Service Security and Privacy as a Socio-Technical Problem: Literature review, analysis methodology and challenge domains

Bella, G; Curzon, P; Lenzini, G

Journal of Computer Security 0 (0) 1
IOS Press

Service Security and Privacy as a Socio-Technical Problem

Literature Review, Analysis Methodology and Challenge Domains

Giampaolo Bella [a], Paul Curzon [b], Gabriele Lenzini [c]
[a] *Dipartimento di Matematica e Informatica, Università di Catania, Italy*
E-mail: giamp@dmi.unict.it
[b] *School of Electronic Engineering and Computer Science, Queen Mary University of London, UK*
Email: p.curzon@qmul.ac.uk
[c] *Interdisciplinary Centre for Security Reliability and Trust, University of Luxembourg*
Email: gabriele.lenzini@uni.lu

Abstract. The security and privacy of the data that users transmit, more or less deliberately, to modern services is an open problem. It is not solely limited to the actual Internet traversal, a sub-problem vastly tackled by consolidated research in security protocol design and analysis. By contrast, it entails much broader dimensions pertaining to how users approach technology and understand the risks for the data they enter. For example, users may express cautious or distracted personas depending on the service and the point in time; further, pre-established paths of practice may lead them to neglect the intrusive privacy policy offered by a service, or the outdated protections adopted by another.

The approach that sees the service security and privacy problem as a socio-technical one needs consolidation. With this motivation, the article makes a threefold contribution. It reviews the existing literature on service security and privacy, especially from the socio-technical standpoint. Further, it outlines a general research methodology aimed at layering the problem appropriately, at suggesting how to position existing findings, and ultimately at indicating where a transdisciplinary task force may fit in. The article concludes with the description of the three challenge domains of services whose security and privacy we deem open socio-technical problems, not only due to their inherent facets but also to their huge number of users.

Keywords: security ceremony, concertina, cloud, cybersecurity, modelling, analysis, verification, awareness

1. Introduction

The availability of web services is changing the way humans rely on data and computing resources in general. Cloud infrastructures have given additional momentum to the use of services; for example, a researcher claims: “I am a cloudy researcher: I do not need a hard drive any more: I keep my documents on Dropbox and spideroak, my code on assembla, sourceforge, google code, github, literature papers on zotero and cloudme, my bookmarks on xmarks, my mail on several imap servers” [74]. This calls for research in Computer Science to ensure security and privacy of service computing, namely that the technology works as intended by its designers. An additional hierarchy of threats comes from the users,

who may have a varying degree of familiarity with the technology, and fail or refuse to use it as intended by its designers.

A number of examples can be drawn from the real world. Even if password-based authentication works in purely technical terms, it will not work in practice if passwords are chosen following predictable patterns or are written on sticky notes affixed on monitors for passersby to see. Users may do fuzzy matching and accept a spoof web site, say `http://www.europe.eu`, as the real one, `http://www.europa.eu`. They may succumb to *click-whirr* responses [47], namely perform a routine series of steps absent-mindedly in an insecure setting, such as on a public hotspot, simply because they used to perform them every day on their secure institutional LAN.

This suggests that an extended view of a security protocol is needed to include human users, behaviours and social protocols: that is, see the system as a much more complex socio-technical system. This extension of a security protocol is termed a *security ceremony* [33]. It is widely accepted within security circles that "security is a chain, and people are the weakest link in the chain" [69]; by contrast, our long-term goal is to establish security and privacy *in* the presence of the human. We call for a socio-technical approach, which may ultimately require a transdisciplinary combined effort by computer scientists with social scientists, psychologists, etc. We argue that this is the main security and privacy challenge of the current decade.

In particular, this challenge also expands to High Performance Computing (HPC). With the USA's setting out to develop a one exaflop computer by 2025 [92], the researcher could envision a tremendous benefit to their computationally intensive security analysis. However, one risk becomes clear, the potential abuse of that enormous power by criminals aiming at breaking computationally-established security measures. If HPC really is to become available to every possible subscribing security researcher working remotely, then that potential abuse will also exploit socio-technical attack patterns.

The present article consolidates service security and privacy as a socio-technical problem. To achieve this aim, its contribution is threefold. It starts off by reviewing the relevant literature that looked at the problem either as a technical or, more extensively, as a socio-technical one. In particular, works by Blaze [21], Whitworth [99] and Ellison [33] are among the main contributions to broadening the traditional alice-and-bob setting of security protocols. Its second contribution is an analysis methodology for service security and privacy that leverages on a recent model by Bella and Coles-Kemp [13] and adapts it for web services. Termed the *ceremony concertina*, the model links technology to society through a number of *layers*, which represent the interposing stakeholders, ranging from computer processes to user personas. Correspondingly termed the *ceremony concertina traversal*, the analysis methodology partitions the problem of socio-technical security and privacy into smaller sub-problems. These are the analysis of each layer individually and then their analysis in combination.

The methodology also offers the researcher the freedom to concentrate either on specific layers at a time or on all layers at the same time. It purposely does not prescribe the use of specific research methods of analysis; rather, depending on the researcher's focus, the most appropriate combination of research methods are left as their choice, from formal methods, analytical methods and empirical ones. Analyses that combine formal methods with analytical or empirical ones will be termed *semi-formal* (§3.3). The ceremony concertina model offers anyone from a range of disciplines, who wants to investigate socio-technical aspects of security and privacy, a canvas on which to paint their findings. The ceremony concertina traversal methodology offers practical directions on where and how to paint on that canvas, namely obtain findings. It enables the researcher to take the guarantees of security and privacy that the technology establishes and to transmit them reliably and effectively to its users. For example, Bella et al. have recently adopted it to analyse the TLS certificate validation ceremony [17], Huynen et al. to identify

critical decision points in the ceremonies that users follow to access WiFi networks via Hotspots [35], and Ferreira et al. to outline a research framework [34].

The third contribution of this article is the definition of three domains of services that we deem particularly challenging socio-technical problems. These are File Hosting, the domain of services that offer remote storage, Collaborative Editing, grouping services for multi-author document preparation, and Electronic Exam, which sees services for computer-assisted assessment of candidates towards a qualification. These domains are selected because of their many facets as socio-technical problems, and also because they reach a huge number of users worldwide. Five services per domain are discussed, demonstrating that the niceties of technology may remain opaque to the users who engage with it; because the technology often handles sensitive user information, that information may be put at risk despite the correctness of the technology.

This article extends a previous conference paper [16] with a broader literature review (§2), a more detailed discussion of the analysis methodology (§3), and the introduction of the challenge domains (§4). The treatment terminates with some conclusions (§5).

2. Literature Review

Our literature review is partitioned into two main blocks. The first block (§2.1) pertains to the analysis of service security and privacy of services while a service is approached as an algorithm, hence as a purely technical problem. It means that the service is studied deterministically and its security and privacy properties established or refuted against a stated threat model. No elements of human activity are considered, hence models suffer a severe limitation. By contrast, the second block (§2.2) features the main existing works where some account for human activity is made. Out of this review, we see that a comprehensive methodology to tackle the security and privacy problem as a socio-technical one is still missing.

2.1. The Technical Perspective

An important starting point is offered by Gonzalez et al. [37], who show that most existing work addresses legal, compliance, and governance issues; only little work tackles the issues that are more of interest for Computer Scientists, such as those concerning the security in interfaces (API, administrative, and user interfaces), data security (confidentiality, redundancy, and data disposal), network security (security protocols in general) and virtualisation. This suggests that there is still room for analysing services from the security and privacy standpoint, which may not be surprising due to the relatively young age of this research area.

Somorovskly et al. analyse the security of control interfaces of Amazon, a well known representative of the public cloud, and of Eucalyptus, a widely used private cloud software [71]. This analysis is not carried out by means of formal methods but by empirical evidence that the targeted interfaces can be successfully attacked. By contrast, Jana and Shmatikov developed a tool called EVE [44] to verify whether a service exposed by an untrusted provider is flawed. Flaws here can be due to bugs or to misconfigurations lying anywhere through the components supplied by the provider. Arapinis et al. [7] use formal methods for the security and privacy analysis of a service. More precisely, this work leverages on the process algebra Applied π-calculus [3] and the computer tool ProVerif [20] to model and verify forms of the anonymity property over known conference management services such as EasyChair, EDAS, and ConfiChair.

This Section is kept brief due to the focus of this article on socio-technical aspects. The work by Gonzalez et al. [37] also overviews the current status of security issues and solutions. It then reviews more than two hundred references from different research segments of academia (IEEE, ACM, Springer, Webscience and Scipress), organisations (CSA [5], NIST [46,58,51], ENISA [27], Gartner Group, KVM.org, OpenGrid, OpenStack, and OpenNebula), and companies (ERICSSON, IBM, XEROX, Cisco, VMWare, CITRIX, EMC, Microsoft, and Safeforce). Therefore, this work can be easily appealed to for further reading in the area.

2.2. The Socio-Technical Perspective

Since Kevin Mitnick, a renowned and reformed hacker, explained in a book how an attacker can succefully deceive people to get access to their systems [59], the security and privacy problem has gained a new dimension. Creese et al. elaborate that dimension through seminal work [32] that reviews properties of authentication and confidentiality in a broader, human-scale, perspective. The properties become of trust rather than of security. Without the support of a PKI infrastructure, the strength of authentication depends on an entity's trusting a name; even with a PKI, trust is needed over Certification Authorities to abide by the rules. Such trust cannot be ensured by purely technical means because people may be deceived. In this vein, Ferreira et al. highlight the pitfalls and subtleties of trusting a name [35]. Also confidentiality becomes a matter of trust when interpreted on a human scale; even messaging a peer over an encrypted channel requires the sender to trust the peer to keep the messages or the encrypting keys from third parties. Bella terms this the *minimal trust* [11]. More recent attention to the human nodes comes from an authoritative NIST report [45], where Janser surveys technical security and privacy issues in service computing, stressing that the protection of the client side is often overlooked, but becomes more critical in service computing. The intensive use of browsers, of social media, and of other public services or platforms, will make the consequences of social engineering attacks more critical.

Security experts can no longer ignore the humans in the security chain given the evidence that, in attacking information systems, *social engineering* may be more effective than hacking the system's technical defences [59]. Sometimes technical flaws may provide the basis for launching a social engineering attack. For example, in context-aware phishing [43], the hacker uses a flaw in the victim's browser to obtain personal information about the victim's bidding history or shopping preferences. This stolen information lets the attacker customise its scam messages to gain the victim's trust.

Studying service security and privacy as a socio-technical problem is more than understanding how social engineering practically works. It also concerns unveiling and describing the subtle interactions between users and systems, which is a topic related to the *usability* of systems. Bella and Coles-Kemp inspect the usability of the Amazon registration/login ceremony [12], and Jaferian at al. draw a number of heuristics to evaluate tools for IT security management [42]. A socio-technical problem also demands understanding the *psychology* of users when interacting with digital resources: for example, in the perception that users have of their own system, security might be completely non-aligned with respect to the factual security that the system is able to guarantee. A misunderstanding of these subsidiary aspects will lead to a system being insecure overall. Such aspects can be assessed at least empirically. Barrera et al. assess the permission-based security model of Android [9], while Zhang et al. assess the security of password expiration and its replacement with a new one [101].

Many socio-technical attacks are possible because security mechanisms are not designed *for* the users. This may sound paradoxical but has roots in the usual practice of reproaching users who commit security naiveties after ignoring security advice. This practice is being proved wrong: many users consider

current security mechanisms unhelpful, if not completely annoying [39], to their daily work. This is the ultimate reason why people often strive to bypass even the strongest security mechanism, sometimes in surprisingly ingenious ways [41,30]: the suggested "secure" behaviour is not sustainable from the usability-centred and psychology-centred point of view of users. Therefore, far from being irrational, users commonly follow a rational economic strategy, which the traditional technically-oriented approach to security often ignores. The claim that humans are always the weakest link in the security chain also requires understanding what makes the system (humans included) insecure. Applying this knowledge to secure system design can be effective [2,64].

The socio-technical aspects of information security captured the interest of Computer Scientists only recently. Very little has been done to study, mathematically and systematically, the nature of the socio-technical deficiencies of on-line systems and protocols, of socio-technical attacks, and of the possible defenses. Only a few approaches are there to develop a formal background for the analysis of human factors [22,62,68], with fewer still applying this to security [67]. Few approaches include humans in the design of systems to improve their security [64]. Socio-technical security relates also to the understanding of the psychology of security [25,28] and of deception [40,49,70]. Stajano and Wilson contribute a useful study about how people fall victim to scams and frauds [72]. They observe that the victims' behaviour follows precise patterns, and identify a list of seven principles, each expressing a mechanism exploited by the hustlers in performing their deceptions. The study of human behavioural patterns makes it possible to understand the failure modes of the user "component" [6,98]. We share this viewpoint.

Socio-technical security is also about understanding and formalising the interactions between people and systems. People quite naturally execute high-level security protocols, for example, when conducting a commercial transaction. Blaze calls them "human-scale security protocols" [21]; he advocates that these protocols form the basis of trust in the complex systems used for society's basic functions. A precise framework for describing "human-scale protocols" is needed to understand how human reactions are involved in security critical functions. This practice is common in experimental psychology [29], but lacks the formal semantics needed for a rigorous security analysis.

Gunter et al. use process algebras (in particular CSP) to model and analyse the dependability (liveness and safety properties) of automated identification and data capture work-flow in a hospital [38]. Masci et al. analyse workflows in medical scenarios [55,56] from a distributed cognition perspective. While this workflow research does not focus on properties against an attacker, it demonstrates the use of formal methods over systems whose users interact with objects, interfaces and other people. Masci et al. also show how a device can be verified to be *predictable*, namely to have the property of enabling users to discern the state of the device simply from its current output [57].

Conducting security analysis motivates Ellison in defining *security ceremonies* [33]. According to him, the term "ceremony" was first coined by Jesse Walker to indicate those communications between human nodes and other nodes that happen usually not via network connections, but instead through user interfaces, face-to-face interactions, peripheral devices, or transfers of physical objects that carry data (for example USB memory sticks). Examples of ceremonies include password authentication and registration procedures, or the protocol that users follow interacting with an ATM machine. Thinking of protocols as ceremonies brings new insights on how security does or does not work, and reveals flaws that a sheer reductionist approach to technical security is not able to capture. This is clearly shown in recent work of Radke et al. [65]. The authors identify a flaw in the Opera Mini browser ceremonies emerging from the HTTPS protocol when used in a certain context, despite the fact that the protocol is secure in the traditional sense (§3.4). Their result shows that the practice of security protocol analysis must be bound to the ceremonial context in which a protocol runs: "even when considering the same protocol, a different

context is a different ceremony". Similarly, Radke et al. comment on the security of a ceremony that involves the TLS protocol [36]. Karlof et al. propose design principles for obtaining conditioned-safe ceremonies [47]. A conditioned-safe ceremony is one that conditions users to take safe decisions even in the presence of social engineering attacks. They evaluate their principles by conducting a study over some two hundred participants. These are observed while using different email registration/authentication ceremonies that are occasionally violated by an attacker.

Also the threat model bears non-technical dimensions. Kumar et al. introduce the *rushing user*, who tends to skip anything, such as a phishing warning, not directly connected to their main goal [48]. Although this work unfolds in the specific context of device pairing ceremonies, its principles appear to be general, hence applicable to a variety of ceremonies such as the one for user consumption of a web service. Creese at al. [31] advocate that the all-powerful Dolev-Yao model is not realistic, and prove it too powerful by analysing protocols in a *pervasive environment*, here addressed as a *socio-technical* protocol. Carlos et al. develop this argument [24] substantially. They derive more realistic threat models by removing capabilities from the Dolev-Yao intruder, and apply their models to authentication protocols with Wi-Fi printers and to Bluetooth pairing protocols. This work continues in a paper by Martimiano et al. [53], and then gets expanded through Carlos's Ph.D. thesis [23], for example with the notion of human-to-human or human-to-machine *channels*. Each such channel can be interpreted over the ceremony concertina model of Bella and Coles-Kemp [13] by compressing specific layers of the concertina, as we shall see (§3.3); for example, a human-to-human one compresses the technical layers, and other channels may demand only certain other layers of the concertina. Also each channel used by an attacker (for example, the visual, auditive or environmental ones) can be layered through a concertina.

The international work towards threat models for socio-technical analysis has only just begun [34,54]. For example, it is as yet unclear how society shapes up users with a generally negative (that is, reluctant, impatient, etc.) attitude towards security; it is equally not yet fully understood what makes a user express an attacking persona, one who deliberately attempts to subvert the security elements of the technology; and blocking an audiovisual cue, although it may seem impossible [54], could be achieved by elementary social engineering practices of distraction. However, it must be remarked that the present article does not aim at directly contributing to the debate on the most appropriate threat models. By contrast, it adopts and generalises the ceremony concertina model for socio-technical protocols to make the more fundamental contribution of an analysis methodology for the security and privacy of such protocols; the methodology systematically considers the range of layers between society and the Internet, and can precisely position any of the threat models mentioned above through that range. For example, the rushing user can be viewed as a specific persona of a user's, who may express a very different persona through another ceremony at a different point in time.

3. Analysis Methodology

The literature review presented above shows that previous efforts have been exploring various dimensions of security and privacy, also as a socio-technical problem, but no structured methodology appears to have been followed. In consequence, it becomes difficult to evaluate how contributions relate to or complement each other. For example, it is not straightforward to relate Blaze's human-scale protocols to Ellison's ceremonies. However, we suggest that understanding this and similar relations is needed to solve the socio-technical problem termed security and privacy. It is towards that understanding what the analysis methodology presented in this Section can add value.

Our methodology stems from an original approach (§3.1), based upon a recent model (§3.2), to the security and privacy analysis of services. In targeting both social and technical aspects, the methodology is socio-technical, as its steps indicate (§3.3). Example uses of the methodology follow (§3.4).

3.1. Approach

Our methodology insists on a *multi-layer though integrated* approach to the analysis of the security and privacy of services. To the best of our knowledge, this is innovative and, we shall see, promising. It is the multi-layer approach what makes the analysis socio-technical. The analysis is targeted at complex socio-technical properties centred on the human [17], rather than merely technical ones such as key confidentiality in the traditional sense of security protocol analysis [10]. The findings at the various layers are combined to provide assurances or pinpoint weaknesses to the actual human users of the services. This approach therefore aims to make the outcome of the analysis valuable for users, as opposed to the outcome of traditional technical analysis, where humans are not accounted for.

It is worth remarking that our methodology is not specifically concerned with software verification; it is designed to support the upcoming formal analysis of abstract specifications of protocols with their surrounding use contexts, rather than of actual programming code.

3.2. Model

As mentioned above, a security ceremony expands a security protocol with the out-of-band, notably with the user [33]. Our research leverages upon the recent model of security ceremonies of Bella and Coles-Kemp [13], in Figure 1.

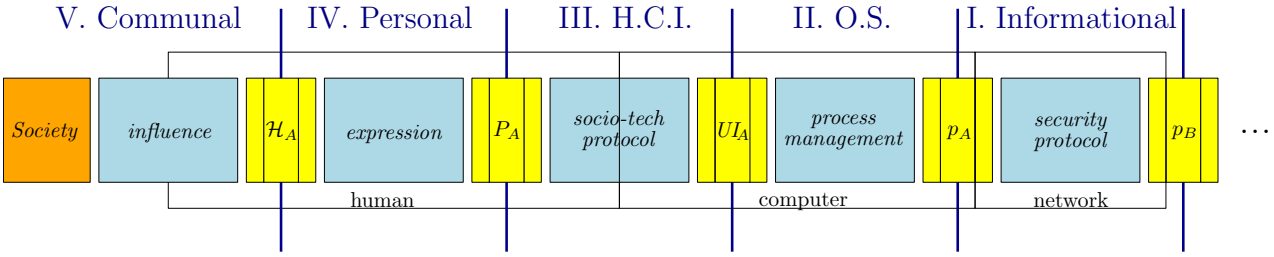

Fig. 1. The model of the full security ceremony [13] underlying our analysis methodology

The model identifies several layers, which go beyond the original ceremonies between users and systems as described by Ellison [33]. This ceremony model is capable of capturing additional elements of the interaction between users and technology. This aim is also supported by Whitworth [99], who argues for the importance of the interfaces between humans and machines, but also acknowledges the outermost layer whereby society influences behaviour by means such as word of mouth, media publicity and the users' engagement with technology [100]. Therefore, our methodology is oriented to see the workbench for a socio-technical security analysis as a finer-grained picture, termed the *full security ceremony*.

The layers in Figure 1 feature various abstractions of two example users Alice and Bob, additionally expanded with *Society*. Such abstractions are termed *players*. From left to right, the small, yellow boxes indicate the players. They are, respectively, the computer process p_B running a security protocol with Alice on Bob's behalf and the computer process p_A running the security protocol with Bob on Alice's

behalf. Then comes the user interface UI_A for her, a generic persona P_A of hers, and finally Alice as a human, that is, herself $\mathcal{H}_A$.

The layers can be understood as follows.

- Layer I, Informational, concerns the security protocol running between computer processes in order to secure Alice and Bob's communications over a potentially insecure network.
- Layer II, Operating System, manages the inter-process communication between the process that executes the security protocol on behalf of a user and the process that runs the interface presented to that user.
- Layer III, Human-Computer Interaction, indicates the socio-technical protocol whereby a user interacts with a user interface, such as by filling in forms in a graphical interface. This is clearly a technical protocol because of the interaction with the technology, but is deeply intertwined with the social protocols [66] regulating the individuals' expressions of social capabilities such as trust, recommendations and advice. The user is not involved directly but instead through one of their personas expressed through the next outermost layer.
- Layer IV, Personal, pertains to the user expression of a persona in order to engage with specific technology. Persona is used to refer to a particular, abstracted view of a class of common user behaviour. A user may express various personas. For example, when accessing on-line bank services to pay for bills, users may well express different personas to when accessing their Facebook accounts to catch up with friends. They may be less willing to download new applications when in the middle of bank transactions, for example, than when attempting to share content with friends.
- Layer V, Communal, reflects the reciprocal influence of society, including other players, over individuals engaging in a security ceremony. The influence can be in the full range from positive to negative, and about a variety of stimuli, such as (dis)trust, (in)caution, (dis)satisfaction, etc. For example, a national campaign could influence users towards being more careful in opening attachments from unknown sources or, vice versa, more trustful towards certain services. Someone working in a team might be influenced by the norms of that team.

Adjacent layers share a player, who plays in both. Each layer features what is termed an *interaction* between a pair of players, such as the socio-technical protocol or the security protocol. The players of a layer only interact within that layer. Interacting players do not belong to the same user in the case of layer I.

Our research demonstrates that the full security ceremony model can be modified to reflect human interaction with web services. We build this modified model by means of two changes: one is to replace the network with an infrastructure in general as the means of communications, which could then be instantiated with the Internet or the cloud depending on the application scenario; the other is to collapse one of the two sides, say B's, as a service. Although general pictures are omitted here, the example uses of the methodology (§3.4) will feature some example pictures.

Figure 1 shows that each player has some internal separations by means of vertical lines, but the original paper about the model [13] omitted an explanation. This is worthy of clarification, and therefore introduce some suitable terminology. Each player has a *core*, indicated by the inner rectangle featuring the player name, and two *front-ends*, depicted by the outer rectangles surrounding the core. While the core stands for the internal logics or calculations of the player, each front-end represents (part of) the input/output interface to and from the core. Each player has two front-ends for convenience, separating the input/output with specific players lying on its left or right side in the model. Due to the heterogeneity that the model incorporates, layers I and II are the only ones such that both front-ends of the layer carry

digital information: the facing front-ends of players p_A and p_B in layer I carry the messages of the security protocol; the facing front-ends of players UI_A and p_A in layer II carry the data of the inter-process communication, realising the process management.

The front-ends of layer III are of mixed nature. One carries the digital information that that user interface process UI_A shows or receives; the other one carries the cues and senses of security and privacy of the persona P_A. This layer therefore is particularly heterogeneous, inviting effort from transdisciplinary research teams composed of Technologists as well as of researchers from the Humanities.

The front-ends of the remaining two layers carry non-digital information, respectively supporting the human being $\mathcal{H}_A$'s expression of the persona P_A, and the societal influence on $\mathcal{H}_A$. Although these layers are the traditional research fields for the Humanities, layer IV at least seems worthy of transdisciplinary investigation, for example to unveil the mechanisms that regulate the human expression of a specific persona in front of a given technology.

3.3. Steps

Our methodology is termed the *ceremony concertina traversal* methodology, as it proceeds from the interpretation of the layers in the full security ceremony as a concertina. The full security ceremony can be compressed or expanded conveniently, depending on the researcher's target: the ceremony layers of interest. Compressing means that the players of a layer can be collapsed as a single player by folding the interposing layer as a concertina can be folded. For example, let us consider a verbal communication between Alice and Bob by means of Skype. It means that the model of Figure 1 should continue to the right hand side with the layers II, III, IV and V for Bob. If we assume that the analysis has no interest in the societal influence over both players, then layers V at both users can be folded, leaving players $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$ visible. Further, if we assume no interest in how Alice and Bob express their respective personas, then also both layers IV can be folded. If we also assume no interest in how Skype instructs the user interface, then also layers II can be folded at both ends. The resulting model would only have $\mathcal{H}_\mathcal{A}$ interacting with UI_A through Alice's layer III, which would be interacting with Bob's UI_B through layer I, which in turn would be interacting with $\mathcal{H}_\mathcal{B}$ through Bob's layer III. If there is no interest in how Skype works over the network, then the concertina can be squeezed in further, folding layer I. This would produce a model where Alice and Bob talk via an interface, which could be interpreted either as digital or as aerial. Every time a layer is folded, it is assumed to enjoy its stated properties; the player remaining visible after the folding exposes such properties through its new interactions (those that were adjacent to the one that was folded).

We are not aware of existing analysis methodologies aimed at bringing technical guarantees on security and privacy of services up to the level of humans in a systematic way, and this may be due to the relative scarcity of the transdisciplinary research effort pointed out above.

Our ceremony concertina traversal methodology consists of two steps.

1 **Traverse the target ceremony layers in isolation by means of semi-formal analysis.** To *traverse a layer* means to analyse an interaction between a pair of players, and may also require analysing each player. The methodology does not compel the researcher to traverse all layers of the full security ceremony together in one go. By contrast, the methodology allows layers to be concertinaed together, retaining the full ceremony in outline but abstracting away from the details of the particular layers. For example, if one does not need or want to analyse how society shapes the human engagement with technology and how this engagement gets reflected back over society, then they will not traverse layer V. In consequence, layer V could be collapsed. Depending on the

researcher's expertise and interest, a variety of example traversals can be envisaged, such as of layers I or III while collapsing the others, or of part of layer IV — of course, an analysis that is confined within layers I and II would be purely technical. Then, depending on the layer to traverse, the researcher will select the most appropriate research methods and corresponding tools, such as analytical and empirical ones for layer IV, and formal ones for layer II.

2 **Traverse the target ceremony layers in combination by means of semi-formal analysis, aiming at building the target traversal, that is one between the society surrounding a human and a remote computer process.** Part of the combination is achieved by analysing the layers in synergy, that is by using the insights deriving from the analysis of a layer to orient the analysis of adjacent layers. This makes it possible to address stringent though yet unanswered questions as to whether there exist realistic (in the sense of widespread in our world) personas to comply with given secure technology or, dually, whether secure technology can be designed to comply with given realistic personas. Another form of combination is the analysis of adjacent layers in sequence, in such a way that the findings from a layer can be ported over the other layer and vice versa. For example, over layers I and II, this will make the security and privacy properties of a service available at the local user interface. A third aspect of the combination stems from the attempt to reuse over a layer the formal techniques typically adopted over other layers, expecting fresh insights. For example, security protocols and socio-technical ones have many similarities though they concern different layers, hence the reuse of typical interaction design techniques over security protocol analysis and vice versa appears promising.

A strength of this analysis methodology is that the target traversal between society and technology could be built by composing shorter traversals, such as layer traversals, each time with potential for novel insights. For example, traversing from right to left involves starting with a security protocol analysis. Once the security protocol properties are established, they can drive the user interface analysis and the socio-technical protocol analysis to ultimately assess whether the technical properties can be successfully transmitted to realistic personas as human-perceivable senses of security. If the security protocol were SSL, then the researcher should be able to define a real-world persona to whom the user interface and then the socio-technical protocol together manage to transmit senses of authentication and confidentiality, perhaps also through convincing cues that the recent Heartbleed bug [84] is resolved. This persona could then be assessed for its plausibility by empirical methods, to establish how likely that persona is to exist.

The target ceremony traversal could also be built from left to right. A Social Scientist might want to start with layer V or IV or, possibly with the collaboration of a Computer Scientist, with the analysis of the socio-technical protocol of layer III to assess the senses of security it delivers to what persona. This direction ultimately guides the security protocol analysis towards properties that can support those senses of security. Potential modifications to the security protocol arising from this direction would be in the desirable spirit of human-compliant technology. A known example comes from cash machines: people using cash machines tended to walk away with their cash forgetting their debit card (this is an example of a general phenomenon known as a post-completion error). This issue was overcome by adjusting the technology to dispense cash only after returning the card. Curzon's user model based analysis is one way to detect post-completion and similar issues [62].

3.4. Example Uses

A variety of uses could be made of our methodology depending on which layers are folded as explained above (§3.3) and which remain in the focus of the current analysis. Each use could provide

valuable findings on its own, but these findings could further be interfaced together. In this vein, this Section outlines three notable example uses of our ceremony concertina traversal methodology that the researcher could realistically make. These respectively focus on layers I and III, then on aspects of layers IV, and finally on parts of layer II. As observed above, each layer demands specific expertise, with the lower layers more naturally targeted by Computer Scientists, the higher layers by Social Scientists, and layer III inherently demanding their transdisciplinary work.

Example Use 1. The formal analysis of the two-layered security ceremony consisting of layers I and III for services. This ceremony is depicted in Figure 2, which is derived from Figure 1 by collapsing certain layers and instantiating it over the infrastructure as discussed above (§3.2). Precisely, because layer II is collapsed, the user interface for Alice and the process executing the security protocol for her coincide, here indicated as UI_A; because Alice is interacting with a web service, the latter is monolithically indicated as p_B. The focus of the analysis is shaded, emphasising its three parts: layer I (dashed border), layer II (dot-dashed border) and, specifically, the user interface player (dotted border). Each of these offers research challenges in their own right, as well as challenges arising from their combination: the analyses of security protocols, of socio-technical protocols, of user interfaces and the interaction design all these embody. Therefore, the two steps of our methodology can be taken rather naturally here, offering respectively isolated and combined analyses of the layers.

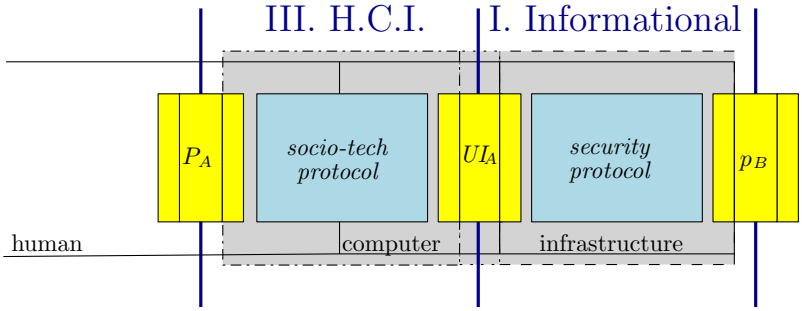

Fig. 2. The two-layered security ceremony instantiated over the infrastructure: the focus of example use 1 of our ceremony concertina traversal methodology is shaded

For what concerns the isolated analysis, assessing the security protocols in support of services involves dealing with tricky properties such as the various versions of privacy. For example, users may not entirely trust the service provider and may thus require unlinkability with their identity of some of the data that they transmit. Then, analysing human-computer interaction with the service, namely socio-technical protocols, entails the range of issues related to human beliefs and misconceptions about services outlined above (§2). Finally, designing good user interfaces with services is far from trivial, not least in the need to balance usability and customisability. For example, it may not be immediately visible to users that a popular application for File Hosting such as Dropbox allows the user to decide which shared folder to synchronise with their local device, and which ones to leave only with the service. An example of an isolated analysis of layer III of a security ceremony is already published [13].

The combined analysis of the system consisting of all shaded areas in Figure 2 sees UI_A playing as a user interface on one side and at the same time as a process executing a security protocol on the other side — because layer II is collapsed. The analyst is left with the challenge of mapping security protocol properties onto a persona's senses of security and privacy. An example of such a combined analysis

tackles layer III as done in a published isolated analysis [13], but now together with any security protocol, say SSL. Confidentiality of a session key, say the Master Secret of SSL, could be mapped to a sense of confidence if certificate validation succeeds without user intervention, or to a stance of caution and puzzlement otherwise.

Example Use 2. The experimental analysis of part of layer IV of the security ceremony for services. The target layer for this example use of our methodology, as depicted in Figure 3, is layer IV. Here, the focus is on how a human being, subject to a huge spectrum of stimuli coming from society, expresses a specific persona; this is therefore an instance of step 1 of the methodology. It becomes an instance of step 2 by studying the expression of the persona while the human is facing a certain technology at some point in time. Here, the interaction "expression" is conventionally drawn smaller than in Figure 1 to indicate that only a *part of* the interaction, as defined below, is targeted in this specific example use of the methodology.

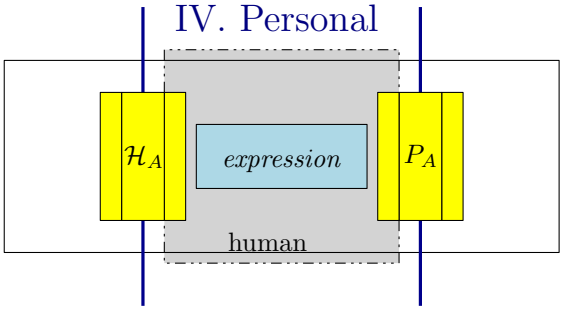

Fig. 3. Part of layer IV of the security ceremony: the focus of example use 2 of our ceremony concertina traversal methodology is shaded

Here, the part of the interaction that is tackled concerns the characterisation of the personas that a human can express for what concerns security and privacy when using a service. The analytical and empirical analysis of this part also reveals whether the specific personas utilised in layer III in the previous example are realistic, that is whether they are statistically significant. Such analysis consists of conducting experiments to monitor how users generally behave when facing specific tasks on services, or guided surveys to denote how they would abstractly design the interface with the technology if they could [50]. Of course, these experiments require the availability of reasonably large sample populations to submit questionnaires to, but this can be made simple by appealing to crowdsourcing services such as Amazon Mechanical Turk [73]. This example use of our methodology contributes to grounding other findings to the real world.

Example Use 3, the formal analysis of part of layer II of the security ceremony for services. This example use tackles layer II. Hence, the security ceremony featuring layer II only, where all other layers have been collapsed, is visualised in Figure 4. Similarly to the previous example, the interaction "process management" is drawn smaller than in Figure 1 to indicate that only a part is analysed.

Because Operating System analysis already is a large and well-established research area (with some 32 million Google entries at the time of this writing), a variety of research methods can be appealed to. In particular, the part of the interaction that this example use tackles concerns the specific inter-process communication between the process p_A running the security protocol and the user interface process UI_A aimed at signaling to the user the security properties established by the protocol. For example, at some

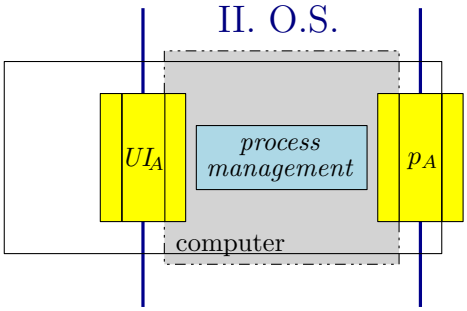

Fig. 4. Part of layer II of the security ceremony: the focus of example use 3 of our ceremony concertina traversal methodology is shaded

point the protocol process should send the interface process data signifying that end-to-end security was established, and this data obviously is sensitive. The interface process could then display an appropriate visual signal — often a padlock or a green address bar. Also the data that the user enters in the interface may be sensitive.

This interaction is very much worth the analysis effort for various reasons. One is that there exist no standards as to how an interface should treat security guarantees coming from the security protocol, and how they should be conveyed to users. The issue is with the very data that the protocol process should send to the interface process, which are to be interpreted with specific visual or acoustic signals aimed at transmitting the appropriate sense of security corresponding to the data. Such a piece of data in practice is not specific, hence far from being standardised. In consequence, how the interface is to be notified, for example, that the security protocol authenticated the remote peer remains a protocol-dependent choice. Moreover, also the cues that the user interface should use have not been codified, let alone standardised. Notably, a recent release of the Opera Mini browser, with its 300 million worldwide users in February 2013 [88], was found to display a padlock when an intermediate server interposes between the client and the server, hence without end-to-end security [65].

Another reason is that various interfaces could be used to access services while favouring the user's feeling of locality, that the application is running locally rather than remotely. This aim has inspired various forms of desktop integration for services, such as dedicated icons or integration with pre-existing programs with which the user is likely to be already familiar. A representative example of the latter is the seamless integration of applications, such as the version control system Tortoise [93] and the File Hosting application Dropbox [80], with the standard program to explore the local file system.

A third reason is the variety of security properties that are relevant for services today. It can be seen that one of the many security and privacy properties specifically formulated for services by the NIST is *data ownership*. It means that the "organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust" [46]. It implies that the service provider "acquires no rights or licenses through the agreement to use the data for its own purposes" [46]. Hence, the range of corresponding senses of security that the interface should transmit to users becomes proportionally large.

This example use of our ceremony concertina traversal methodology has ambitious aims. Inter-process communication does not seem to have been analysed so far at the level of abstraction advocated here. It is expected that this layer can be ultimately specified in terms of exchanges between two parties, and that the methods used to analyse layer I could be tailored to the new layer. Ambition does not derive only from sheer complexity, but also from the expected resistance that could be encountered in suggesting conventional associations, that is, standards: between security properties and process data

for inter-process communication, and consequently between process data and visual or acoustic signals. With standards in place, the future analyses would gain more clear-cut objectives.

3.5. Position within the literature

Our methodology has advocated service analysis to be carried out in a more structured way than existing work. We have seen that the methodology insists on a more detailed and, we argue, more appropriate model of the system than what has been used so far. The multi-layer model [13] that it adopts and adapts for service computing features more layers than those advocated by Ellison [33], where only two layers were envisaged, one between computer pairs and one between each human and a computer. The same two layers underly the work of Blaze [21]. The model is also more expressive than Whitworth's [99], to which it acknowledges inspiration. In consequence, the analysis methodology built on it can be made more precise than the routes taken by previous analyses.

It is clear that existing work that only takes a technical perspective of analysis (§2.1) can be positioned either at layer I or at layer II. It would seem that all work outlined above under the socio-technical perspective (§2.2) treat the human as a monolithic entity, overlooking their attitude at following different paths of practice depending on context — context is understood here to include also the features of the very service the human approaches and the specific point in time when this takes place. In brief, the human expression of different personas in front of technology is neglected, although humans express various personas also on Twitter for example, simply because "Our identities are prismatic. We're not the same person to everyone." [89].

It means that existing socio-technical works collapse layers III and IV together. This practice proved effective by yielding useful findings, and in fact it is in line with our methodology, whose step 1 allows for the researcher's focus layers to be analysed in isolation while collapsing the others. However, this practice ignored step 2 of the methodology, thus raising concern of having produced only incomplete analyses. It turns out that step 2, which prescribes a combined analysis of the layers, cannot be taken without expanding layers III and IV. In practice, personas may feedback one another through the human being, and this is precisely what layer IV represents. It is worth stressing once more that this layer is worthy of transdisciplinary research effort, especially when analysed in combination with layer III.

Socio-technical systems have been tackled from the standpoint of requirement engineering too [4,63]. *Actors* and *roles* are represented in a diagrammatic, graph-like form with their goals and security needs. Our standpoint is different. Rather than using an informal graphical language with the aim of requirement elicitation, our methodology advocates a formal, or semi-formal as defined above (§1), analysis of the complex system involving society and technology. Arguably, an actor could be interpreted as the human and a role as the persona who interact in our layer IV. However, the interaction termed "expression" (§3.2) goes beyond the one-to-many relation between actors and roles. Our methodology in fact prescribes that interaction to be analysed, in isolation and in combination with other layers (§3.3), in terms of its properties and preconditions.

Also, it must be observed that Computer Scientists traditionally assume the most careless persona, hence aim at a technology that *compels* every possible user to a secure interaction. By contrast, Social Scientists typically find that assumption too restrictive, especially for ensuring that the user *engages* with the technology and is satisfied; hence they recommend consideration of a variety of personas. By the analysis of layer IV, our methodology supports the latter standpoint, therefore allowing the analysis to capture the security and privacy expectations of the various personas of the user's.

In summary, it appears that existing works have only considered a specific persona of the user's rather than the actual user, and how the user approaches technology. It might be conjectured that this limitation

of existing research is due to the purely technocratic, rather than transdisciplinary, composition of the research teams. We are fully aware that overcoming this limitation is challenging, especially for certain domains of services. Three such domains are discussed in the following Section.

Finally, a limitation of our methodology is that analysing layers I and II of proprietary services is impossible because the specifications are not available. However, these layers could be assumed to function correctly and collapsed as we shall see below, hence other layers could still be analysed.

3.6. Tools

We have seen that our methodology leaves the researcher the freedom to choose their research methods and tools, and tailor them to the specifics of the target layers — prescription would be too limiting. Still, some indications have been given so far, and are summarised here depending on the type of analysis, whether it is formal, analytical or empirical. This summary should be read recalling the related work (§2)

Formal analysis prescribes a specification of the target system and its expected properties using a formal language, following by verification of the properties. Formal analysis is routinely applied to layers I and II, but also stretched out over layer III through the known methods of *theorem proving* or *model checking*. In particular, existing works [13,56,57] rely on tools such as Isabelle [60], PVS [61] and SAL [19], but we anticipate that other popular tools such as ProVerif [20] and the AVANTSSAR platform [8] could be extended to cope with socio-technical protocols. In general, it can be expected that whenever the interaction in a layer can be specified as a distributed protocol, then traditional tools for security protocol analysis could help out — hence, potentially also over layers IV and V, although this is yet to be explored.

Analytical analysis prescribes the evaluation of the target system using expert analysis. A team of experts evaluates a preliminary design of the system — prior to its use — using the known methods of *cognitive walkthrough* or *heuristic evaluation* [12,42]. The typical computer tool in support of these methods is a traditional office suite, namely spreadsheets and charts, with only minor attempts at ad-hoc tools [1,26]. The natural application for these methods and tools is layer III. For example, a cognitive walkthrough implicitly represents a number of personas through the sequence of steps they choose to interact with the technology. We believe that formal and analytical methods could be combined profitably: one could reason about the niceties of walkthroughs by means of formal methods.

Empirical analysis prescribes the evaluation of the target system by means of user participation. A prototype of the system is made available for users to practically use, and evaluated through the known methods of *laboratory studies* or *field studies*. Existing works [9,101] often combine both methods, relying on the traditional tools of engaging users through experiments, watching them and noting the outcomes. The computer tools adopted may combine a traditional office suite with tools for statistical evaluation. Empirical analysis can be used profitably over layers III, IV and V. In particular, it could be combined with formal analysis over layer III to define the relevant personas.

4. Challenge Domains

This Section identifies three domains whose socio-technical analyses of security and privacy we recognise to pose open critical challenges to researchers. Our ceremony concertina traversal methodology, which has already produced valuable findings [17,35], shall be used to fully address these challenges.

Each domain is a set of similar services. The three domains, which reach a huge number of users worldwide, are File Hosting, Collaborative Editing, and Electronic Exam.

- **File Hosting** is the service of providing space to host user files. It serves many purposes, such as personal storage and backup. It is changing the attitude of users towards managing files. Rather than being carried around in laptops or portable hard discs, files can be found as a service through any access platform, including smartphones. It is also used in a human-to-human style for sharing files, and this raises the risks around file ownership. For example, if a user opts for deleting their local copy, it must be decided what to do with the service copy and other users' local copies, and how to inform all other users of the actions taken.
- **Collaborative Editing** is the participation of more than one contributor to the preparation of a document, which may equally contain text or programming code, for example. Several technologies are used in this domain, notably versioning, wikis and real-time collaboration. Versioning involves keeping the various contributors' document versions separate and eventually merging them. Wikis are web pages where changes are published for collaborators to inspect. Real-time collaboration involves actual concurrent editing. The last appears to be the most challenging from a socio-technical standpoint due to the intensive human interaction.
- **Electronic Exam** is the assessment of tests whose author ought to be kept anonymous from the evaluator to improve objectivity of the evaluation. It is far from trivial at least due to the requirement of authenticating the tests, linking each test to its candidate, only after marking. By minimising the need for the candidates' trust in the evaluator's objectivity, it has the potential to secure the way University exams and public competitions are held worldwide, hence huge societal impact. Its implementation as a web service raises challenges due to threats such as evaluator coercion and candidates' exchange or trading of credentials.

Table 1 lists five chief representatives per domain, discussed in the sequel of this Section.

Challenge Domain	**File Hosting**	**Collaborative Editing**	**Electronic Exam**
Service	Dropbox [80]	CVS [79]	Viatique [95]
	Box [76]	Google Docs [83]	INFOSAFE [86]
	Apple iCloud [85]	Etherpad [81]	NEMO-SCAN [87]
	Ubuntu One [94]	ShareLaTeX [91]	WATA [15]
	Microsoft Skydrive [97]	Papeeria [77]	Blind Grading Number [82]
	Bitbucket [75]	Overleaf [78]	SEB [90]

Table 1
Chief service examples per challenge domain

File Hosting is becoming more and more widespread, with Dropbox having reached 400 million users in June 2015 [52], and Box following from a distance. Alternatives exist tied to each of the common Operating Systems, such as Live Skydrive for Windows, iCloud for Apple and Ubuntu One for Linux. Each provides some related functionalities, such as online treatment of Microsoft Word documents. Bitbucket also provides a form of version control, making it useful for Collaborative Editing. These services are all proprietary, including the Ubuntu One client.

As for Collaborative Editing, one of the most widely used services is CVS, which does version control by means of conflict resolution and merging tools. Google Docs supports multiple-user collaborative

editing in real-time. So does Etherpad, but requires some local installation, in contrast to Google Docs. ShareLaTeX (formerly ScribTeX) is an online collaborative editor for LaTeX document preparation with online compilation, sided by the more recent Papeeria. These services are all closed-source, except CVS and Etherpad, which are open-source.

Electronic Exam is perhaps the least popular domain at the moment, but is bound to become widespread. Many European universities, such as Dublin City University and Imperial College, currently use their own systems, locally developed, for anonymous marking, as do the top USA academias, such as Stanford and Harward Law School. The latter rely on the Blind Grading Number system whereby each candidate is assigned a number to blind their details, and the number is somewhat released after marking. SEB is a browser specifically simplified to run exams securely, and is the only open-source project in this domain.

4.1. Challenges

We discuss the challenges for each domain.

File Hosting shows the popular Dropbox to be designed with simplicity in mind. A user can successfully permanently delete a file created by a collaborator without being warned that this action will also delete all collaborators' copies as soon as they access the service. One could think of addressing this either by statically negotiating a suitable policy at file creation time about file ownership, or by dynamically seeking confirmation on sensitive operations such as deletion from all collaborators; but both modifications would require reviewing the existing interfaces and corresponding human-computer interaction. Not only does this teach us that a viable solution that could be easily understood by every possible user is not trivial to design, but it also reconfirms the subtleties of the issues socio-technical analysis should account for. At present, only the browser interface of Dropbox allows deleted files to be restored, and we do not feel that this functionality is appropriately transmitted to those users who rely on the version integrated with their file manager. Only a socio-technical analysis could establish whether this holds true, in particular by instantiating the Example Use 1 of our methodology over both Dropbox interfaces. Also, instantiating our Example Use 2 would usefully distill out the personas expressed in front of this service. Instantiating our Example Use 3 would in turn require the definition of effective ways to convey the variety of security properties of the service to its users.

We also argue that the recent leak of sensitive files stored on Dropbox or on Box [96] was due to the insufficient consideration, which gives foundations to the present article, of service security and privacy as a socio-technical problem, and to the lack of that analysis that the article advocates. Both services offer a facility to let a user generate a unique web address for a file; the user could then share this address with others, who will be able to access the file without needing to log in the service, or even to possess a service account. Although such an address is difficult to guess, it is technically public, being carried around, for example, through web sites' referral data, hence has public exposure. While users currently get informative warnings before they can share their files through this facility, the providers' initial reaction was that this was not a security flaw but was rather to be blamed on the users, due to their lack of an "appropriate level of knowledge" [96].

Collaborative Editing sees CVS as a widespread service. However, our experience shows that its management of conflicting documents and conflict resolution strategies may be ill-understood even among Computer Scientists. This raises significant risks of loosing portions of documents, which only a socio-technical analysis can appropriately account for and ultimately suggest how to mitigate. The same ap-

plies to the support of Google Docs for Microsoft Word documents, which may seem complete but in fact is weak at least for the editing of tables. Although these issues veer towards usability, the Example Use 1 of our methodology would lead the analysis to highlight the cues reaching a given persona while she handles the conflict resolution ceremony, and our Example Use 2 would provide realistic personas.

Latex Lab brought an access control issue that is still open. As an external service to Google Docs, it required the user to explicitly allow it to access the user's files on Google Docs. However, if the user granted this, the account authorisation page on Google Docs would then show that Latex Lab had complete access to the account. This gave it the ability to read/write all user files, and not just those with the "tex" extension as the user might have understood. These sorts of partial access control issues over web services deserve attention because they stem from an environment, the web services, that a number of user may perceive as local to their computers, and this would determine the personas they express. Our Example Use 3 would be particularly appropriate here due to its focus on the substance of each and every security property and on how to express them through a user interface.

Electronic Exam brings in peculiar challenges. Viatique is a proprietary online marking system claiming "digital end-to-end management of anonymous marking" although this has not been confirmed by appropriate analysis. INFOSAFE provides physical tamper-evident sheets for written tests. Candidates physically write their personal details and seal them with a cover that is stuck by a permanent adhesive. After marking, the personal details can be retrieved by tearing off a perforated strip. However, the evaluator must still be trusted to do this only after marking. As with the Blind Grading Number system, INFOSAFE is not computer-supported. Not surprisingly, these seem to be the weakest two: the Blind Grading Number is vulnerable to human collusion, while INFOSAFE still requires trusting the evaluator to tear off the sheet cover after marking. NEMO-SCAN uses patented anonymity sheet covers with two parts, one with the covered candidate details, the other with a section to type the mark on. At notification time, both parts are entered in a scanner and the proprietary software reads the candidate details and so assigns the mark.

WATA is software developed at the University of Catania, and successfully used on a departmental scale. It uses conventional printouts and gives the ability to de-anonymise a test solely to the candidate who wrote that test. This works well in a threat model where each candidate wants to be marked anonymously [15]. Porting it over a client-server architecture [14] and then re-implementing it as a web service [18] raised a variety of additional security challenges. This domain is a clear challenge for socio-technical analysis due to the vast participation of humans in sensitive operations. These operations will enable security and privacy only if carried out in a specific way, and will hinder it otherwise. For example, test sheets should be randomly distributed to candidates otherwise the examiner could learn by heart the test identifier of a specific candidate. This is easy to achieve by asking each candidate to collect the test sheets at random from a pile sitting on a desk.

Once more, any analysis within this growing domain must be socio-technical; for example, it cannot be anticipated how random candidates would understand Viatique's claim quoted above, and what sort of personas they would express — a clear call for the Example Use 1. Example Use 2 of our methodology could tell us whether candidates exhibit attentive personas that would claim random distribution of test sheets should the invigilator attempt to distribute them manually. Our Example Use 3 would lead to user interfaces capable of signaling the variety of security properties of WATA.

5. Conclusions

Service computing is tightly intertwined with human interaction. The security and privacy problem then acquires more facets than the typical technical problem has. It cannot conclude with evidence that the technology works as intended by its designers because that technology is meant to be practically used by humans. They may have varying degrees of familiarity with computers, so fail or refuse to use it as intended by its designers. Hence, security and privacy should be considered a socio-technical problem and treated accordingly.

This article described the relevant literature, an overarching analysis methodology and three domains of services that are challenging for a socio-technical analysis. It was noted that the literature in the analysis of service security and privacy is not huge. The three challenge domains involved a total of 18 services of large use, along with a few examples of the issues forming the socio-technical problem each service raises. It was easy to explain how these issues escape a traditional technical analysis, namely one where the presence of the human is overlooked.

As for the ceremony concertina traversal methodology, the article explained how it prescribes the various layers that combine the technology with the human to be analysed systematically. This encompasses research on security and privacy in various areas, identified by the layers of the underlying model, such as networks and service infrastructures, Operating Systems, user interface design, personas that users express in front of the technology and societal influence.

Positioning the methodology within the existing literature highlighted that each user has been treated as a monolithic entity so far. By contrast, the user may express various personas depending on how they feel about the specific service they face, and on how they feel at a specific point in time. The same user might be very careful with Internet banking and very relaxed with a one-click purchase from their favourite shopping site. It remains to be fully understood how such different personas may influence each other through the self, or how technology may inspire a specific persona to certain user groups.

The ceremony concertina traversal methodology implicitly demands the definition of appropriate threat models and realistic requirements for the systems, as well as a variety of skills and research methods for researchers. Computer Scientists could introduce formal methods, which bring the rigour of mathematical reasoning, Social Scientists could introduce empirical methods, which ground all arguments upon real users, and psychologists could introduce analytical methods, which insist on structure and schematisation. This transdisciplinary combination of efforts towards the practical enforcement of security and privacy seems the biggest challenge ahead.

References

[1] A tool to evaluate the business intelligence of enterprise systems. *Scientia Iranica*, 18(6):1579–1590, 2011.

[2] M. A. S. A. Beautement and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proc. of the 2008 Workshop on New Security Paradigms (NSPW'08)*, pages 46–58. ACM, 2008.

[3] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. of the 28th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115. ACM Press, 2001.

[4] R. Ali, C. Solís, I. Omoronyia, M. Salehie, and B. Nuseibeh. Social adaptation — when software gives users a voice. In *Proc. of the 7th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE'12)*, pages 75–84, 2012.

[5] C. S. Alliance. Security guidance for critical areas of focus in cloud computing. Technical Report Version 3.0, CSA, 2011.

[6] R. J. Andersen. *Usability and Psychology*, chapter 2. Security Engineering. Wiley Publishing, Inc., 2008.

[7] M. Arapinis, S. Bursuc, and M. Ryan. Privacy-supporting cloud computing: Confichair, a case study. In *Proc. of the 1st Conference on Principles of Security and Trust (POST'12)*, pages 89–108. Springer, 2012.

[8] A. Armando, W. Arsac, T. Avanesov, M. Barletta, A. Calvi, A. Cappai, R. Carbone, Y. Chevalier, L. Compagna, J. Cuéllar, G. Erzse, S. Frau, M. Minea, S. Mödersheim, D. von Oheimb, G. Pellegrino, S. E. Ponta, M. Rocchetto, M. Rusinowitch, M. Torabi Dashti, M. Turuani, and L. Viganò. The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures. In *Proc. of the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'12)*, LNCS 7214, pages 267–282. Springer, 2012.

[9] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji. A methodology for empirical analysis of permission-based security models and its application to android. In *Proc, of the 17th ACM Conference on Computer and Communications Security (CCS'10)*, pages 73–84. ACM, 2010.

[10] G. Bella. *Formal Correctness of Security Protocols*. Information Security and Cryptography. Springer, 2007.

[11] G. Bella. The principle of guarantee availability for security protocol analysis. *International Journal of Information Security*, 9:83–97, April 2010.

[12] G. Bella and L. Coles-Kemp. Internet users' security and privacy while they interact with Amazon. In *Proc. of IEEE International Workshop on Trust and Identity in Mobile Internet, Computing and Communications (IEEE TrustID'11)*. IEEE Press, 2011.

[13] G. Bella and L. Coles-Kemp. Layered analysis of security ceremonies. In D. Gritzalis, S. Furnell, and M. Theoharidou, editors, *Proc. of the 27th IFIP International Information Security and Privacy Conference (IFIP SEC'12)*, volume 376 of *IFIP Advances in Inf. and Communication Technology*, pages 273–286. Springer, 2012.

[14] G. Bella, L. Coles-Kemp, G. Costantino, and S. Riccobene. Remote management of face-to-face written authenticated though anonymous exams. In *Proc. of the 3nd International Conference on Computer Supported Education (CSEDU'11)*, pages 431–437. INSTICC Press, 2011.

[15] G. Bella, G. Costantino, and S. Riccobene. Wata: A system for written authenticated though anonymous exams. In J. Cordeiro and B.Shishkov, editors, *Proc. of the 2nd International Conference on Computer Supported Education (CSEDU'10)*, pages 132–137. INSTICC Press, 2010.

[16] G. Bella, P. Curzon, R. Giustolisi, and G.Lenzini. A socio-technical methodology for the security and privacy analysis of services. In *Proc of the 38th IEEE International Computer Software and Applications Conference Workshops (COMPSACW'14)*, pages 401–406. IEEE Press, 2014.

[17] G. Bella, R. Giustolisi, and G.Lenzini. Socio-technical formal analysis of TLS certificate validation in modern browsers. In J. C.-R. et al., editor, *Proc. of the 11th International Conference on Privacy, Security and Trust (PST'13)*, pages 309–316. IEEE Press, 2013.

[18] G. Bella, R. Giustolisi, and G.Lenzini. Secure exams despite malicious management. In *Proc of 12th International Conference on Privacy, Security and Trust (PST'14)*, pages 274–281. IEEE Press, 2014.

[19] S. Bensalem, V. Ganesh, Y. Lakhnech, C. MuÃśoz, S. Owre, H. RueÃ§, J. Rushby, V. Rusu, H. SaÃŕdi, N. Shankar, E. Singerman, and A. Tiwari. An overview of SAL. In *Proc. of the 5th NASA Langley Formal Methods Workshop (LFM 2000)*, pages 187–196, 2000.

[20] B. Blanchet. An efficient cryptographic protocol verifier based on Prolog rules. In *Proc. of the 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, pages 82–96. IEEE Press, 1998.

[21] M. Blaze. Toward a broader view of security protocols. In *Proc. of the 12th Security Protocols Workshop (SPW'04)*, pages 106–120. Springer, 2004.

[22] H. Bowman, G. P. Faconti, and M. Massink. Towards integrated cognitive and interface analysis. *ENTCS*, 43:97–112, 2001.

[23] M. C. Carlos. *Towards a Multidisciplinary Framework for the Design and Analysis of Security Ceremonies*. PhD thesis, Royal Holloway, University of London, 2014.

[24] M. C. Carlos, J. E. Martina, G. Price, and R. F. Custódio. An updated threat model for security ceremonies. In *Proc. of the 28th Annual ACM Symposium on Applied Computing (SAC'13)*, pages 1836–1843. ACM, 2013.

[25] K. B. Carnelley and A. C. Rowe. Priming a sense of security: What goes through people's minds? *Journal of Social and Personal Relationships*, 2:253–261, 2001.

[26] S. R. Carter and D. A. Walsh. A hypercard-based tool for studying cognitive processes in complex problem solving. *Behavior Research Methods, Instruments, & Computers*, 24(2):286–297, 1992.

[27] D. Catteddu and G. Hogben. Benefits, risks and recommendations for information security. Technical report, ENISA, November 2009.

[28] D. Cohen. *Fear, Greed and Panic: The Psychology of the Stock Market*. John Wiley & Son Ltd, 2001.

[29] L. F. Cranor. A framework for reasoning about the human in the loop. In *Proc. of the 1st Conference on Usability, Psychology, and Security*, pages 1:1–1:15. USENIX Association, 2008.

[30] L. F. Cranor and S. Garfinkel. *Security and Usability: Design Secure Systems that People can use*. O'Reilly Media, 2005.

[31] S. J. Creese, M. Goldsmith, A. W. Roscoe, and I. Zakiuddin. The attacker in ubiquitous computing environments: Formalising the threat model. In *Proc. of the 1st International Workshop on Formal Aspects in Security and Trust (FAST'03), Pisa*, 2003.

[32] S. J. Creese, M. H. Goldsmith, A. W. Roscoe, and I. Zakiuddin. Authentication in pervasive computing. In *Proc. of the 1st International Conference on Security in Pervasive Computing*, March 2003.
[33] C. Ellison. Ceremony design and analysis. Technical report, International Association for Cryptologic Research, 2007.
[34] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini. A conceptual framework to study socio-technical security. In T. Tryfonas and I. Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *LNCS*, pages 318–329. Springer, 2014.
[35] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini. Socio-technical security analysis of wireless hotspots. In *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *LNCS*, pages 306–317. Springer, 2014.
[36] S. Gajek, M. Manulis, and J. Schwenk. User-aware browser-based mutual authentication via passwords and cookies with provable security on top of TLS. *Journal of Applied Cryptography*, 1(4):290–308, 2009.
[37] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, and M. Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. In *Proc. of the IEEE 3rd International Conference on Cloud Computing Technology and Science*, pages 231–238. IEEE Press, 2011.
[38] E. L. Gunter, A. Yasmeen, C. A. Gunter, and A. Nguyen. Specifying and analyzing workflows for automated identification and data capture. In *Proc. of the 42st Hawaii International International Conference on Systems Science (HICSS-42 2009), Proceedings (CD-ROM and online), 5-8 January 2009, Waikoloa, Big Island, HI, USA*, pages 1–11. IEEE Press, 2009.
[39] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proc. of the 2009 New Security Paradigms Workshop (NSPW'09)*, pages 133–144. ACM, 2009.
[40] R. Hyman. The psychology of deception. *Annual Review of Psychology*, 40:133–154, 1989.
[41] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In *Proc. of the 28th International Conference on Human Factors in Computing Systems, Atlanta, GE, USA*, pages 383–392. ACM, 2010.
[42] P. Jaferian, K. Hawkey, A. Sotirakopoulos, and K. Beznosov. Heuristics for evaluating it security management tools. In *Extended Abstracts on Human Factors in Computing Systems (CHI'11)*, 2011.
[43] T. N. Jagatic, M. J. N. A. Johnson and, , and F. Menczer. Social phishing. *Comm. of the ACM*, 10(50):94–100, 2007.
[44] S. Jana and V. Shmatikov. EVE: Verifying correct execution of cloud-hosted web applications. In *Proc. of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud'11)*, pages 11–11, 2011.
[45] W. Jansen. Cloud hooks: Security and privacy issues in cloud computing. In *Proc. of the 44th Hawaii International Conference on System Sciences (HICSS'11)*, pages 1–10, 2011.
[46] W. Jansen and T. Grance. Guidelines on security and privacy in public cloud computing. Technical Report 800-144, NIST - National Institute of Standard and Technology, January 2011.
[47] C. Karlof, J. D. Tygar, and D. Wagner. Conditioned-safe ceremonies and a user study of an application to web authentication. In *Proc. of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*, pages 1–20. ACM, 2009.
[48] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing*, 5:734–749, 2009.
[49] S. Lachapelle. From the stage to the laboratory: Magicians, psychologists, and the science of illusion. *Journal of the History of the Behavioral Sciences*, 44(4):319–334, 2008.
[50] J. Lazar, J. H. Feng, and H. Hochheiser. *Research Methods in Human-computer Interaction*. John Wiley & Sons Inc, 2009.
[51] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf. NIST cloud computing reference architecture. Technical Report Special Publication 500-292, NIST - National Institute of Standard and Technology, 2011.
[52] M. Lynley. Dropbox now has more than 400 million registered users. `http://techcrunch.com/2015/06/24/dropbox-hits-400-million-registered-users/`, 2015.
[53] T. Martimiano, J. E. Martina, M. M. Olembo, and M. C. Carlos. Modelling user devices in security ceremonies. In *Proc. of the 4th Workshop on Socio-Technical Aspects in Security and Trust, (STAST'14)*, pages 16–23. IEEE Press, 2014.
[54] J. E. Martina, E. dos Santos, M. C. Carlos, G. Price, and R. F. Custódio. An adaptive threat model for security ceremonies. *International Journal of Information Security*, 2(14), 04 2014.
[55] P. Masci and P. Curzon. Checking user-centred design principles in distributed cognition models: a case study in the healthcare domain. In *Information Quality in eHealth: the 7th Conference of the Austrian Computer Society Workgroup: Human-Computer Interaction*, volume 7058 of *LNCS*, pages 95–108. Springer, 2011.
[56] P. Masci, P. Curzon, A. Blandford, and D. Furniss. Modelling distributed cognition systems in PVS. In *Proc. of the 4th International Workshop on Formal Methods for Interactive Systems (FMIS'11)*, volume 45 of *Electronic Communications of the EASST*. EASST Press, June 2011.
[57] P. Masci, R. Rukšėnas, P. Oladimeji, A. Cauchi, A. Gimblett, Y. Li, P. Curzon, and H. Thimbleby. The benefits of formalising design guidelines: a case study on the predictability of drug infusion pumps. *Innovations in Systems and Software Engineering*, 11(2):73–93, 2015.

[58] P. Mell and T. Grance. The NIST definition of cloud computing. Technical Report Special Publication 800-145, NIST - National Institute of Standard and Technology, 2011.
[59] K. Mitnick and W. Simon. *the Art of Deception*. Wiley Publishing Inc., 2002.
[60] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. Springer, 2002. LNCS Tutorial 2283.
[61] S. Owre, J. M. Rushby, and N. Shankar. PVS: A Prototype Verification System. In D. Kapur, editor, *Proc. of the 11th International Conference on Automated Deduction (CADE'92)*, volume 607 of *LNCS*, pages 748–752. Springer, 1992.
[62] C. P., R. R., and B. A. An approach to formal verification of human-computer interaction. *Formal Aspects of Computing*, 4(19):512–550, 2007.
[63] E. Paja, F. Dalpiaz, and P. Giorgini. Managing security requirements conflicts in socio-technical systems. In *Proc. of the 32nd International Conference on Conceptual Modeling (ER 2013)*, pages 270–283, 2013.
[64] S. Parkin, A. van Moorsel, P. G. Inglesant, and M. A. Sasse. A stealth approach to usable security: Helping IT security managers to identify workable security solutions. In *Proc. of the 2010 New Security Paradigms Workshop (NSPW'10)*, pages 33–50. ACM, 2010.
[65] K. Radke, C. Boyd, J. G. Nieto, and M. Brereton. Ceremony analysis: Strengths and weaknesses. In *Proc. of the IFIP Information Security Conference (SEC2011), June 7-9, 2011, Lucerne, Switzerland*, pages 104–115. Springer, 2011.
[66] J. M. J. Reagle. Social protocols. `http://www.w3.org/Talks/980922-MIT6805/SocialProtocols.html`, 1998.
[67] R. Rukšėnas, P. Curzon, and A. Blandford. Modelling and analysing cognitive causes of security breaches. *Innovation in Systems and Software Engineering*, 4(2):143–160, 2008.
[68] J. M. Rushby. Analyzing cockpit interfaces using formal methods. *ENTCS*, 43:1–14, 2001.
[69] B. Schneier. John Wiley & Sons, 2000.
[70] B. Schneier. The psychology of security. `http://www.schneier.com/essay-155.html`, 2008.
[71] J. Somorovskly, M. Jensen, J. Schwenk, M. Heiderick, N. Gruschka, and L. L. Iacono. All your clouds are belong to us: security analysis of cloud management interfaces. In *Proc. of the 3rd ACM Workshop on Cloud Computing Security (CCSW'11)*, pages 3–14, 2011.
[72] F. Stajano and P. Wilson. Understanding scam victims: seven principles for systems security. Technical Report UCAM-CL-TR-754, University of Cambridge, August 2009.
[73] URL. Amazon mechanical turk. `http://aws.amazon.com/mturk/`.
[74] URL. Angelo gargantini's web page. `http://cs.unibg.it/gargantini/`.
[75] URL. Bitbucket. `https://bitbucket.org/`.
[76] URL. Box. `https://www.box.com/`.
[77] URL. Cloud research platform. `https://papeeria.com`.
[78] URL. Collaborative Writing and Publishing. `https://www.overleaf.com/`.
[79] URL. CVS — Concurrent Versions System. `http://cvs.nongnu.org/`.
[80] URL. Dropbox. `https://www.dropbox.com/`.
[81] URL. The Etherpad foundation — collaborate on documents in really real-time. `http://etherpad.org/`.
[82] URL. Evidence of use of Blind Grading Numbers at Stanford Law School. `http://www.law.stanford.edu/school/offices/osa/pdf/at_the_exam.pdf`.
[83] URL. Google Docs — Online documents. `https://docs.google.com/`.
[84] URL. The heartbleed bug. `http://heartbleed.com/`.
[85] URL. iCloud. `https://www.icloud.com/`.
[86] URL. INFOSAFE. `http://www.anonymousmarking.com/`.
[87] URL. Nemo-Scan — anonymous marking made simple and secure. `http://www.neoptec.com/en/products/nemo-scan/presentation.php`.
[88] URL. Opera mini. `http://en.wikipedia.org/wiki/Opera_Mini`.
[89] URL. Persona's machine-learning app lets people follow different sides of your twitter identity. `http://techcrunch.com/2014/09/07/prismatic-identity/`.
[90] URL. Safe Exam Browser. `http://safeexambrowser.org/`.
[91] URL. ScribTeX — Online LaTeX editor. `http://www.sharelatex.com/`.
[92] URL. Supercomputers: Obama orders world's fastest computer. `http://www.bbc.com/news/technology-33718311`.
[93] URL. TortoiseSVN the coolest interface to (Sub)version control. `http://tortoisesvn.net/`.
[94] URL. Ubuntu One. `https://one.ubuntu.com/`.
[95] URL. Viatique — platform for marking exams online. `http://www.neoptec.com/en/products/viatique/presentation.php`.
[96] URL. Warning over unintentional file leak from storage sites. `http://www.bbc.com/news/technology-27285786`.

[97] URL. Windows Live SkyDrive. https://skydrive.live.com.
[98] R. West. The psychology of security. *Communications of the ACM*, 51(4):34–38, April 2008.
[99] B. Whitworth. Social-technical systems. *Encyclopedia of Human Computer Interaction*, pages 533–541, 2006.
[100] B. Whitworth. *Socio-technical Design and Social Networking Systems*, chapter The Social Requirements of Technical Systems, pages 3–22. IGI Global, 2009.
[101] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proc, of the 17th ACM Conference on Computer and Communications Security (CCS'10)*, pages 176–186. ACM, 2010.