Invisible Security

Giampaolo Bella[1(✉)], Bruce Christianson[2], and Luca Viganò[3]

[1] Dipartimento di Matematica e Informatica, Università di Catania, Catania, Italy
giamp@dmi.unict.it
[2] School of Computer Science, University of Hertfordshire, Hatfield, UK
[3] Department of Informatics, King's College London, London, UK

Abstract. In the last decades, digital security has gone through many theoretical breakthroughs, practical developments, worldwide deployments and subtle flaws in a continuous loop. It is mainly understood as a property of a technical system, which is eventually built as a tangible piece of technology for common people to use. It has therefore been assessed in terms of its correctness because it may easily go wrong, of its usability because it may be difficult to interact with, and of its economics because it may be inconvenient to deploy, maintain or re-deploy.

In line with the theme "Evolving Security" of this year's Security Protocols Workshop, our view is that the shape of security as outlined above is in fact getting more and more multifaceted as we write. It was at the same event last year when we depicted an additional facet of security that is its being beautiful [1], namely inherently desirable for its users. Here, we further observe that security should be invisible in the sense that the user's perceived burden of complying with it be negligible. Through a few past, present and (advocated) future examples, this position paper supports invisibility as yet another desirable facet of security.

1 Position

A number of works have advocated that digital security suffers limitations during its practical use and that consequently it should be implemented through a number of defences in depth. By contrast, the current Millennium has taught us that innumerable people consider security an annoying burden and a fastidious waste of time. It is difficult to tell whether this is due, among other reasons, to the adoption of mobile computing devices by a constantly increasing number of people, perhaps with a low attitude towards technology in general, or in haste while on the move.

In this recent, empirically instated setting, we dare contradict the literature (though only apparently, as we shall see) by postulating that the depth of the security mechanisms should be as thin as possible, so that people would not perceive security as an overhead and, rather, would comfortably comply with it. Upon these observations, this position paper poses the extreme question of whether that depth can be reduced so much that people would not notice it at all, and therefore security would become intangible, i.e., invisible to the users

J. Anderson et al. (Eds.): Security Protocols XXIV, LNCS 10368, pp. 1–9, 2017.
DOI: 10.1007/978-3-319-62033-6_1

of the technology to be secured. We shall demonstrate that *invisible security* is possible over some applications and, as such, qualifies as yet another facet of the shape of security.

It must be emphasised that we can shed some light on this new facet of the shape of security only if we take a *socio-technical view* at it, namely a view that accounts for the users as much as it does for the technology; this expands the more traditional *technical view* that saw many defences in depth. Arguably, the interrelation between these two points of view resolves the apparent contradiction hinted at above.

It would be an exaggeration to imagine that invisible security makes sense for every possible application, namely that security can always be made invisible and yet remain as effective as in "Minority Report" [2]. For example, user authentication should arguably be not invisible when the user is authenticating in order to operate a safety-critical application. Invisible security is for mass-use, non safety-critical applications such as those executed on a mobile device, whose users cannot be generally assumed to be security experienced *and* at the same time security aware.

Invisible security is coherent with the facet of beautiful security we introduced last year [1]. It stated that even security can be made beautiful and, by leveraging on some sort of Bettinelli's assumption that people tend to beauty [3], technology users would somewhat instinctively feel comfortable with it and avoid creative attempts at circumventing it. Beautiful security was found to enjoy at least three attributes: to be a primary system feature, not to be disjoint from the system functions, and to be ambassador of a positive user experience. The examples of invisible security found so far may see the security defence well integrated with some system function, thus sometimes meeting the second of the three attributes. Therefore, we can currently logically conclude that invisible security may also contribute to beautiful security.

This paper outlines four possible scenarios prescribing the integration of a security defence with other features of the technical system (Sect. 2). These could be a useful system function that the system users may desire, or an existing security defence that the system users can be assumed to be already happy with. Four examples of such defences are introduced, one per scenario, and their design is discussed and justified as an incarnation of invisible security; an additional, fifth example is advanced as a proposal to make thinner yet more robust the flight boarding protocol that is executed at the airport between a hostess and a passenger (Sect. 3). Remarkably, not only does the novel protocol make security more invisible for the users than the current protocol does, but the novel protocol also is more robust against potential distraction or neglect by the hostess in checking the passenger's boarding card. This is due to the fact that thinner checks are required to prevent an attack whereby two passengers exchange their destinations. Some conclusions terminate the presentation (Sect. 4).

2 Scenarios

This section begins by outlining four possible scenarios supporting the making of security more invisible than it used to be. Each scenario either sees a new security defence become intertwined with existing system features, or an existing security defence become simpler internally.

Scenario 1 *A new security defence is integrated into an existing function of the technical system.* In this scenario, an existing function that users are already used to is assumed.

Scenario 2 *A new security defence is integrated into a new function of the technical system.* A new system function is assumed to be useful and desirable for the system users.

Scenario 3 *A new security defence is integrated into an existing security defence.* A security defence is assumed to be already in place and at the same time to be well received by the system users.

Scenario 4 *An existing security defence is thinned.* An existing security defence is collapsed internally, hence made more invisible and less of a burden.

The next section will provide five example *ceremonies* within the given scenarios, where the term "ceremony" is used to describe a security defence and its human users [4–8].

3 Ceremonies

This section describes four ceremonies as they currently are. We shall see that their design can be considered an application of our principle of invisible security because the security defences are somewhat integrated and thinned with respect to an original design. The section concludes with a proposal to apply the same principle to a fifth example, derived from the flight boarding ceremony.

All our example ceremonies insist on a number of common roles. The following roles can be identified.

Prover (or P for brevity) is the principal who intends to prove his/her identity in order to obtain a service. It is traditionally played by a human being, namely a user who wants to get authenticated to the verifier through some technical system.

Technical system (or TS for brevity) is any piece of technology that may support the prover's authentication, e.g., a computer, a network of computers, a tablet, a smartphone or a smartwatch.

Verifier (or V for brevity) is the principal who intends to verify the identity of the prover. Depending on the application, it may either be played by a human being or coincide with the technical system.

Equipment$_1$, ..., **Equipment**$_n$ (or $E_1, \ldots, E_n$ for brevity) are each an additional tangible item, ranging from a dedicated piece of technology to paper documents, that the prover may appeal to in support of his/her authentication case.

We remark that the principle of invisible security is successfully applied to the following example ceremonies because the resulting security defences, though made more invisible than they were, are not generally weakened.

3.1 iPhone Authentication

Roles and Principals. P = iPhone user, TS = iPhone, $V = TS$. Example of Scenario 1.

Protocol Outline. The current protocol whereby a user authenticates to his/her iPhone can be seen as a successful attempt at making the user authentication protocol invisible. The protocol can be represented simply as follows:

$$\begin{array}{l} 1.\ P \longrightarrow V : \mathit{press}(\mathit{button}(V)) \\ 2.\ V \longrightarrow P : \mathit{ack} \end{array}$$

In particular, by leveraging on the fingerprint reading technology of iPhones, the authentication protocol was integrated with the screen-activation protocol, which originally involved pressing the home button, and indeed the *ack* is simply the granted access to the home screen. Therefore, this design practice is an example of Scenario 1.

Security Analysis. It seems fair to claim that authentication to an iPhone (or a similar smartphone or device equipped with a fingerprint reader) is now seamless, as opposed to more traditional devices without a fingerprint reader, on which the traditional user's quest at simplicity may result in the removal of every authentication procedure.

3.2 ICRTouch EPoS

Roles and Principals. P = waiter, TS = network of distributed tills, $V = TS$, E_1 =waiter's swipe card. Example of Scenario 2.

Protocol Outline. ICRTouch is a company producing solutions for restaurants. Its latest Electronic Point of Sale (EPoS) system relies on networked, distributed tills. It forces each waiter to authenticate to a till to be able to operate on an order and its bill. To support and facilitate authentication, a prover may swipe a personal card and enter a PIN number on any instance of the technical system, namely on any till. The protocol can be represented as follows:

$$\begin{array}{ll} 1.\ P \longrightarrow \mathit{instance}(1,V) & : \mathit{swipe}(E_1, \mathit{instance}(1,V)) \\ 2.\ \mathit{instance}(1,V) \longrightarrow P & : \mathit{ack} \\ & \vdots \\ 2m-1.\ P \longrightarrow \mathit{instance}(m,V) & : \mathit{swipe}(E_1, \mathit{instance}(m,V)) \\ 2m.\ \mathit{instance}(m,V) \longrightarrow P & : \mathit{ack} \end{array}$$

The card swiping was initially received as extra burden through the routine operations; however, it came coupled with an innovative function that turned

out to be very useful: the ability to view a standing order from any till in the shop, which here we have simply abbreviated as the *ack* that is provided by each till $instance(i, V)$. Therefore, this design practice is an example of Scenario 2.

Security Analysis. ICRTouch EPoS is arguably more secure than traditional order management systems not just because it enforces authentication before sensitive operations can be carried out, but because it does so by offering the prover something useful and desirable, namely a new function. In consequence, authentication works well in practice because the prover does not perceive it as useless overhead but, rather, as an add-on that dissolves into a wonderful function.

3.3 Hard-Disc Decryption

Roles and Principals. P = computer user, TS = computer, $V = TS$. Example of Scenario 3.

Protocol Outline. To thwart the risks of data leaks following computer thefts, users may encrypt their home folders using free programs. Traditionally, data at rest must first be decrypted before it can be profitably used. As a consequence, the user should enter a password to run the decryption service, followed by another one to pass the O.S.'s login procedure. Most hard-disc decryption programs integrate the two passwords, so that users do not notice any extra burden. The protocol can be represented as follows:

1. $P \longrightarrow V : insert\_password(P, V)$
2. $V \longrightarrow P : ack$

Here, the *ack* is simply the granted access to the home directory. This choice of internal integration assumes that users are currently happy to enter one password, as multi-user systems have made them become used to through the years. This means that one security defence, that is to enter a password at login time, belongs to the users' normal routine; by contrast, any extra effort to decrypt the home space does not. Therefore, this design practice is an example of Scenario 3.

Security Analysis. It is clear that if all home folders are protected by encryption, then users' security and privacy gain a great lot. Meeting the precondition is greatly facilitated if the security defence dissipates into one that is already well received, such as entering one password at login, and a user perceives no extra hassle.

3.4 Remote Car-Alarming

Roles and Principals. P = car owner, TS = car, $V = TS$, E_1 = car owner's remote control. Example of Scenario 4.

Protocol Outline. Historically, the power-door locks of cars were first operated by the car key and then by a dedicated remote control. In addition to the standard

locking mechanism, a user could have a car alarm installed to counter theft, and this alarm ultimately came with its own remote control. At some point were the two technologies integrated over a single remote control, resulting in the following protocol:

1. $P \longrightarrow V : \mathit{signal\_from\_pressing}(E_1)$
2. $V \longrightarrow P : \mathit{ack}$

Here, the *ack* could be the locking or opening of the doors, possibly accompanied by a flash of the car's lights and/or a toot by its horn. As a consequence, the user is currently able to lock the door and at the same time set the alarm remotely. Therefore, this design practice is an example of Scenario 4.

Security Analysis. We can assume that the two technologies, namely remote power-door locks and remote alarm, existed for some time based upon two separate remote controls. Yet, it is clear that their integration makes them more reliable for the simple fact that the chances of operating one system while forgetting the other one get zeroed.

3.5 Flight Boarding

Roles and Principals. P = passenger, TS = computer with checked-in passenger database, V = hostess, E_1 = passenger's electronically readable identifier, E_2 = passenger's boarding card. Example of Scenario 4.

Current Protocol Outline. The current protocol sees the passenger hand over two things to the hostess who stands at a gate: the passenger's identifier (passport or ID card) and boarding card (printed or displayed on a hand-held device). The hostess is called to check that the passenger's face matches the picture on the identifier, and that the details on the identifier match those on the boarding card; this is a customary, three-valued authentication check. The hostess also scans the boarding card in order to check that the passenger is authorised to fly to the particular destination currently set at the gate. The passenger will be allowed through the gate only if all these checks succeed. The hostess will ultimately return the two documents to the passenger. The protocol can be represented as follows:

1. $P \longrightarrow V : E_1, E_2$
   $V\,\mathit{checks}(E_1, E_2, P)$;
   $V\,\mathit{scans}(E_2)$;
   $\mathsf{if}\ \mathit{OK}(\mathit{all\_checks})\ \mathsf{then}\ \mathit{admitted}(V)$
2. $V \longrightarrow P : E_1, E_2$

Novel Protocol Outline. We suggest a novel boarding protocol that disposes entirely with the boarding card, in the sole assumption that the passenger's identifier can be read electronically, for example by NFC technology. The protocol is obtained from the previous one by merely pruning out any reference to the boarding card. Therefore, it can be described as follows:

1. $P \longrightarrow V : E_1$

   $V\,checks(E_1, P)$;
   $V\,scans(E_2)$;
   if $OK(all\_checks)$ then $admitted(V)$

2. $V \longrightarrow P : E_1$

It can be seen that the manual checks that the hostess has to do get simplified. In particular, the authentication checks reduce to a traditional, two-valued check between the passenger's face and their identifier. Scanning the identifier on the computer will then tell the hostess whether that passenger is allowed on that flight. Therefore, this design practice is an example of Scenario 4.

Security Analysis. Our novel boarding protocol works equally well as the currently known boarding protocol. This is possible because the passenger details can be read electronically from the identifier rather than from the boarding card via a QR code. In return, the passenger gets the bonus of the removal of the need to carry a boarding card, be it paper based or electronic on a smartphone.

From a security standpoint, the novel protocol seems more secure than the current one because the burden on the hostess is lightened, hence reducing the room for human error or distraction. The hostess may read the passenger details mechanically from the identifier rather than from the boarding card. Additionally, the hostess now only needs to check the passenger identifier to match the passenger. This simple check may ultimately thwart an attack whereby two accomplices pass security successfully and then attempt to exchange destinations at the gates; this attack could realistically succeed in the present setting where a passenger was able to board the wrong plane [9] and the issue hit the press perhaps only because the passenger denounced it. This attack is likely to have derived from distraction or negligence in checking also the boarding card, a need that our novel protocol removes.

Note that some airports enforce security procedures in which the boarding card is actually checked several times, e.g., before the passenger is admitted to the security control (where bags and people are scanned) and at the "border" control, before being admitted to the gate to board a flight to an international destination. If these additional procedures are in place, the protocol we discuss will of course require a modification not only of the boarding ceremony but also of the security check and passport control, but also these procedures would actually benefit from the simplified, more invisible security.

4 Conclusions

This paper advances the position that digital security comes with the yet vastly unexplored facet that we call "invisible security". It outlines four possible scenarios in which security has been made effectively more invisible than it was, namely less tangible as a burden for its users and yet perfectly working. It is clear that invisible security makes sense only upon the precondition of looking at

security from a socio-technical standpoint, otherwise we would be content with the more traditional rule of thumb of stacking up more and more defences in depth. Those are likely to look like requiring unjustified effort to the layman, who will therefore engage into finding ways to get around them in practice. This is how a whole stack of security defences may collapse in the real world.

The examples of security ceremonies discussed in relation to each scenario support the claim that invisible security has somewhat been up in the air without, we conjecture, being recognised as a useful facet of security and hence as a working principle to apply. As a result, users perhaps do not even realise that today they are authenticating to a smartphone without remembering a PIN, operating an advanced EPoS without wanting to sellotape their swipe cards to each and every till, decrypting their home space on their computer seamlessly, and locking and alarming their cars with a single press.

Leveraging on our notion as on a fully-fledged principle, we set out to simplify the flight boarding ceremony. The motivation for this choice was multiple. It is a tremendously common ceremony and it would seem desirable to eliminate the need to carry a boarding card and yet keep the ceremony secure. Also, the fact that a passenger recently boarded to the wrong flight shows room for a practical attack that sees two accomplices exchange destinations. Because this is likely to derive from error or distraction of the hostess who is at the gate, we set out to make the security of this ceremony more invisible. This was possible in the sole assumption that the passenger's identifier is electronically readable as it was done with a traditional boarding card. As a result, the checks that the hostess is called to operate are reduced.

We understand that some passengers may feel more relaxed by continuing to carry a boarding card, and of course this may be optionally issued at check-in time. Also, it is clear that our protocol may raise some negative business considerations, and some airline companies may not be happy with it. Quite a considerable percentage of their income comes from charging the passenger even 40 or 50 Euros to print a boarding card at a check-in desk. Since this is generally perceived as an unfair charge by the passengers, we believe that our novel boarding protocol will actually enhance the user experience, ultimately benefiting the airline company as well.

In terms of research, our boarding protocol demonstrates that the current technology makes it possible to effectively simplify such a widespread security ceremony so that a traditional textbook contradiction is subverted: not only security enhances but at the same time also the user experience improves.

References

1. Bella, G., Viganò, L.: Security is beautiful. In: Christianson, B., Švenda, P., Matyáš, V., Malcolm, J., Stajano, F., Anderson, J. (eds.) Security Protocols 2015. LNCS, vol. 9379, pp. 247–250. Springer, Cham (2015). doi:10.1007/978-3-319-26096-9_25
2. Minority Report: A movie directed by Steven Spielberg and starring Tom Cruise. The screenplay was written by Scott Frank and Jon Cohen, quite loosely based on a short story by Philip K. Dick (2002)

3. Bettinelli, S.: Tomo secondo che contiene l'Entusiasmo. Dalle Stampe Zatta (1780)
4. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IAICT, vol. 376, pp. 273–286. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30436-1_23
5. Bella, G., Curzon, P., Lenzini, G.: Service security and privacy as a socio-technical problem. J. Comput. Secur. **23**, 563–585 (2015)
6. Ellison, C.M.: Ceremony design and analysis. IACR Cryptology ePrint Archive 2007: 399 (2007)
7. Martina, J.E., dos Santos, E., Carlos, M.C., Price, G., Custódio, R.F.: An adaptive threat model for security ceremonies. Int. J. Inf. Sec. **14**, 103–121 (2015)
8. Radke, K., Boyd, C., Gonzalez Nieto, J., Brereton, M.: Ceremony analysis: strengths and weaknesses. In: Camenisch, J., Fischer-Hübner, S., Murayama, Y., Portmann, A., Rieder, C. (eds.) SEC 2011. IAICT, vol. 354, pp. 104–115. Springer, Heidelberg (2011). doi:10.1007/978-3-642-21424-0_9
9. Smith, R.: Ryanair passenger gets on wrong plane and flies to Sweden instead of France (2012). http://www.mirror.co.uk/news/uk-news/ryanair-passenger-gets-on-wrong-plane-946207