Cybersecurity's Way Forward: to get Beautiful or Invisible

Giampaolo Bella

Dipartimento di Matematica e Informatica, Università di Catania, Italy
giamp@dmi.unict.it

Abstract. People do not generally like Cybersecurity. Although they do believe it is somewhat good to have, they often cannot be bothered to go through security defences such as registrations, strong passwords' choices, PINs' long waits through the post and all the like. I do believe they are essentially right, especially if modern services are to be enjoyed on the move, while the user is hopping on the tube, or pervasively, while the user is also watching television. Sometimes users *have to* be bothered to go through such defences otherwise they will not get the service they wanted. They may then be nastily rewarded with senses of disappointment and frustration both if they opted to go on and if their pride or boredom prevented them to.
A layman at a cafe was arguing that he found Cybersecurity especially hideous when he was in a rush to get some service. Almost every researcher who looks at Cybersecurity from the socio-technical angle will agree with that layman as much as I do. This position paper outlines my view of the sole way forward for Cybersecurity: a fork in the road that takes either to Beautiful City or to Invisible City. One may of course refuse the fork and go back on the same road to Old City, where Cybersecurity often failed for a variety of reasons, including purely technical bugs and human-centred mistakes. I will postulate how I envisage Beautiful City and Invisible City to be. And do not worry you formal methodists: your help will be most appreciated also in the new cities.

1 Rationale

A modern understanding of Cybersecurity situates it in a real use scenario that sees human users approach a technology that is meant to be secure, and experience it or, more simply, just use it. This is certainly a fuller and yet more insightful understanding than the traditional one, at least because it is clear that no technology will be secure if its users keep the login passwords on sticky notes.

V. Biló, A. Caruso (Eds.): ICTCS 2016, Proceedings of the 17th Italian Conference on Theoretical Computer Science, 73100 Lecce, Italy, September 7–9 2016, pp. 1–7 published in CEUR Workshop Proceedins Vol-1720 at http://ceur-ws.org/Vol-1720

Here comes a new breed of views of Cybersecurity that are pivoted on the users, featuring the *social*, *economic* and *legal* views. These bear a huge potential to unveil niceties that could not be spot before, such as how easy it is for the layman to learn and comply with Cybersecurity, the coexistence with a deployed-though-flawed system version, and the assistance of the law to users who are victims of real-world breaches.

These new views entail what the Technocrats may perceive as a revolution: it will not suffice to look at the technical system in all sorts of ways to make it secure as they were used to do; by contrast, Scientists will have to look at the technical system holistically with its human users, and make that larger "system" secure. Arguably, Scientists will have to collaborate with colleagues from the Humanities to account for the human element. They will still only pass a technical system on to Engineers to build, but the resulting technology will be secure and privacy-preserving when practically used.

The new views of Cybersecurity in fact attract a worldwide, interdisciplinary task force of researchers at present. These are not just Computer Scientists but also Sociologists, Psychologists, Economists and Lawyers, confirming once and for all to everyone that the topic is not a purely technical one, as someone might have believed. A number of research events have appeared to publish the new research output, notably the Workshop on Socio-Technical Aspects in Security and Trust (STAST) [1], the Workshop on the Economics of Information Security (WEIS) [2], and the Workshop on TEchnical and LEgal aspects of data pRIvacy and SEcurity (TELERISE) [3] to just mention one per view.

2 Technology Users

Humans are difficult to fully account for, let alone formalise in the way dear to Formal Methodists. In particular, the human users of a technology are far from being automata executing the perfect program that the Technocrats behind that technology had in mind:

Users may be deceived It is consolidated at least since Mitnick published his famous book on deception that humans are rather easy to be duped into making insecure actions, such as choosing poor passwords or annotating secrets in insecure places [4]. It turns out that humans may effectively be tricked into facilitating the attacker's aims.

Users may make errors There exists vast work from the Humanities studying how and why humans make errors. Norman catalogued errors either as a failure to do what the user intends (*mistakes*) or a momentary lapse when the user takes an unintended action (*slips*) [5]. For example, both types of errors might be due to the often innate quest to operate in a best-effort way.

Users may choose to counter Cybersecurity When humans feel Cybersecurity as a burden more than as a benefit, they may deliberately ignore or oppose it. For example, some companies require card-and-PIN authentication to enter their premises or record work times, but Amazon suggests that cards can be left in a public card rack near the PIN pad [6].

3 The Cybersecurity Planet

I have done some research on the social view of Cybersecurity (not yet on the others), and this position paper gives me the opportunity to summarise and review some of my findings. At the moment, I see Cybersecurity as a planet with just three cities: Old City, Beautiful City and Invisible City. There exists a road that departs from Old, then forks and takes either to Beautiful or to Invisible. I am afraid that I have not explored anything else of that planet yet. It would seem that we researchers have been given the power to put the human users of the technology that we want to be secure in any of the three cities. I speculate that we used to choose Old but we had better take the users to either Beautiful or Invisible if we really care that technology to be secure.

3.1 Old City

This is the oldest city on the Cybersecurity planet, hence technology users have lived it for a long time. Here, Cybersecurity can be particularly hard to understand, interpret and use, and it can be realised empirically that it is often vulnerable. Vulnerabilities exist despite the Technocrats' best efforts at preventing them, hence all sorts of security incidents have happened over time.

Vulnerabilities are not only purely technical as with the SSL Heartbleed and Shellshock bugs. IBM reported that "*over 95 percent of all incidents investigated recognize 'human error' as a contributing factor*" in the 2014 Cyber Security Intelligence report [7], a trend that has not substantially changed ever since. One example dating back to a couple of years ago is how a user could deliberately share a file she stored on Dropbox or on Box with other users and inadvertently disclose it to unwanted parties[8]. Even the established policy of asking users to change their passwords from time to time may falter. It was recently found out that humans often resort to simple, algorithmic changes of the previous password to build the new one, hence attackers will just have to fine-tune their brute-forcing techniques [9]. Cybersecurity often intertwines with people's safety. Last year's Chatham House Report shouts out loud to the world that "*Some nuclear facilities do not change the default passwords on their equipment*" [10].

3.2 Beautiful City

In this city, Cybersecurity is beautiful [11], and I contributed some definition on what that means. Cybersecurity is beautiful if it satisfies a triple of abstract requirements: to be a primary system feature, not to be disjoint from the system functions to be secured, and to be ambassador of a positive user experience. I am going to expand them below.

The first one is not innovative by itself as it appeals to the security-by-design principle that the system should be designed with security in mind since the beginning; this normally enhances the ease of use and at the same time the effectiveness of the security defences. For example, security experts should contribute to the design of *at least* security-sensitive services since the inception.

The second requirement insists on what even security-by-design fails to prescribe clearly, that the secure access to a service be exclusive, namely the only possible one. For example, let us think of a web site secured via HTTPS yet allowing access also via HTTP for whatever legacy or performance reason. Also, when a user connects to a remote host via SSH for the first time, the user will have to accept the host's public key on trust rather than on a viable certification system.

The third requirement is perhaps the most abstract one. I would like Cybersecurity to be nice, desirable, rewarding and, generally speaking, a somewhat positive thing to have. One way to meet this requirement could be to aim at a Cybersecurity perceived as an engaging and fun game. An episode of the Peppa Pig cartoon portrays a group of kids wanting to be part of a "*secret club*" as soon as they come to know of its existence [12]. Can we manage to upturn people's currently negative perception of Cybersecurity to match the cartoon's?

The gist of the beautiful security principle is that all three requirements be met at the same time. It would seem that the use of the web interface of WhatsApp conforms to this principle. The web client prompts the server, who then issues a passcode for the former, stores it and sends it back; the web client displays it as a QR code, which the phone client (the app) scans and sends to the server along with the chat log stored on the phone. Only if the received version matches the stored version, will the server output the chat log to the web client.

Notably, it all takes place over HTTPS except for the step whereby the passcode reaches the phone, which involves a human pointing the phone to the computer screen to scan the QR code. This is a crucial design choice: the passcode is 128 characters long, hence it would have been super tedious for the user to have to read it from the computer screen and tap it in the phone. Here, QR-code scanning conjugates usability, simplicity, security and also some beauty. I gather from random discussions that QR-code scanning normally thrills people.

3.3 Invisible City

In Invisible City, Cybersecurity is not perceived by the technology users although it is still there. The idea is that if we cannot conjugate users and security by means of beauty, then the only option left seems to make security invisible, that is to literally make it invisible to the users' perceptions. I provided various examples on how this could be achieved in practice by integrating the security defences with system functions or with other defences that the users would accept as routine [13].

My favourite example is the Iphone 5S's integration of the screen activation button with the fingerprint sensor. This idea stemmed from the observation that people were used to a stand-by display being off to preserve battery, hence to the need of pressing some button to activate it when needed. This integration combined a routine action with an important security defence, user authentication to the phone, which otherwise required a separate ceremony to insert a PIN or password.

I argue that another security ceremony that could live well in this city would be a modification of the ceremony whereby passengers currently board flights (at the gates of Old City airport). Each passenger gives the gate attendant three pieces of information: the passenger's face, his ID and his boarding pass. The attendant matches face to ID, checks the ID validity, matches the ID to the boarding pass, scans the pass in the airport system and checks that the outcome confirms the identity that is allowed on the flight currently boarding. Only if all checks succeed will the passenger be allowed to go through, otherwise he will be stopped for further scrutiny. These are a number of checks for the attendant to carry out on each passenger in a long queue, hence not surprisingly some passengers complained to have reached the wrong destination [14].

With airport security being so sensitive at present, this scenario could be easily turned into various types of threats if the passenger attempted it deliberately and without reporting it. Therefore, I suggest to completely dispose with the boarding pass. This would leave only the initial authentication checks and the final authorisation one performed on the ID, which should be an electronic one, rather than on the pass. The match between the details of the ID with those of the boarding pass would be eliminated, reducing the risk of mismatching an authenticated identity to an identity that is authorised to board the flight.

4 Formal methods

I am a formal methodist down to the bone, so it is no surprise if I believe that formal methods can help a great lot to assess Cybersecurity from the socio-technical angle, hence to build both Beautiful City and Invisible City. I have published a few contributions to this debate [15,16]. In particular, I used the Cognitive Walkthrough usability inspection method to analyse Amazon's sub-ceremonies for price-quotation, shopping and purchase of the time, observing a few weaknesses. A notable one was that a user could choose a weak login password without getting any warning, and his credit card details would be recorded and protected merely by that weak password. Although these ceremonies have changed repeatedly over time, one of the conclusions of the analysis was:

> "*Amazon should clarify that the password that a user chooses during Registration has an impact on the confidentiality of their credit card details during network traversal at time of Purchase. Hence, Amazon should encourage each user to choose a strong password.*" [17].

The value of this recommendation does not expire; it could be generalised to every service recording users' sensitive information.

5 Conclusions

This position paper demonstrates my view of Cybersecurity as a socio-technical problem, namely one that pertains to both the technology and to how users

receive and avail themselves of it. Cybersecurity is a planet featuring Old City, one in which vulnerabilities and their exploitations are also due to an insufficient account on how humans use technology. I envisaged a road departing from Old City taking to either Beautiful City or to Invisible City, where I argued that Cybersecurity is more mindful of the human element. I also described some recent example uses of formal methods to help consolidate and expand the two new cities. Those are the places where I conclude that we researchers in Cybersecurity had better "move" the technology users from Old City.

References

1. URL: Workshop on socio-technical aspects in security and trust (2016) http://stast.uni.lu/.
2. URL: Workshop on the Economics of Information Security (2016) http://weis2016.econinfosec.org/.
3. URL: Workshop on TEchnical and LEgal aspects of data pRIvacy and SEcurity (2016) – http://www.iit.cnr.it/telerise2016/.
4. Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons (2001)
5. Norman, D.A.: Categorization of action slips. Psychological Review **88** (1981) 1–15
6. URL: STEELMASTER Swipe Card or Badge Rack (2016) https://www.amazon.com/STEELMASTER-Swipe-Capacity-Inches-20401/dp/B002V85VWQ.
7. URL: IBM Security Services 2014 Cyber Security Intelligence Index (2016) http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.
8. URL: Dropbox, Box users Leak Sensitive Information via Shared Links Flaw (2014) – http://techfrag.com/2014/05/08/dropbox-box-users-leak-sensitive-information-via-shared-links-flaw/.
9. URL: Frequent password changes are the enemy of security, FTC technologist says (2016) – http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/.
10. URL: Chatham House Report (2015) https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.
11. Bella, G., Viganò, L.: Security is Beautiful. In: Proceedings of the 23rd International Workshop on Security Protocols (SPW'15). LNCS 9379, Springer (2015) 247–250
12. URL: Peppa Pig, Series 3, Episode 38, "The Secret Club" (2010) https://www.youtube.com/watch?v=QSQhScDvOao.
13. Bella, G., Christianson, B., Viganò, L.: Invisible Security. In: Proceedings of the 24th International Workshop on Security Protocols (SPW'16). LNCS Series, Springer (2016) In press.
14. URL: Ryanair passenger gets on wrong plane and flies to Sweden instead of France (2012) – http://www.mirror.co.uk/news/uk-news/\discretionary{-}{}{}ryanair-passenger-gets-on-wrong-plane-946207.
15. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: IFIP SEC, Springer (2012) 273–286

16. Bella, G., Giustolisi, R., G.Lenzini: Socio-technical formal analysis of TLS certificate validation in modern browsers. In et al., J.C.R., ed.: Proc of 11th International Conference on Privacy, Security and Trust (PST'13), IEEE Press (2013) 309–316
17. Bella, G., Coles-Kemp, L.: 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) 878–883