2014 IEEE 38th Annual International Computers, Software and Applications Conference Workshops

A Socio-Technical Methodology for the Security and Privacy Analysis of Services

Giampaolo Bella
Dipartimento di
Matematica e Informatica
University of Catania, Italy
Email: giamp@dmi.unict.it

Paul Curzon
School of Electronic Engineering
and Computer Science
Queen Mary University of London
Email: p.curzon@qmul.ac.uk

Rosario Giustolisi
Interdisciplinary Centre for
Security Reliability and Trust
University of Luxembourg
Email: rosario.giustolisi@uni.lu

Gabriele Lenzini
Interdisciplinary Centre for
Security Reliability and Trust
University of Luxembourg
Email: gabriele.lenzini@uni.lu

***Abstract*—There is a widely accepted need for methodologies to verify the security and privacy of services. A typical service requires user data and then makes them available through the Internet independently from access platforms or user locations, but the layman is rarely aware of the entailed risks and seldom acts cautiously. The combined human-and-technology system is complex: it intertwines the technical protocols that establish the technical security and privacy properties, with the social protocols that regulate human attitudes to and behaviour with computers. A number of security and privacy threats are therefore inherently socio-technical. An appropriate methodology to tackle security and privacy of web services from a socio-technical standpoint, namely when the human is in the loop, is still missing. This paper introduces one, termed the *ceremony concertina traversal* methodology. It advocates that technology is analysed *in* the presence of the human through the various structural layers that arise, from computer processes to user personas. Layers should be analysed individually then in combination, so as to transmit the guarantees that the technology is sound to its users in practical scenarios.**

Keywords*—*security ceremony; concertina; cloud; cybersecurity; modelling; verification; awareness;

I. 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 an 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" [1]. 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 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 [2], 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 institutional LAN.

This suggests that an extended view of a security protocol is needed to include human users, social protocols and behaviours: that is, see the system as a much more complex socio-technical system. This extension of a security protocol is termed a *security ceremony* [3]. It is widely accepted within security circles that "security is a chain, and people are the weakest link in the chain" [4]; by contrast, our long-term goal is to establish security and privacy *in* the presence of the human. This calls for a socio-technical approach that 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.

An example of a transdisciplinary contribution comes from Bella and Coles-Kemp, who recently provided a model in support of the socio-technical analysis of security and privacy termed the *ceremony concertina* [5]. The concertina links technology to society through a number of *layers*, which represent the interposing stakeholders, ranging from computer processes to user personas. The present paper adopts that model and easily tailors it to service computing. The main contribution of this paper is the use of that concertina to define a socio-technical methodology for analysing security and privacy in the world of service computing. Termed the *ceremony concertina traversal* methodology, it 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 on certain layers rather than others, or on all layers at the same time.

Our methodology purposely does not prescribe specific research methods; rather, depending on the researcher's focus, the most appropriate research methods are left as their choice, to make among formal methods, analytical methods and empirical ones. The ceremony concertina model offers anyone from virtually any discipline, who wants to investigate socio-technical aspects of security and privacy, a canvas on which to paint their findings. Our ceremony concertina traversal methodology offers practical directions on where and how to paint on that canvas, namely obtain findings. The practical value is to enable the researcher to take the guarantees of security and privacy that the technology establishes and

978-1-4799-3578-9/14 $31.00 © 2014 IEEE
DOI 10.1109/COMPSACW.2014.69

transmit them reliably and effectively to its users. For example, Bella *et al* have recently adopted it successfully to analyse the TLS certificate validation ceremony [6], and Huynen *et al* to identify critical decision points in the ceremonies that users follow to access WiFi networks via Hotspots [7]. After the related work (§II), the present paper gives the full details of the methodology (§III), and concludes (§IV).

II. Related Work

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 [8]. Sometimes technical flaws may provide the basis for launching a social engineering attack. For example, in context-aware phishing [9], 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 customize its scamming messages to gain the victim's trust.

It has only recently become fully understood by security researchers that very many socio-technical attacks are possible because security mechanisms are not designed to be *used* by the users. This sounds paradoxical from a socio-oriented perspective, but it has roots in the usual practice of reproaching users who commit security naiveties after ignoring security advice. This practice is, indeed, being proved wrong: many users consider current security mechanisms unhelpful, if not completely annoying [10], to their daily work. This is the ultimate reason why people often bypass even the strongest security mechanism, and often in surprisingly ingenious ways [11]: the suggested "secure" behaviour is not sustainable from the usability-centred and psychology-centred point of view (economy) 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, and applying this knowledge to secure system design can be effective [12].

The socio-technical aspects of information security have 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 have been proposed to develop a formal background for the analysis of human factors [13] and fewer still applying this to security [14]. Few approaches include humans in the design of systems to improve their security [12]. Socio-technical security relates also to the understanding of the psychology of security [15] and of deception [16]. Stajano and Wilson published a useful study about how people fall victim to scams and frauds [17]. They observed that the victims' behaviour followed precise patterns, and identified 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" [18]. We share this viewpoint.

Conducting security analysis motivated Ellison in proposing *security ceremonies* [3]. 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 in understanding 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* [19]. The authors identify flaws in the Mini Opera browser ceremonies emerging from the HTTPS protocol when used in a certain context, despite the fact that the protocol is correct and secure in the traditional meaning of those terms. 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". This is a complementary perspective from that of provable security which, instead, aims to ensure that a protocol is secure regardless of how it is used. Similarly, Radke *et al* comment on the security of a ceremony that involves the TLS protocol [20]. Karlof *et al* proposed design principles for obtaining conditioned-safe ceremonies [2]. A conditioned-safe ceremony is one that conditions users to take safe decisions even in the presence of social engineering attacks. They evaluated their principles by conducting a study of over two hundreds participants, who were observed while using different email registration/authentication ceremonies that where occasionally attacked by an adversary. Martina and Carlos comment on formal approaches that can potentially be applied to analyse security ceremonies [21].

III. A Socio-Technical Methodology

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

A. Approach

Our methodology insists on a *multi-layer though integrated* approach to the analysis of the security of services. To the best of our knowledge, it is the first time that the analysis of services is advocated to happen in a multi-layer and integrated way. 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 [6], rather than merely technical ones such as key confidentiality in the traditional sense of security protocol analysis [22]. As it shall be seen below, it is the integrated approach what makes the analysis of practical value for real-world mass use. The findings at the various layers are combined to provide assurances or pinpoint weaknesses to the actual human users of the services.

It is worth remarking that our methodology is not concerned with software verification. Rather, it is designed to support the upcoming formal analysis of abstract specifications

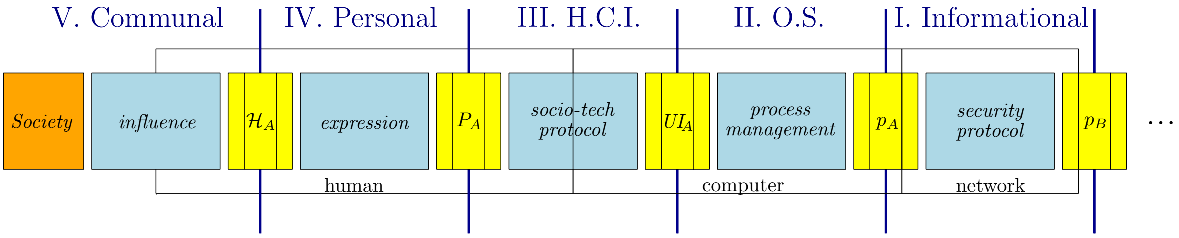

Fig. 1. The model of the full security ceremony [5] underlying our research methodology

of protocols with their surrounding use contexts, rather than of actual programming code.

B. Model

As mentioned above, a security ceremony expands a security protocol with the out-of-band, notably with the user [3]. Our research leverages upon the recent model of security ceremonies of Bella and Coles-Kemp [5], in Figure 1.

The model identifies several layers, which go beyond the original ceremonies between users and systems as described by Ellison [3]. This ceremony model is capable of capturing additional elements of the interaction between users and technology. This aim is also supported by Whitworth [23], 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 [24]. 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 exchange 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 graphical user interface, such as by filling in forms. This is clearly a technical protocol because of the interaction with the technology, but is deeply intertwined with the social protocols [25] 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 outermore 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 contents with friends. Computer scientists typically tend to assume the most careless persona, hence to develop a technology that compels every possible user to a secure interaction; by contrast, social scientists often find this approach limitative and inappropriate to ensure user engagement and satisfaction, hence recommend consideration for a variety of personas.

Layer V, Communal, reflects the reciprocal influence of society, including other players, over individuals engaging in a security ceremony. For example, a national campaign could influence users towards being more careful in opening attachments from unknown sources. Someone working in a team might be influenced by the norms of that team.

Additional considerations on the full security ceremony now become intuitive. One is that adjacent layers share a player, who plays in both. Also, each layer features what is termed an *interaction* between a pair of players, such as the socio-technical protocol or the security protocol. Players only interact within a layer. Interacting players may not belong to the same user, as is 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 contribute this modified model by means of two modifications: 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. General pictures are omitted here due to space limitations, but the following example uses of the methodology (§III-D) feature some.

C. Steps

Our methodology could be termed the *ceremony concertina traversal* methodology, as it proceeds from the interpretation of the layers in the full security ceremony as a concertina. Therefore, the full security ceremony can be compressed or expanded conveniently, depending on the researcher's target: the ceremony layers of interest.

We are not aware of existing research 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 joint research by computer scientists with social scientists. Our ceremony concertina traversal methodology consists of two main steps.

Step 1. Traverse the target ceremony layers in isolation by means of semi-formal analysis. Here, *traversing a layer* means to analyse an interaction between a pair of players, but may also require analysing each player. The methodology does not compel us to traverse all layers of the full security ceremony extensively. By contrast, the methodology allows layers to be concertina-ed together, retaining the full ceremony in outline but abstracting away from the details of 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 both layers I and 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.

Step 2. Traverse the target ceremony layers in combination by means of semi-formal analysis, aiming at building the target traversal, that is one between human personas and technology. 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 aspect of the combination is achieved by attempting to reuse over a layer the formal techniques typically adopted over other layers, expecting fresh insights. For example, security and socio-technical protocols have many similarities though they concern different levels of abstraction, hence the reuse of typical interaction design techniques over security protocol analysis and vice versa appears promising.

An additional strength of our methodology is that the target traversal between human personas and technology could be built by composing shorter traversals, such as layer traversals, in many ways, and 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. For example, 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. This persona could then be assessed for its plausibility by empirical methods.

The target ceremony traversal could also be built from left to right. A social scientist could start with layer V 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 simple existing example occurs with respect to 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. Incidentally, Curzon's user model based analysis is one way to detect post-completion [26].

D. Example Uses

This section details three 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 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 (III-B). Precisely, because layer II is collapsed, the user interface for Alice and the process executing the security protocol for her coincide, indicated as UI_A; because Alice is interacting with a web service, this is monolithically indicated as p_B. The focus of the analysis is shaded, indicating its three parts: layer I (dashed border), layer II (dot-dashed border) and the user interface (dotted border). Each of these offers research challenges in their own right: the analyses of security protocols, of socio-technical protocols, of user interfaces and the interaction design all these embody.

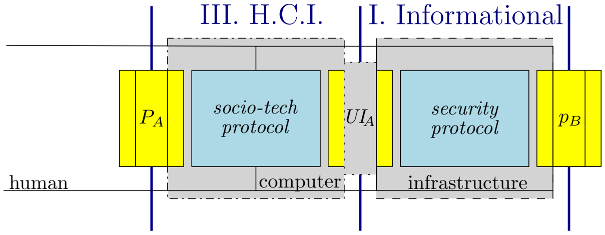

Fig. 2. The two-layered security ceremony instantiated over the infrastructure: focus of example use 1 of our ceremony concertina traversal methodology is shaded

In particular, analysing 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 (II). Finally, user interfaces with services are far from trivial to design well, 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 to leave only with the service.

The combined analysis of the system consisting of all shaded areas in Figure 2 appears to be more challenging. The ceremony traversal can be carried out in both directions according to what we described above (§III-C). In consequence, the findings of security protocol analysis will inspire socio-technical protocol analysis and vice versa.

Example 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 in facing certain technology at some point in time. Here, the interaction "expression" is drawn smaller than in Figure 1 to indicate that only a *part of* the interaction, as defined below, is targeted in this example use of the methodology.

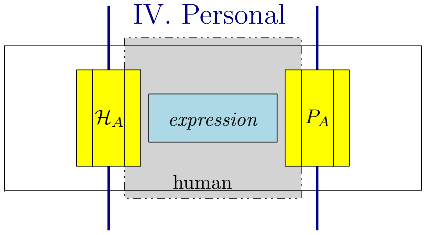

Fig. 3. Part of layer IV of the security ceremony: focus of example use 2 of our ceremony concertina traversal methodology is shaded

In this example, 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 [27]. Of course, these experiments require the availability of reasonably large sample populations to submit questionnaires to. This example use of our methodology is fundamental because it contributes to grounding other findings to the real world.

Example 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.

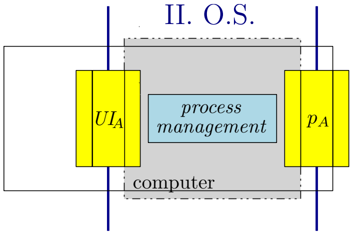

Fig. 4. Part of layer II of the security ceremony: focus of example use 3 of our ceremony concertina traversal methodology is shaded

Because Operating System analysis already is a large and well-established research area (with more than 39 million Google entries at 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 point the protocol process should send the interface process data signifying that end-to-end security has been established, which means that the interface process can display an appropriate visual signal — often a padlock or a green address bar — and that data clearly is security sensitive. Similarly, the data that the user enters in the interface often are privacy 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 very sense of security corresponding to the data. Such data in practice is not specific, and far from being standardised. In consequence, how the interface is to be notified, for example, that the security protocol authenticated the remote peer remains protocol-dependent. Moreover, also the cues that the user interface should use have not been codified, and are far from being standardised. Notably, a recent release of the Opera Mini browser, with its 144 million users each month worldwide [28], was found to display a padlock when an intermediate server interposes between the client and the server, hence without end-to-end security [19].

Another reason is that various interfaces could be used to access services while favouring the user 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 [29] and the File Hosting application Dropbox [30], with the standard program to explore the local file system.

This example use of our 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 on one hand, and consequently between process data and visual or acoustic signals. With standards in place, the future analyses would gain clear-cut objectives.

IV. 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 paper described a methodology for the socio-technical analysis of security and privacy of web services. The ceremony concertina traversal methodology prescribes the various layers that combine the technology with the human to be analysed systematically. This encompasses research on security and privacy of 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, societal influence, etc.

Our 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. For example, 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.

Acknowledgements G. Lenzini was supported by FNR, CORE project C11/IS/1183245 "Socio-Technical Analysis of Security and Trust".

References

[1] URL, "Angelo gargantini's web page," http://cs.unibg.it/gargantini/.

[2] 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), July 15-17, 2009, Mountain View, CA, USA*. ACM, 2009, pp. 1–20.

[3] C. Ellison, "Ceremony Design and Analysis," Cryptology ePrint Archive, Report 2007/399, Tech. Rep., 2007.

[4] B. Schneier, *Secrets and Lies*. John Wiley & Sons, 2000.

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

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

[7] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini, "Socio-technical Security Analysis of Wireless Hotspots," in *Proc. of the 16th Int. Conf. on Human Computer Interaction (HCI International), Heraklion, Crete, Greece, 22-27 June, 2014*, 2014, (to appear).

[8] K. Mitnick and W. Simon, *the Art of Deception*. Wiley Publishing Inc., 2002.

[9] T. N. Jagatic, M. J. N. A. Johnson and, , and F. Menczer, "Social Phishing," *Comm. of the ACM*, vol. 10, no. 50, pp. 94–100, 2007.

[10] C. Herley, "So Long, And No Thanks for the Externalities: the Rational Rejection of Security Advice by Users," in *Proceedings of the 2009 workshop on New security paradigms workshop*, ser. NSPW '09. New York, NY, USA: ACM, 2009, pp. 133–144.

[11] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proc. of the 28th Int. Conf. on Human Factors in Computing Systems, Atlanta, GE, USA*. ACM, 2010, pp. 383–392.

[12] 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 New Security Paradigms Workshop (NSPW 2010) Concord, MA, USA, Sept. 21-23, 2010*. ACM, 2010, pp. 33–50.

[13] H. Bowman, G. P. Faconti, and M. Massink, "Towards Integrated Cognitive and Interface Analysis," *ENTCS*, vol. 43, 2001.

[14] R. Rukšėnas, P. Curzon, and A. Blandford, "Modelling and Analysing Cognitive Causes of Security Breaches," *Innovation in Systems and Software Engineering*, vol. 4, no. 2, pp. 143–160, 2008.

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

[16] R. Hyman, "The Psychology of Deception," *Annu. Rev. Psychol.*, vol. 40, pp. 133–154, 1989.

[17] F. Stajano and P. Wilson, "Understanding scam victims: seven principles for systems security," Univ. of Cambridge, Tech. Rep. UCAM-CL-TR-754, August 2009.

[18] R. J. Andersen, *Usability and Psychology*, ser. Security Engineering. Wiley Publishing, Inc., 2008, ch. 2.

[19] 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*. Springer-Verlag, 2011, pp. 104–115.

[20] S. Gajek, M. Manulis, and J. Schwenk, "User-aware browser-based mutual authentication via passwords and cookies with provable security on top of TLS," *J. of Applied Cryptography*, vol. 1, no. 4, pp. 290–308, 2009.

[21] J. E. Martinal and M. C. Carlos, "Why Should We Analyse Security Ceremonies?" in *Proc. of CryptoForma Formal Methods and Cryptography: The Next Generation of Abstractions (CryptoForma) May 25, 2010, Paris, France*, 2010.

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

[23] B. Whitworth, "Social-technical systems," *Encyclopedia of Human Computer Interaction*, pp. 533–541, 2006.

[24] ——, *Socio-technical Design and Social Networking Systems*. IGI Global, 2009, ch. The Social Requirements of Technical Systems, pp. 3–22.

[25] J. M. R. Jr., "Social Protocols," http://www.w3.org/Talks/980922-MIT6805/SocialProtocols.html, 1998.

[26] C. P., R. R., and B. A., "An approach to formal verification of human-computer interaction," *Formal Aspects of Computing*, vol. 4, no. 19, pp. 512–550, 2007.

[27] J. Lazar, J. H. Feng, and H. Hochheiser, *Research Methods in Human-computer Interaction*. John Wiley & Sons Inc.

[28] URL, "State of the mobile web: The mobile webs top 10 sites in 2011," http://www.opera.com/press/releases/2011/12/20/.

[29] ——, "TortoiseSVN the coolest interface to (Sub)version control," http://tortoisesvn.net/.

[30] ——, "Dropbox," https://www.dropbox.com/.