Invisible Security
(Transcript of Discussion)

Giampaolo Bella[✉]

University of Catania, Catania, Italy
giamp@dmi.unict.it

I'm presenting joint work with Luca Viganò and Bruce, and it's all going to be about what I like to call *invisible security*. This concept tries to make the very security mechanisms and stakeholders that we have to go through in our everyday's lives less of a burden for ourselves, for the user. But before I dig into it, let me ask you a hopefully thought-provoking question. We are all used to fly, and therefore we all have to use boarding cards to board a flight: that's the protocol we have to go through. We have various versions of boarding cards, the most traditional version up here on the slide, then the printout version and the mobile version, but the question is, why do we need a boarding card in the first place, what are boarding cards there for? If you don't mind, I leave this question open, and I'll get back to it later on.

The current security baseline, the way we can look at security today, consists essentially of these two views. As a student I was taught the defense-in-depth principle, so don't just use one security mechanism, use many in a row because you have all sorts of limitations in the real world. Things may go wrong in practice when you implement the mechanisms, so use many in a row in such a way that if one breaks down, you still have all the other security mechanisms to make the attacker's life difficult hopefully. Well, this makes perfect sense for highly security-sensitive services or applications, such as military applications, or for example, industrial control systems (are they secure nowadays?) but it doesn't work equally well for our day-to-day applications.

I imagine a user who is doing security-sensitive transactions such as accessing her bank account while she is using a mobile phone hopping on the tube, and I'm not sure whether this user would like to have many security defenses to go through. So, when we take the socio-technical standpoint, a very interesting question would be whether we can compress the security mechanisms together and make them as thin as possible, and ultimately invisible to the user's eyes, to the user's perception. Of course, we would love them to be yet effective.

To answer this question, we have at least four approaches. Approach one says: assume there is a wonderful system function that the users tremendously like to have, like to use; if we manage to integrate the security defense to the system function, and I'll have examples of such integration, then the user, who is typically goal-oriented and wants that system function, will probably not realize the burden of having to go through the security defense. And you can do quite the same, approach two, if you have a new system function that turns out to be tremendously useful as well, and if you integrate the security defense to this new

system function, then you may get the same result that the user doesn't really realize that he's going through some hassle, or some security defense, simply because he wants the new system function.

Approach three says that you can do something very similar by conjugating two security defenses together. Suppose there is one mechanism that's well-established, well-accepted, either because it's very thin, very light, or because it's been there for many years so people accept it nowadays; for example, I'm thinking that we all have to enter a password when we switch on our laptop. If you integrate a new security defense with this old, previously well-established, security defense, then the burden of having to go through the new one will probably be compressed, and the user won't realize he's actually going through two security defenses tied together. Approach four says: let's compress a security defense internally, let's simplify it, let's make it thinner so that security will become ultimately more invisible.

I have examples of all these approaches, namely scenarios in which these approaches have been taken already or could be taken. The best example about approach one is the iPhone 5S's idea of integrating the fingerprint scan to the screen activation function. I think this was a cool idea, because we're all used to the fact that we need to somehow activate the screen of our phone before using it, in order to wake it up. Nowadays, when you press the button, you won't probably realize that you are actually going through a security defense because you just wanted to press the button, you had to press the button, you knew this beforehand. This is a clear example of integration of a security defense with a system function in such a way that they security defense will become more invisible.

Approach two can be exemplified easily as well. I remember that at last year's event Bruce put forward the example of an Electronic Point Of Sale system by ICRTouch which would ask each waiter to authenticate to the till by swiping a card and inserting a code. You may imagine that at the very beginning this was not very well received, we have a busy restaurant, waiters are running around, and they still have to authenticate, swipe, insert the PIN every time they need to use a till. But there may be many tills in a restaurant, and the waiters might find it nice, easy and ultimately convenient to be able to login to different tills depending on where they are in the restaurant. The new function that Bruce was describing last year is that they could find their standing orders inside any till they would login to. Very quickly was this found to be a useful function, and so the burden of swiping the card and then entering the PIN number was kind of forgotten because of this integration with a useful system function.

We now come up to the approach of integrating two security defenses together. If you really want to apply the defense-in-depth principle to your laptop, you would have to have a boot password, namely a BIOS/EFI password, then a password to decrypt your hard disk, then a user password. I wonder if we really use three passwords to operate our laptops. But here's a screen that comes from the Ubuntu installation routine: you may choose to encrypt your home folder, it's asking the user password here. What happens in practice is

that, after the installation, when you login by inserting that password, you're actually decrypting the home folder first, and then doing the routine user access procedure. The second and third passwords that I was describing earlier have been integrated together. You insert one password, but you still are activating two security mechanisms. Here's another example of approach three: with one remote control you activate the power-door locks of your car and you also activate an alarm system, but I remember many years ago people actually holding two remote controls, one for the car door locks, and one for the alarm system. These two mechanisms have been integrated together, and everything is much easier to actually use.

What about approach four? Here comes my question about why we need boarding cards in the first place. I'm showing you my personal distillation of the flight boarding protocol that is executed at the gate before you actually step on the aircraft. Essentially, the passenger will hand over to the gate attendant three pieces of information: face, an ID such as a passport, and the boarding card. What the attendant does is normally, check A, match your face to the picture on the passport in such a way to make sure that the passport really belongs to you. Then, check B, check if the passport has been tampered with. The attendant also uses the ID as a source of important information, your name and surname, which then, check C, the attendant will match to the name and surname on the boarding card. Ultimately, check D, she will scan the boarding card and use its information to query a database of all the people who are checked-in for that particular flight, and will be able to check that the information is correct, namely this name and surname is registered to board the very flight that is sitting at her back, behind the gate.

Finally, if everything is successful, the attendant will tell you go through, or else stop for further scrutiny. A few observations can be made. Check A and B could be swapped, you could first check the passport and then match it to the face. Check C and D can be equally swapped, but I guess the crucial check is check C, because authentication here is based on the passport and authorization is based on the boarding card. Therefore, the attendant needs to make sure that the same person she's authenticating is also authorized to board the flight.

I guess this is an important security protocol for the simple fact that boarding a flight is a security-sensitive service, and particularly security-sensitive perhaps nowadays. The question I was asking myself: is it secure? Does it work in practice? We would call it a human scale protocol, because it involves a lot of human checks and so on and so forth. Humans may make mistakes, so I wouldn't call this 100% secure, at least for what we read from the news, that a passenger taking off from Stansted ended up being in Sweden rather than in France as he would have wanted. Then he complained with Ryanair that he really wanted to go to France.

Is this an attack? Perhaps not, but we can see the same scenario as a threat, because you may imagine for example that I may like to buy a cheap ticket to fly somewhere, and then try to use the boarding card to go to a different place whose airfare was much more expensive. Or you may imagine that two

accomplices with two valid tickets and boarding cards pass security, and then they try to swap destinations at the gates. And I'm afraid we should also worry about other terrorism-based scenarios I can't see at the moment. I think this is an important issue, I think we need to look at this protocol with much criticism, and we really want to make sure it is secure. Now, let me recall that my main point originally was whether I can make this security defense more invisible to the user, but obviously I still want it to be effective.

Hugo Jonker: I've seen other stories about people who boarded the wrong plane, I've never seen a story about an attack in the sense that you described, so deliberately boarding the wrong plane. Do you have an example?

Reply: No, I don't, I was just conjecturing it, and well, perhaps there has been an attack where the attacker went unspotted. We don't know, I'm saying that if this is possible you may easily turn into a threat and open up new attack scenarios.

Hugo Jonker: I was wondering that because people made mistakes here, but that doesn't necessarily imply that you can count on those mistakes being made when you want them to be made.

Reply: Of course, but if this passenger didn't complain with Ryanair afterwards, and was happy to have gone to Sweden instead of France, then you would've called this an attack, but perhaps we wouldn't have known because he wouldn't have reported the issue.

Bruce Christianson: Indeed, if the person gets on the plane, and they're detected, "You're on the wrong flight!", then they're not going to say, "Oh, my attack has been foiled".

Reply: That's what I meant.

Bruce Christianson: "Oh, that's a good thing you spotted that." Almost by definition, there's going to be no example of a detected unsuccessful attack.

Reply: And who knows how many examples of undetected successful attacks there are. So, I think that this protocol can be simplified and made more invisible to the humans who have to go through it by using an electronic passport.

Hugo Jonker: You're looking at it from a very, I would say, European or like perspective. In India, my favorite example, they follow a completely different procedure, and with different goals. I don't believe in the simplification in the sense of simplifying overall the boarding card without fully considering what the protocols about the use of the boarding pass actually are.

Reply: I couldn't agree more, but in fact you'll probably agree with me that the main goal of the boarding card, or one of the main ones, is authorization. Here I'm precisely questioning this very goal, then I would ask you what other goals you are thinking about: memorizing, perhaps memorizing the seat number? But that's not a security goal as such.

Ross Anderson: Well, one would be reassuring the passenger. 25 years ago if you bought a plane ticket it was a fancy multi-part thing with red carbon paper, you went and checked in, you got a boarding card that was fancy. It had a mag stripe on this side, it had a tear-off bit and printing, it looked official, you were reassured you were holding something that might actually get you on the plane. Nowadays, you can dispense with your boarding card, you can have something on your mobile phone. I don't do that because I'm nervous that my mobile phone will run out of battery and I will end up being charged by Ryanair for an extra 45 quid to print another boarding card. I would say that a boarding card is actually pure security theater, whether or not you get on the plane depends on whether your name and passport number are entered against that flight number on the Amadeus computer at the end of the runway in Munich airport. If some jumbo crashes on takeoff, nobody's going to fly for months, and months, and months.

Reply: Yeah, I think I'm in line with that comment. I'm not saying that I want to dispose with this whole reassurance thing, you still have to go through check-in, for example, for the overbooking story and the like, but you might easily just get a printout to memorize the seat after you went through check-in. Here I'm only talking about the authorization goal as such.

Ross Anderson: Well, now you need seat numbers, three years ago Easyjet didn't, but now they give you seat numbers so they can charge you an extra 13 pounds.

Reply: Exactly.

Frank Stajano: In a previous slide you had something that said "20 years ago". In fact, 20 years ago what happened, especially in America with all these inside-the-US flights, so you basically bought a ticket and all that matters was someone paid for the ticket, and they can basically exchange, nobody would even check your name, all that mattered was the seat was paid for, that was pre-9/11, now after 9/11 there's all this business about security and this and that to which airlines latch on because it means that you cannot resell your ticket, you cannot give your ticket to someone else, they would have to buy a new one which is very neat for them because this trading of tickets of course can be useful. I don't know to what extent the fact that someone has had their name entered is any more authorization than the fact that they have paid, I don't know if they have how many background checks, or this guy was a terrorist before, or something like that, and I don't know how effective they are. One goal is just to extract more money by preventing the recirculation of tickets that have already been paid.

Reply: Yeah. I'm not trying to rule out the business considerations of course, so I agree with you. But what I'm saying is that from a security standpoint today, it is important to match the authentication with the authorization, the piece of information that authentication is based upon with the piece of information that authorization is based upon, at least because as you are saying, you want the same person who bought the tickets under their name to be the one who is flying.

Jonathan Anderson: I think that actually, from a security perspective, we don't care very much that the person who paid is the person who gets on board, but I think what we really care about is that the person who gets on board has been checked not to have any bombs, and that somebody paid for the seat, and that somebody is now sitting in the seat, and there is a mapping of no more than one person per seat. The other thing that airlines really care about is the penalty that they pay if they get to the other country, and then somebody gets turned back from the border, and they have to ship them back because they let someone on the airplane who shouldn't have been allowed on the plane because they didn't have their passport, or something silly like that. I think that, that pressure is the only reason. And even then it's not so much about matching the name on the passport to the boarding pass, it's just that this person has a passport that will let them into Austria, and they also have a boarding card that says somebody paid for the seat. I think the airline, except for all of the no-fly or whatever that the regulators impose, the airline doesn't actually care, and from a security perspective, I'm not sure it really matters.

Reply: Right, but still they do care because as Frank was saying, they want to make sure that who flies is precisely who bought the ticket under the name so that if this is not the case they may charge you. You can't just give your ticket to someone else because that's convenient.

Jonathan Anderson: Again, that's a business resale consideration.

Reply: I guess also a security consideration because as you said, they need to check that you have a valid passport, so they really want to check the person who's flying to have a valid passport. Perhaps they could do that without checking that name is the same name as the one printed on the ticket, so I concede that the current protocol aims at a mix of security and business goals.

Brian Kidney: That actually pre-supposes that requires a passport. To fly within Canada you do not actually need a photo ID, you can either have a government issued photo ID, or two other pieces of government issued ID, one of which has your address on it. An actual picture is not a requirement for flying within Canada. It's a little old man and he goes, "Well, do you have a license?" I know because my mother-in-law doesn't, so she doesn't actually have a government issued photo ID.

Reply: Right, so I'm not sure how they make sure that the ID really belongs to you.

Brian Kidney: They don't.

Reply: They don't, they don't care?

Brian Kidney: As long as the name and address matches the ticket, you can get on the plane.

Reply: So the identity is just attested there, it's not really linked to you as a physical person. I find that a bit surprising, and especially these days, in terms of both security and safety.

Bruce Christianson: It relies on the ID being hard to forge and the person holding it having an incentive not to let it out of their sight.

Hugo Jonker: It's also hard for a terrorist to enter the country on an in-country flight.

Ross Anderson: Well there's also the point that, as a practical matter, people cannot recognize a human person in front of them against a photo ID. There's a famous study on this by University of Westminster about 20 years ago, a double-blind study, half a dozen Sainsbury's checkout people, forty-odd students, each with and without photos, basically people cannot identify people from photos.

Reply: And that's why people can fly to the wrong destinations.

Bruce Christianson: The protocols that have been mentioned where you're getting stamped on your boarding card... the reason those stamps are going on your boarding card is because you already have a boarding card, it's convenient to do that. In other places, what they will do is give you a piece of plastic and say, "don't lose this or you're not getting on the plane", thereby aligning your incentives with theirs. The threat is an insider attack, the threat is someone in a position of trust with the airline smuggling a passenger on a plane.

Audience: They do that because it's convenient. Maybe a boarding card is not really needed for security today but to help people not to get lost because people get lost in the airport.

Reply: Are you sure?

Audience: I can imagine lots of people confusing their planes.

Reply: I can imagine the opposite scenario, I live in Sicily, which is quite far, at least it is far because to come here, you always need to go through Rome. For some time Alitalia decided that they would allow printout boarding cards, and you would have to have two sheets of paper, two sheets of boarding card literally for each single leg of flight. To go to Vienna I had to have four sheets of paper with me, then my mobile phone of course because we all want that, and the ID, and let me tell you, I didn't really like that. Now I have a QR code on my phone, I still have a boarding card literally speaking, but I'm much happier that way.

Audience: It may be much easier for operating the services of the aircraft if it's known that everybody has a piece of paper at the airport to help you find your plane and so on, you wouldn't get lost, and "I don't really know, which flight is it?" and people would need to go and query a database based on their IDs to find their flight. Having that, maybe, it is one of your cases, maybe it's easier to build security on top of that, providing that people already have their boarding cards.

Ross Anderson: There is another incentive to put the boarding card on the phone, which is that a big cost for airlines, it is that people are late at the gate. They're sitting in the bar, or they're sitting in the duty-free shop, and there's

always one sot who's ten minutes late and the plane misses its departure slot. Now, if everybody had to have their boarding card on the phone, you could send the heavy squad into the bar to fetch Mister Smith and drag him to the Stockholm flight. That would be a value-add for the airlines.

Jonathan Anderson: Well, that's assuming that the airlines don't *want* you to miss your flight so that they don't get dinged for overbooking.

Reply: I still only see two different types of passengers: a passenger who memorizes the flight details so he knows where to go, looks it up on the screen and finds out the gate, and that's it; and a passenger who doesn't. For the first passenger, I don't see the need of a boarding card, not even as a memo. And simply for the second passenger I see the need of a boarding card *merely* as a memo, but not for authorization purposes. In fact, this revision I'm presenting here of the boarding protocol tries to make sure that the passenger is both authenticated and authorized simply by means of, say, an electronic passport.

You see that checks B and C have been emptied completely, you see that what is scanned here is the electronic passport, and the resulting protocol is lighter, the security mechanisms are thinner. I would argue that this protocol's security is more invisible than the original protocol's. The question is, is it as effective as the original protocol? I guess so, in terms of authentication and authorization, and let me argue, perhaps it's even more secure than the original protocol, because the amount of human intervention here is reduced. You may even think that the passport has a scan of your fingerprint, and so you just go through even without a human attendant there, you just go through, scan your passport, scan your finger, and you would be let in or not. Doesn't it work like that to enter the UK if you have an electronic passport nowadays?

Ross Anderson: Yes, but it takes ten seconds, fifteen seconds at the gate.

Reply: Yes, but tomorrow it will take three seconds. The question is, would a human attendant take less than ten seconds? That was certainly not the case with my last flight.

Ross Anderson: Well, with people checking you in at the gate, it will typically take one or two seconds if they are rushing through a big queue. There's another reason why you may want a boarding card, which is when you are on top of the airplane steps, she has a quick look at your boarding card, and most of the time if you're trying to go to Dublin and the plane's for another city, she'll say, "Excuse me sir, you are on the wrong plane". Do you want to dispense with that entirely? Perhaps the occasional person will go to the wrong city. Perhaps civilization can survive that.

Reply: I'm arguing from a security/safety standpoint, I don't really like that.

Ross Anderson: Why? A terrorist on one plan blows up one plan instead of another plan, the same number of casualties, the same difference. Who cares whether it's a flight to Sweden or to Dublin?

Reply: Well, which plane it is may matter to me!

Brian Kidney: There's a question there as well about the actual security, because we use no-fly lists to keep people off planes that we don't actually want on there, but a big problem with the no-fly list is that there is no picture attached, and there are lots of people with the same name who don't have a piece of ID. I think that the protocol is thinner and more invisible, however I don't think that the original protocol is much more than security theatre.

Reply: All I'm saying is that if we have any passport, and we have the infrastructure, namely a database with the details of who's flying to that particular flight, all the stakeholders could be mechanized, and by merely authenticating yourself through your electronic passport, I guess that these various security problems of authentication of authorization could be solved.

Jonathan Anderson: However, one unique thing about the boarding card that's different from your ID, and that's different from your face, is that it is under the control of the airlines, that they can put whatever they want on it, and the atomic transaction involved from when you purchase the ticket to when you get on the plane, those two discrete events are bound by this boarding card, whereas, if I buy a flight three months in advance to save on the cost, and then I get a new passport, I have to renew my passport in the meantime, I go and look and say, "Oh, my passport's expired" after I buy the flight. Well then, what happened in this protocol, if you are authenticating just the name, well that's not really more secure, however you need a strong binding between the passport itself, and getting on the flight, well then, we need an additional protocol for me to transfer my ticket from my old passport to my new passport, and I think that is where the vulnerabilities are likely to lie in the new protocol.

Reply: It looks like I haven't got time to give you a full answer, but let me just say that Ryanair asked me the details of my passport *when* I purchased my ticket to Pisa. Isn't that more problematic than having my revised protocol in place? I believe so.

Jonathan Anderson: Not all airlines do that though. We should not substitute "Ryanair" for "an airline"! [laughter].

Reply: True, no, but logically the claim I'm making here is that the problems that you fear my protocol would be introducing are already in place at least for one airline that is very popular.