are introduced to discuss the potential for a family of modelling techniques. In this paper we examine the attributes of everyday security problems and reflect upon how such a modelling family might influence both academic research and practice in contemporary information security.

1 Introduction

The subtleties of secure human-computer interaction are often hard to pin down. The design of security technologies focuses on the protection of data and the usability requirements for that technology. Rarely does the security technology design process address the human security needs of the individual where human security needs fundamentally address a sense of confidence to achieve well-being e.g. financial well-being and emotional well-being. In security theory, protection

* This paper should be cited as: Coles-Kemp, L. and Hansen, R.R., 2017, July. Walking the Line: The Everyday Security Ties that Bind. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 464-480). Springer, Cham.

from harms is sometimes termed negative security whilst the freedom to achieve human security needs such as financial security or well-being is termed positive security [25, 33]. Whilst security technology design is well-established in terms of protecting data and by extension, the owners and dependents of that data, from harm, security technology design is less well-established in enabling the freedom to use that data in a way that enables individuals to meet their other human security needs. For example, when a granddaughter helps her grandmother conduct important on-line activities [23], e.g., by conducting on-line banking or interacting with the on-line welfare system on her grandmother's behalf, the granddaughter is acting as a so-called social proxy, a position of power that can be either supportive or abusive. In a supportive situation, the grandmother may want to have the freedom to share her access with her granddaughter as a means of enabling financial security through the receipt of care from her granddaughter. Similarly, when a grandmother gives her granddaughter advice on which friends to block or whether to respond to a social media post, the grandmother is acting as a type of gatekeeper that in a supportive situation enables the granddaughter to maintain her social relationships.

Although such usage scenarios are not uncommon and have obvious consequences for the security of the system and the safety of the actors, it is a very rare digital service design that takes such scenarios into account and even rarer that the underpinning system has an underlying security model that can capture the many subtle aspects of such scenarios. In this scenario the sharing of passwords, the incorporation of those typically considered to be non-users of a system is often built around the human security need to build and maintain trust relationships to engender confidence and a sense of well-being, rather than the focus on protecting data on a system. For this reason, standard technical responses of delegated authority and role-based access control do not fully suffice because these technological responses focus on the data and system protection needs, with an assumption that these fully correspond to the human security needs.

In the example outlined above, the technological problem is one of ensuring managed access, the human problem is one of preventing outsiders from gaining access and of enablement to meet the fundamental need of a sense of well-being through the receipt of care and support from family members. The technological controls respond to the former human security problems but not the latter ones. The technological support needed for the latter human problem is one of building and maintaining care relationships and managing the trust relationships needed to support those care relationships.

The focus of information security practice and academic study has traditionally been squarely aimed at IT security [16]. IT security can be explained as the protection of computer produced data and information and the associated protection of the infrastructure that makes possible the production, circulation, protection and curation of that data. However, the protection of data is not solely a question of IT security. The widespread adoption of digital technology across all strata of society and the increasing reliance by governments and industry on

engagement with citizens through digital media brings data protection into the realm of everyday life for citizens. If data protection is to make sense to citizens as they go about their everyday lives, IT security must clearly link to human security needs such as those related to an individual's financial, health, physical well-being and stability. This paper asks how might we model data protection in this everyday realm, how this model might improve understanding of everyday security practices and how it might help broaden IT security.

2 Security: a divided field of study

The separation that we can see in information security between the human security needs of the actors and the data security needs of the infrastructure is common to many studies of security, not only technological ones. As McSweeney highlights in the introduction to "Security, Identity and Interests: A Sociology of International Relations" [25] security is a term that is used in a wide range of contexts in all aspects of life and it can refer to people, things, practices, external events and innermost feelings. The study of security is equally broad and is studied from many different perspectives [28] across many different disciplines including Politics and International Relations e.g. [29], Geopolitics e.g. [8, 1], Critical and Social Geography e.g. [13], Psychology e.g. [7, 4], Sociology e.g. [12, 26], Computer Science e.g. [21, 20] and Maths e.g. [3]. These different perspectives of security often influence each other. For example, Security Studies focuses on the protection of the State and is often located within Politics and International Relations but also crosses over into Geopolitics in order to examine the security of borders and of populations e.g. [1]. Regardless of the focus of security study, there is a tendency to focus on the materiality of security using epistemologies related to positivist forms of knowledge [25]. Materials of security range from battlefield technology to surveillance technologies and information access control systems. Just as traditional international relation security theorists emphasise the use of the military, traditional computer security theorists emphasise the use of cryptography and access control protocols. In pursuing this focus on the materiality of security, traditional security studies across all disciplines tend to focus on the externalising of security problems and ignore the question of the internalising of security problems within the individual and the central question of how the individual conceptualises security [25]. However, the relationship between the externalisation of security problems (how they are articulated and framed) and how an individual conceptualises security is an important dimension to secure human-computer interaction.

Studies of security do, however, differ in the families of referent objects that are the focus of each type of study [25]; a separation often motivated by academic rather than governmental politics. In the case of information security, the primary referent object is the computer generated data or information with a secondary referent object being the computational infrastructure that supports the generation, storage, circulation and curation of the data, e.g. [24, 3, 17, 34, 2, 21]. When humans are introduced into this picture of information security by

way of sociotechnical security modelling, they are typically subjugated to the needs of the protection of data and their actions are analysed in terms of their contribution to or detracting from the protective act. The implicit assumption in this type of modelling is that the protection of data and the concomitant protection of the technological infrastructure is a human security need. Examples of this genre of security modelling include: [31, 11]. Traditional models of information security extended to include human action therefore reflect this assumption that human actions related to the needs of data protection are modelled. However, human-centered studies of information security consistently demonstrate that the relationship between data protection and the needs of individuals is complex [30, 19]. In order to achieve this the perspective of information security needs to be broadened to include a focus on the connection between human security needs and IT security needs and the development of a meaningful connection between the two.

3 The case for broadening the focus of information security

Over the last two decades there has been a growing call for the broadening of security studies in the international arena [25]. Sociologist Bill McSweeney argued that security in a broader context should be regarded as both protection *from* (negative freedoms) and the freedom *to* (positive freedom) [25]. In terms of negative freedom there is a freedom from threat and is, as McSweeney argues, characterised in objects such as locks, doors, walls etc. that protect things and prevent things from happening. However, there is another form of security, this is adjectival rather than normative — “secure” rather than “security” — a quality that conveys the essence of making things possible. This related form is “freedom to” rather than “freedom from” and should not be seen as an alternative to the more traditional conceptualisation of security as freedom from threat but should be seen as an interrelated concept. From this perspective access control to a particular data file, for example, should not only be seen as a mechanism for the protection of the data but also as the granting of access to data that empowers an individual to build and sustain relationships as they go about their daily activities. In this case the human security need is focused on the relational use rather than on the material protection of data. If the need for the material protection of data is to be understood, the protection mechanisms must support, and be understood to support, the building and maintenance of relationships in order to capture the co-constituted nature of the negative security protection of the data (data protection need) and the positive security enablement of a sense of security derived from trusted human relationships (human security need). This broader view of information security that more fully captures the relationship between data and human security needs is highly relevant to the understanding of secure human-computer interaction.

In the following two sections we examine how information security is traditionally modelled when the primary referent object is data and how relational

security might be modelled. We start with a description of Bell/LaPadula, Role Based Access Control and Harrison/Ruzzo/Ullmann modelling and explain the focus of these classic access control models. We explore the security goals that can be expressed through such models. We then move to a description of two rich-picture based modelling attempts to articulate patterns of relational security within a scenario.

4 Modelling the granddaughters and grandmothers case using traditional security models

From the granddaughter and grandmother example in the introduction section, it is clear that the (strategic) security needs of the grandmother and granddaughter example is quite different from the kind of security formalised in the classic access control models such Bell/LaPadula (BLP) [3], Role-Based Access Control (RBAC) [34], and Harrison/Ruzzo/Ullmann (HRU) [17]. In the following sub-sections we explore how such access control models can be applied in the granddaughter and grandmother example and, in particular, to what extent they are able to capture and support (and possibly enforce) the grannies' security goals.

4.1 Bell/LaPadula (BLP)

The Bell/LaPadula access control model, also called the multi-level security (MLS) model, was originally proposed as a solution to the problem of Trojan horses stealing information in classified military systems. In the BLP model, every information source (called an object in the BLP terminology) is assigned a security level, e.g., secret or top secret (security levels are assumed to be totally ordered), and every user or user-process of the system (called a subject in the BLP terminology) is assigned a corresponding clearance level, indicating the level of information the user is allowed to access. The BLP model then defines (and enforces) security by preventing users from reading information above their own level (no read-up) and from writing information below their own level (no write-down). In other words, a user with a "secret" clearance level can only read information that is classified as secret or lower and can only write information at level secret or higher.

In order to apply the BLP model in the context of the granddaughter and grandmother scenario, we must first identify the relevant objects (information sources) and subjects (information sinks, e.g., users). In the interest of readability, we shall use the terms "user(s)" and "subject(s)" as well as "information (sources)" and "objects" interchangeably. An obvious first choice is to let grannies and granddaughters be subjects and then define the information provided by on-line services, e.g., Facebook, to be objects. Even with this simple modelling, we have captured essential security features/requirements for typical on-line services: the login process and the privacy/security settings of the service. In principle, a grandmother could classify information and/or activities

meant to be shared with a granddaughter, such as games provided by the on-line service, at a low security level and other, more sensitive information as at a high security level. In this way, the grandmother could make a “low level” login when sharing the on-line account with a granddaughter, e.g., for playing games or simply sharing information, and a “high level” login when using the on-line service for private/personal purposes. Using the framework of the BLP model, the set of security/clearance levels is subject to very few constraints (technically they must form a lattice) and can be constructed with arbitrarily high granularity and thus cover most use cases occurring in practice.

Of course, for the above access control to work, grandmothers would have to manage on-line identities with several security/clearance levels and, potentially, several completely different digital identities with different levels of authorisation and access and, not least, with different login credentials — a daunting task for even the most tech-savvy granny. One traditional way of solving or at least alleviating the problem of managing multiple identities, or roles, is to use the role-based access control model which we will discuss next.

4.2 Role-Based Access Control (RBAC)

The notion of security that underpins and motivates the RBAC model is the same as for the BLP model discussed above: essentially preventing users with a given clearance level from accessing information at a higher security level. However, in addition, the RBAC model explicitly acknowledges that (1) a user may interact with the system in several different capacities, e.g., both as an administrator as well as a “normal” user; (2) some system activities may be performed by any user in a group of users, e.g., any user belonging to the “auditors” group may perform certain system audit functions. In the RBAC model this is captured by introducing *roles* that can be assigned to users in such a way that a user may have several roles and a role may be assigned to several users. Roles are typically defined by the collection of functions (on the system) that a user performing that role must have access to. This approach has several advantages over “raw” BLP: it makes administration of access control policies much easier (at least for large systems with many users and security levels) and more robust since the required access rights for specific items of information can now be specified “abstractly” based on what the information should be used for rather than on an individual basis. This also makes it easier to manage when a users’ access rights should be expanded/revoked.

For grandmothers wanting to play on-line games or share on-line information with their granddaughters, the RBAC model offers a cleaner and easier way to manage security than the BLP model. Instead of managing different identities and several on-line accounts and their concomitant access control policies, it is a matter of specifying the different roles a user (grandmother) can perform in a given on-line service. As an example, a grandmother could specify a “sharing” or “public” role and a “private” role where the latter is obviously used for interactions the grandmother does not necessarily wish to share with her granddaughter, and the former for the kind of shared on-line experience(s) mentioned

above, e.g., playing games or watching video clips together. The notion of roles can be refined almost endlessly, facilitating a very granular approach to access control: the grandmother could specify roles to use with each of her grandchildren or specify roles based on age intervals (of her grandchildren or, indeed, any other family member or friend) ensuring that even the youngest grandchildren will not accidentally see or access information intended for an older audience.

Although RBAC offers simpler management of access control policies, it is important to note that the underlying security notions of the RBAC model are equivalent to those of the BLP: everything that can be (conveniently) specified in the RBAC model could (much less conveniently) be encoded in the BLP model.

4.3 Harrison/Ruzzo/Ullmann (HRU)

The Harrison/Ruzzo/Ullmann model [17] of access control significantly extends the previous access control models by allowing access control rights to be changed *dynamically*, i.e., during operations, and also makes it possible to *delegate* authority to other subjects. Unfortunately, the increased expressivity of the HRU model also makes it much more difficult to reason about the security of a given system, since it is not generally possible to adequately account for all the dynamic behaviour of a system. In fact, determining the security of a given system in the HRU model has been shown to be *undecidable* in the general case [17].

With the HRU model a grandmother can, dynamically and temporarily, grant her granddaughter access rights to information and authority to perform certain functions on behalf of the grandmother, e.g., in order to play on-line games, all *without* letting the granddaughter use grandmother's login credentials. Another use of the HRU model would be for a grandmother to *delegate* authority over certain aspects of an on-line service to, e.g., a granddaughter. The granddaughter (with delegated authority) would then be able to both act on behalf of the grandmother, but also potentially to *further delegate* authority, e.g., to a carer or another family member.

Although the HRU model solves (part of) the problem of a grandmother sharing login credentials with her granddaughter in order to play (on-line) games and engage in on-line activities, it also introduces a much more complex dynamic (security) behaviour that is potentially even harder to manage than different on-line accounts. Even more to the point, the formal access control models discussed above, i.e., BLP, RBAC, and HRU, all miss the important point that maybe a grandmother deliberately *wants* to share her login credentials with her granddaughter in order to form a stronger bond, i.e., strengthen her *relational security*.

5 Modelling the relational security aspects of granddaughters and grandmothers

The granddaughter and grandmother study was conducted as part of a UK research council funded research project titled Visualisation and Other Methods of

Expression (VOME) that gathered everyday security narratives in the context of digital services from communities that hitherto had not been part of the digital service debate. In particular, the project focused on digital service use and the associated security needs of underserved communities, including: lower socio-economic groups, long-term unemployed, use of digital services within families and families separated by prison. The project developed methods of engagement that were designed to elicit everyday security narratives and develop an articulation of human security needs in the context of digital service use [5]. One of the project findings was that human security needs were related in large part met through the management of relationships and the development of new relationships [6, 32]. In two follow-on projects, the UK research council funded research project titled Cyber Security Cartographies (CySeCa) and the EU FP7 funded project TREsPASS, methods of visualising and modelling human security needs were developed. In both projects methods of data elicitation and abstraction were developed that used techniques to gather narratives of everyday security and then to abstract relationship networks from the narratives. The approaches were based on a soft systems modelling technique known as rich picturing [27].

The goal of the CySeCa project was focused on understanding the intersection between digital data protection mechanisms and relational security practices. There were two work streams within the project, one that examined relational security practices from the perspective of human social networks and one that examined data protection mechanisms at the digital network level. Both work streams developed analytical methods to identify and analyse the information sharing and protection activities taking place within each type of network. They also developed visualisations to communicate the security practices and mechanisms in operation within each network. In this paper, we use an example of the relational security work from CySeCa to illustrate how the modelling of relational security might be undertaken. In one case study in the CySeCa project, the relational security work stream examined the sharing and protection of information flows within a community centre providing digital service support for essential service such as housing, welfare, food, health, education etc. [22]. The analytical goal of this study was to explore how people feel about using the centre and the different roles that the centre plays in their lives. In particular, in this study we wanted to understand how people felt about sharing information while at the centre — both as part of the process of obtaining the practical assistance they need in accessing on-line services and also as part of the socialising and social network building that takes place at the community centre. In this study we developed visual and written narratives to show how people experienced information sharing and protection within the community centre and then used social networking techniques to show the trust bonds between people in the community centre and the information that flows through and is protected by those bonds.

This type of approach could be used to produce visual and written narratives as shown in Figure 1 to describe the interaction between grandmother and granddaughter. In particular, these narratives show the role of the “non-users” or

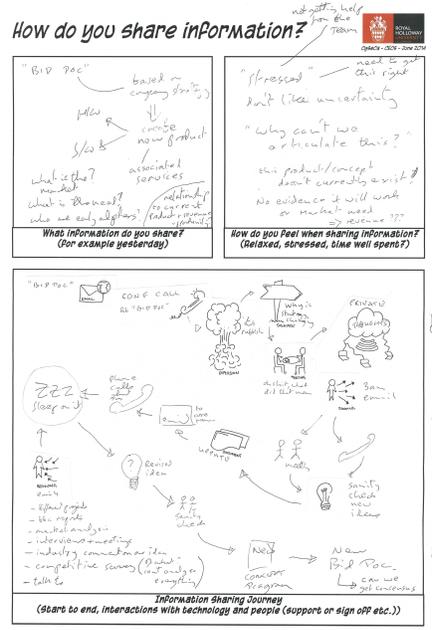


Fig. 1. A storyboard of everyday information sharing

the social proxy who is helping the service user to carry out a task. For example, such a narrative might show the granddaughter logging on to on-line banking on behalf of her grandmother or the grandmother giving advice as to how the granddaughter might respond to a conflict on Facebook. These narratives could then be abstracted using social network analysis to show the trust relationships between grandmother and granddaughter.

Whilst the CySeCa work was successful in depicting the relational security practices and the relationship of those largely positive security practices to the human social network, the modelling work did not articulate the interaction between the relational security practices and the digital security practices which largely reflect negative security of data protection. The EU FP7 project, TRES-PASS [35] developed methods and tools to quantify, analyse and visualise sociotechnical information security risks in dynamic organisations. The TRES-PASS project included a work stream to explore the visualisation of sociotechnical information security risk. The goal of this work stream was to extend the state of the art in cyber security risk tools by developing visualisations that combine information visualisations with techniques from critical cartography and digital humanities to articulate different sociotechnical dimensions of risk and provide tools through which to explore these dimensions. A form of participatory diagramming and physical modelling [18] was deployed in TRES-PASS using physical modelling tools such as LEGO as shown in Figure 2. The modelling approach places social data gathered directly from case-study participants at centre-stage

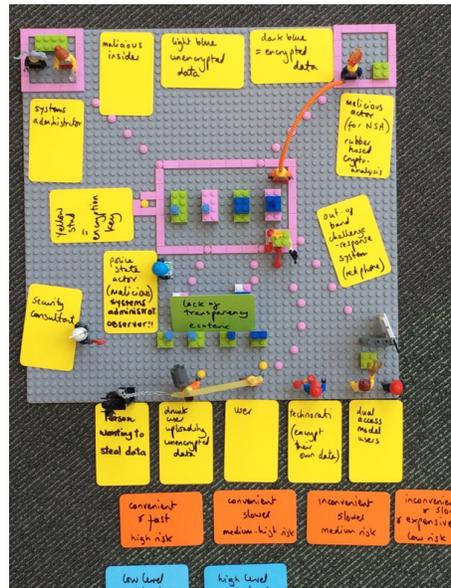


Fig. 2. LEGO model of a data sharing and protection scenario

which has the effect of broadening the traditional process of information risk assessment, accessing social data as a starting point for identifying and then scoping the issues that are of paramount interest to the stakeholders in a risk scenario.

The physical modelling process uses the following steps to brainstorm risk scenarios: (1) A context or scenario for information sharing and protection is agreed with a participant group. (2) Participants identify their core values and the basis on which they share and protect information. (3) Participants are given physical modelling material, for example LEGO building bricks of given types and colours, selected so as to encode the movement of shared information and data, actors, and devices. (4) Participants collaboratively model the chosen context or scenario in the physical modelling medium and, during this collaborative process, discuss the types of information generation and flows that occur within this space. (5) Participants identify information sharing and protection narratives relevant to the context.

Open questions and provocations are used by the modelling session facilitators to encourage participants to focus on a particular sociotechnical information security risk theme and thereby draw out both the positive and negative security responses to the scenario. This type of approach could be used to show where the emphasis of control is in the granddaughter and grandmother scenario and to enable analysis of where both the human and data security needs might not be met.

6 Modelling information security’s broader view

The TREsPASS’ physical modelling approach, whilst it combines the positive and negative security perspectives, is still focused on human security needs as the referent object rather than data security needs as is the case for the traditional security models. This difference in referent object focus makes combining the models a complex task. The challenge that then emerges is how to enable interaction between the formal data security models and the relational models of human security needs. In everyday terms this is particularly challenging because the referent object (the individual) is inherently unstable [25].

Formal security models are typically regarded as incapable of capturing or modelling the proximity and relational attributes and aspects of human security needs. Indeed, much of the terminology and many of the fundamental ideas and concepts in information security originate from military needs and military thinking with a strong focus on “asset protection” and automated (or automatable) technological protection mechanisms e.g., network firewalls and access control models [34, 24, 17, 3]. Even though the traditional security models have been successfully applied in many cases both to design and reason about the security of a system, there are a number of challenges and pitfalls with this approach. First of all, there is an implicit assumption that it is possible to identify and define all the relevant assets and authorised entities in a system. Furthermore, the security goals (of the authorised entities) must be aligned and non-contradictory. Finally, although some formal security models allow for dynamic changes in the model, e.g., dynamic updates of access control lists, typical (formal) security models assume that the underlying security goals of a system do not change (too often) and that such changes are handled “out of band”. This traditional asset-based approach to information security contrasts with a focus on human security needs where security is a property of relationships and enables a form of security located in how we build relationships within our kin and friendship networks. In order to understand this type of security a different type of knowledge is developed from a socially-constructed knowledge paradigm where formal mathematical models are replaced by patterns of connections forming and reforming over time and space.

One approach might be to combine the two types of security goals but as the granddaughter and grandmother example shows, this requires the modelling of contradictory goals. Another possibility is to articulate a complex scenario such as the grandmother and granddaughter case using a family of models where the data security and relational security models are separate and a third type of model is introduced which captures the negotiation and navigation between the two. This third type of model would be a model of everyday negotiation and serves to shine a light on the important practices undertaken by individuals to marry data security needs with their human security needs in order to achieve the most effective co-construction of positive and negative security in a given context. In the following sections below we introduce the notion of the everyday into positive and negative security and conclude with a short discussion of the potential for modelling such everyday security interactions.

7 Introducing the everyday

One of the touch points between the computer security models and the relational security models is the individual. The individual has to manage the computer security requirements inscribed into the computer security models with the relational security requirements inscribed in the relational security model. For example in our scenario the grandmother has to manage the banking requirement to use a username and password for her on-line banking account alongside her practice of sharing technology use with her granddaughter as part of the grandmother's approach to managing her fear of losing financial security. This social practice is based on her trust relationship with her granddaughter. This is a complicated negotiation between the two types of security models. It requires the grandmother to, amongst other things, judge the trustworthiness of the granddaughter, be aware of any potential changes in her granddaughter's behaviour and to understand the purpose of the username and password controls and agree a course of action with her granddaughter. This is an everyday security problem that requires negotiation between the granddaughter and grandmother.

In recent years there has been a move to develop a scholarship that explores, theorises and develops an understanding for security in the everyday. The everyday has become a category of security studies where the focus is “the ‘everyday’ as a category of analysis — with its alternative temporal stress on rhythm and repetition and scalar emphasis on the micro and proximate” [36]. For example, we can see in the grandmother and granddaughter example that there are information sharing routines between the granddaughter and grandmother that are both frequent, small and happen in close proximity blending on- and off-line information sharing.

This direction of study is driven by the perspective that the individual is the ultimate referent object in security studies [25, 33]. The focus of the social sciences in studying the everyday has largely been developed from a critical position. Critical theorists argue citizens have not been engaged with in order to understand their security needs and concerns [36]. In HCI and usable security studies, the focus has been on describing security practices found in the wild [14, 37] but with little fundamental discussion as to the security goals that these practices support. In this paper we use the critical theory perspective to augment our understanding of security practices in the wild wild by taking a closer look at the interaction between the traditional information security goals related to the protection of data and human security needs. This augmented understanding is needed if the grandmother's and granddaughter's security practices are to be understood. In the scenario we have sketched in this paper, both grandmother and granddaughter need guidance on their security responsibilities to each other and approaches for ensuring that the trust bonds between them are sufficiently strong as well as guidance to develop their technical know-how.

8 Security and the everyday

Human security needs are the primary referent object of everyday security as patterns of practice are, in part, routinised and repeated to develop an individual's ontological security, a form of security founded on basic trust within relationships [15]. Croft and Vaughan-Williams [10] citing Croft 2012 [9] describe ontological security as follows: "the key elements of an ontological security framework are a biographical continuity, a cocoon of trust relations, self-integrity and dread, all of which apply at the level of the individual, and all of which are constructed intersubjectively." In our example we can see that as family members the granddaughter and grandmother are embodiments of each other's biographical continuity, which help to foster strong and deep trust bonds. Each provides the other with trust relations that insulates or cocoons the other from unwelcome events using digital services. The self-integrity of both the grandmother's and granddaughter's identity is seemingly intact in the sense that both grandmother and granddaughter are willing to share different parts of their lives with each other, fostering a sense of security and safety in the other. Both granddaughter and grandmother routinise each other's lives and help to give structure which helps to manage the dread of insecurity (for example the dread of financial or social insecurity).

As we can see from the above examples, ontological security therefore manifests itself in the everyday practices that are designed to build and maintain routines that enable an individual to use trust relationships to cope with complex and uncertain situations. The main focus of ontological security practice is to routinise life to prevent it from tipping into chaos and to enable individuals to have the confidence to go about their daily activities. In a digitally-mediated society, an individual's everyday security is characterised by combining positive and negative security techniques in order to maintain an individual's sense of ontological security.

In our example of granddaughters and grandmothers the following aspects of everyday security need to be navigated. The scenario is everyday in the sense that it is composed of proximate, close, micro relationships between family members. These close relationships are founded on a repetition of micro interactions. It is also co-constituted by positive and negative security practices because the relationship between the granddaughter is in part strengthened by sharing access to essential on-line services and supporting each other in the use of those services. The close relationship between granddaughters and grandmothers make possible the sharing of access and the flow of personal information, equally the sharing of access and the flow of personal information serve to further strengthen those bonds meeting the human security need of being confident to engage with the on-line services and achieve financial security (on-line banking) and relationship security (mediated through social media).

9 Modeling the everyday

Everyday security can not be reduced to a simple model and to encompass the different views and the interactions between those views make models too complex to construct and interpret. An alternative approach is to introduce a family of security models, where computer security models and relational security models are linked by everyday security models that capture the interaction between positive and negative security techniques and which show the outcomes of the negotiation between human security and data security needs.

Models of everyday security need to capture the relationship between positive and negative security techniques. As our grandmother and granddaughter example shows, positive and negative aspects of security are concomitant of each other; the negative protection of username and password protects the grandmother and granddaughter as service users from attacks from outside the family and also give each the positive freedom to engage in services that help each to meet their human security needs of economic stability (on-line banking) and relational security (social media). Equally granting the other access to their on-line accounts, either through login credentials or by allowing the viewing of account activity, provides the positive security of further building trust bonds through sharing and also the negative security of an additional person to check the integrity of the on-line transactions. The negative security aspects of this example can be modelled using standard security modelling techniques such as BLP and RBAC. The relational aspects of this example can be modelled using social network analysis. However, neither of these modelling approaches capture the concomitant nature of positive and negative security and in particular the different ways in which the individual has to navigate and bring together these two forms of security to construct an everyday security strategy for a given situation.

Models of everyday security also need to capture the ontological security position. Traditional and relational security models also do not explicitly take into account the ontological security position of both grandmothers and granddaughters. Furthermore, current modelling techniques do not enable security goals to be understood from multiple perspectives. In order to understand the security goals of the granddaughter and grandmother scenario, the security positions of both the granddaughter and the grandmother has to be taken into account as well as the perspective of the digital service provider and as well as the perspectives of other family members.

Everyday security models also need to capture the issues arising from emotional, physical and social proximity. These issues include: the negotiation of proximity and the evaluation of what to share and what to keep private and an on-going assessment of the motivations of the other in maintaining the trust relationship.

In summary, a family of models that include the computer security and relational modelling approaches linked by models of everyday security is one possible approach to responding to the complexity of everyday security. By introducing a linked family of models, the security knowledge becomes less fragmented and,

importantly, is brought together without denying the different epistemologies in which each security knowledge is grounded. In this section we have sketched some of the requirements for models of everyday security. Such models make visible the positive security goals arising from fixed-space interaction which is traditionally invisible to the service security design. Whilst these interactions are outside of the realm of technological security mechanisms, they have an important bearing on the meaning and the significance of such mechanisms and can be used to shape technological security mechanism design.

10 Conclusion

Information security practitioners and scholars have long understood the importance of context when defining and responding to information security problems. It is also understood that in real world security multiple perspectives need to be worked with in order to understand both the problem and the most appropriate responses. However, as the grandmother and granddaughter scenario shows, information security is not solely about protection, it is also a story of enablement and achievement that result in the meeting of an individual's human security needs as well as data protection needs. A modelling approach that relates human security needs with data protection needs and shines a light on the negotiation process between the two, enables us to connect these two families of security need and identify how each can support the other. Such a modelling approach also contributes to the reunification of the field of security, something that is needed for an effective response to complex real-world everyday security problems.

Acknowledgements

Lizzie Coles-Kemp's contribution was funded by EPSRC grant: ESSfES: Everyday Safety-Security for Everyday Services (grant number EP/N02561X/1).

References

1. Adey, P.: Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space* 27(2), 274–295 (2009)
2. Anderson, J.P.: Computer security technology planning study. Tech. Rep. ESD-TR-73-51, Electronic Systems Division, Hanscom Airforce Base, Hanscom, MA, USA (Oct 1972)
3. Bell, D.E., LaPadula, L.J.: Secure computer systems: Mathematical foundations. Tech. Rep. ESD-TR-73-278, ESD/AFSC, Hanscom AFB, Bedford, Mass. (Nov 1973), also appears as MTR-2547, vol. 1, Mitre Corp., Bedford Mass. Digitally reconstructed in 1996.
4. Briggs, P., Jeske, D., Coventry, L.: Behavior change interventions for cybersecurity. *Behavior Change Research and Theory: Psychological and Technological Perspectives* p. 115 (2016)

5. Coles-Kemp, L., Ashenden, D.: Community-centric engagement: lessons learned from privacy awareness intervention design. In: Proceedings of BCS HCI 2012 Workshops: Designing Interactive Secure Systems. pp. 4:1–4:4 (9 2012)
6. Coles-Kemp, L., Kani-Zabihi, E.: Practice makes perfect: motivating confident privacy protection practices. In: Proceedings of the IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT 2011) and the IEEE Third International Conference on Social Computing (SocialCom 2011). pp. 866–871. IEEE (2011)
7. Coventry, L., Briggs, P., Jeske, D., van Moorsel, A.: Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In: International Conference of Design, User Experience, and Usability. pp. 229–239. Springer (2014)
8. Crampton, J.W.: Cartographic rationality and the politics of geosurveillance and security. *Cartography and Geographic Information Science* 30(2), 135–148 (2003)
9. Croft, S.: Constructing ontological insecurity: the securitization of Britain’s muslims. *Contemporary Security Policy* 33(2), 219–235 (2012)
10. Croft, S., Vaughan-Williams, N.: Fit for purpose? Fitting ontological security studies ‘into’ the discipline of International Relations: Towards a vernacular turn. *Cooperation and Conflict* 52(1), 12–30 (2017)
11. David, N., David, A., Hansen, R.R., Larsen, K.G., Legay, A., Olesen, M.C., Probst, C.W.: Modelling social-technical attacks with timed automata. In: Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST 2015). pp. 21–28. ACM (2015)
12. Denney, D.: *Risk and society*. Sage (2005)
13. Dodds, K.: Jason bourne: Gender, geopolitics, and contemporary representations of national security. *Journal of Popular Film & Television* 38(1), 21–33 (2010)
14. Dourish, P., Grinter, R.E., de la Flor, J.D., Joseph, M.: Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8(6), 391–401 (2004)
15. Giddens, A.: *Modernity and self-identity: Self and society in the late modern age*. Stanford University Press (1991)
16. Hansen, L., Nissenbaum, H.: Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4), 1155–1175 (2009)
17. Harrison, M.A., Ruzzo, W.L., Ullman, J.D.: Protection in operating systems. *Communications of the ACM* 19(8), 461–471 (Aug 1976)
18. Heath, C.H.P., Coles-Kemp, L., Hall, P.A., et al.: Logical Lego? co-constructed perspectives on service design. In: Proc. 10th Biannual Conf. Design and Development. pp. 416–425 (2014)
19. Inglesant, P., Sasse, M.A.: Information security as organizational power: A framework for re-thinking security policies. In: Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop on. pp. 9–16. IEEE (2011)
20. Jeske, D., Briggs, P., Coventry, L.: Exploring the relationship between impulsivity and decision-making on mobile devices. *Personal and Ubiquitous Computing* 20(4), 545–557 (2016)
21. Lampson, B.: Protection. In: Proc. 5th Princeton Conference on Information Sciences and Systems. Princeton (1971), reprinted in *ACM Operating Systems Rev.* 8, 1 (Jan. 1974), pp 18-24.
22. Lewis, M.M., Coles-Kemp, L., Siganto, J.: Picture this: Tools to help community storytelling. Presented at the CHI 2014 Workshop on Tactile User Experience Evaluation Methods (2014), available from <https://www.riscs.org.uk/?p=832>

23. Light, A., Coles-Kemp, L.: Granddaughter beware! an intergenerational case study of managing trust issues in the use of Facebook. In: Proceedings of the 6th International Conference on Trust and Trustworthy Computing (TRUST 2013). Lecture Notes in Computer Science, vol. 7904, pp. 196–204. Springer (2013)
24. McLean, J.: Security models. In: Marciniak, J. (ed.) Encyclopedia of Software Engineering. Wiley (1994)
25. McSweeney, B.: Security, Identity and Interests: A Sociology of International Relations. Cambridge Studies in International Relations, Cambridge University Press (1999)
26. Molotch, H.: Everyday security: Default to decency. *IEEE Security & Privacy* 11(6), 84–87 (2013)
27. Monk, A., Howard, S.: Methods & tools: the rich picture: a tool for reasoning about work context. *interactions* 5(2), 21–30 (1998)
28. Neocleous, M.: Critique of Security. Edinburgh University Press (2008)
29. O’Loughlin, B., Gillespie, M.: Dissenting citizenship? young people and political participation in the media-security nexus. *Parliamentary Affairs* 65(1), 115–137 (2012)
30. Pfleeger, S.L., Sasse, M.A., Furnham, A.: From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management* 11(4), 489–510 (2014)
31. Probst, C.W., Kammüller, F., Hansen, R.R.: Formal modelling and analysis of socio-technical systems. In: Semantics, Logics, and Calculi - Essays Dedicated to Hanne Riis Nielson and Flemming Nielson on the Occasion of Their 60th Birthdays. Lecture Notes in Computer Science, vol. 9560, pp. 54–73. Springer (2016)
32. Reddington, J., Coles-Kemp, L.: Trap hunting: Finding personal data management issues in next generation aac devices. In: Proceedings of the second workshop on speech and language processing for assistive technologies. pp. 32–42. Association for Computational Linguistics (2011)
33. Roe, P.: The ‘value’ of positive security. *Review of International Studies* 34(04), 777–794 (Oct 2008)
34. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. *Computer* 29(2), 38–47 (Feb 1996)
35. The TRESsPASS Project. Project web page, <http://trespass-project.eu>, last accessed on 10 February 2017
36. Vaughan-Williams, N., Stevens, D.: Vernacular theories of everyday (in)security: The disruptive potential of non-elite knowledge. *Security Dialogue* 47(1), 40–58 (2016)
37. Vines, J., Blythe, M., Dunphy, P., Vlachokyriakos, V., Teece, I., Monk, A., Olivier, P.: Cheque mates: participatory design of digital payments with eighty somethings. In: Proceedings of the Conference on Human Factors in Computing Systems (CHI 2012). pp. 1189–1198. ACM (2012)