I've stolen from someone's Festival Card

Originally published in Hungarian by leading Hungarian news portal Index.hu
08/14/2012 12:01 by Gábor Stöckert

An IT company found a security vulnerability in Metapay's Festival Card[1] system. By the [opening of the] Sziget [Festival], operators had achieved considerable security improvements, but we've still managed to break the system and found the way to cheat money from each other. Metapay has no knowledge of such an incident happening in real life.

At one of the festival's wine booths, the guest paying before me is *Pozsi*[2], a living legend. He has seen every day of every Sziget since 1993; if anyone, it's him who knows every trick and trap at the Hajógyári[3]. Nearly all tricks, that is, because he is holding his Festival Card in a way that I can easily take a snapshot of its number from behind. He doesn't even notice. If I wanted to, I could now steal Pozsi's riches intended to be spent on wine with coke, since there is a security glitch in the Festival Card system.

Enjoy other people's cards

Since last year, the Metapay Festival Card has been the official[4] means of cashless payment at four festivals [in Hungary]: Gourmet, Volt, Balaton Sound and Sziget. This means that the security flaw has been present in the system for over a year. How is it possible that it was discovered by an expert of an IT security analyst company, SEARCH-LAB, at this year's Volt [Festival]? It drew his attention that the only data required for card registration was the card number. Thinking further, he realized how one could use other people's cards to drink 3-euro glasses of brandy and 2-euro glasses of wine, or how could one even take all the money from someone's card. In addition, the glitch in the system doesn't stem from technology but rather from organization, meaning that one doesn't need any special expert knowledge to exploit it.

Now that there won't be any more events this year where the flaw could be exploited, we'll disclose the know-how. Card registration is not mandatory. However, if a card gets lost, its owner can block it or recover the balance on it only if it was registered. The only thing you need for a successful cheat is to get a card number that hasn't been registered. As we could see in Pozsi's case, this is quite easy. You don't even need to take a picture. You could just memorize the number of the card of the person, who is paying before you. Or you could use some excuse to ask for the other guest's card "to check something on it". At this year's Balaton Sound [Festival], it was even enough to pick up a receipt slip issued upon card (re)charge that most visitors threw away, since the slip was printed with the card number on it.

Once having obtained an unregistered card number, the crook registers it by sending a text message or on Metapay's home page. They don't need to hold the card itself to do so; it's enough to know its number. They are also asked to provide an e-mail address and a cell phone number. But as it's very easy to register a new e-mail account, and, in Hungary, you can start a cell phone service by just telling your data (without having to present any official documents), a card can be registered without leaving a single trace to the crook's identity.

[1] In Hungarian: Fesztiválkártya [festivʌ:lkʌ:rtiə]
[2] [poʒi]
[3] Hajógyári [həiodiʌ:ri], named after a famous shipyard on its shores, is the island in the Danube that is home to the Sziget Festival. Sziget [sigɛt], means "island" in Hungarian.
[4] And also mandatory

Then the crook blocks the card, and goes to Metapay's customer service desk at the festival to declare that the card has been lost. After answering a few questions, the crook will get a new card with the other one's balance, ready to be spent or to be recovered in cash at a charging booth. The only thing the original card's owner will notice is that their card doesn't work anymore.

Hole in the shield

At this year's Balaton Sound [Festival], SEARCH-LAB proved that the method described above works. Of course, they used their own cards rather than those of unknown visitors, and documented the process. During the event, they notified the operator of the Metapay Festival Card, Meta-MPI Financial Information Technology Ltd., and, after Balaton Sound, they started talks with the company. "We pointed out that the main issue is that a card can be registered without actually holding it, so [first of all] this should be fended off in some reassuring way. We suggested to print a code on the charge receipt slip that should be required for registration. At the same time, irrespective of this solution, the card number should be partly hidden on the slip. In this way, neither the card number, nor the slip in itself would contain enough information to register the card", explains *Kristóf Kerényi,* an expert of the company highlighting the problem.

Metapay took the advice and added a further security measure that made it easier to identify the swindler if, despite reinforced security, an incident occurs. "We've made some changes in helpdesk processes that enabled us to remedy problems in a more precise way. Before issuing a replacement card, we ask for personal information and an id", says *Gábor Lévai,* the CEO of Meta-MPI Financial Information Technology Ltd. Indeed, a new clause has been added to the Terms and Conditions of using the Festival Card on metapay.hu: "Lost cards can be replaced at a Helpdesk point in person, by presenting a personal identification document (id, passport), after the card was blocked."

As we wanted to check if, by these measures, the security hole got plugged, we, too, tried to cheat at Sziget. Using the above method, I tried to steal from my colleague *Zoltán Szabó* (rather than from Pozsi – he is a legend, after all). I succeeded, and it wasn't even difficult, despite the fact that Metapay had apparently tightened the security in its system.

A mandatory code that is not mandatory

Indeed, for example, part of the card number was replaced by asterisks on charge receipt slips which also contain a registration code. The code was indeed mandatory for text message registration. On Metapay's site, however, the security hole remained unplugged. I could register with Zoltán Szabó's card number without entering a registration code, though it was indicated as a required field in the form. Then I tried to block Zoltán's card by texting, but that attempt failed. Therefore, I walked to the helpdesk where I had the card blocked. This went quite smoothly, and, in thirty minutes I could pick up my new card to replace the old, "lost" one, with my colleague's money on it.

The questions mentioned above resulted easy to answer. At the helpdesk, I had to know the approximate card balance (that I could see when Zoltán paid before me) and where I used it (same thing). Then, I had to provide the data used for registration (which I had invented myself). I also had to provide an id number, just by telling it. I didn't have to actually present an id, they believed me whatever I said my passport number was.

Then the Cheated Cardholder (starring: Zoltán Szabó) presented himself at the helpdesk, telling them that suddenly his card had stopped working. The lady at the helpdesk was convinced that what had happened could only be an accidental card swap. She came up with a surprising solution: she gave

Zoltán my phone number. Imagine the situation when a card's real owner is calling the crook: "listen, would you please return my money?".

Few register

Thus, even during Sziget, the security hole persisted in the payment system – that is advertised, among others, as secure and which won an innovation prize in Hungary. It should be added that the method described can't be used to steal millions. Of course, it could be very painful to lose a balance that was supposed to last for a whole week, but, according to Mr. Lévai, this has never happened, and none of the festivals have seen a real-life incident. At Sziget, the introduction of the registration code greatly improved security, since, though the site let us pass without providing it, 99.8% of those who register do so by texting, where the code is mandatory, Mr. Lévai said.

Zoltán Szabó's bad luck indicates that, though it's not mandatory, it's worth registering the card. In this way, a lot of problems can be prevented. Still, very few register. At least a non-representative survey carried out among our colleagues at Index led to disappointing results. Pozsi, along with 17 others, didn't register. Only 3 did so, while one of our colleagues said that he hadn't registered because he had gone to the festival for a single day, but would certainly have registered, had he gone for the whole week.

Metapay didn't have too much time between the two events to develop the system, which may have been one of the reasons why they couldn't fix the security issue completely. Next year, however, just as security professionals, we'll also keep an eye on what further steps Mr. Lévai and his team will take. According to the CEO, there will be important security enhancements. For example, this year Metapay has already tested the wristband version of the payment card. This would be a solution for the problem of lost cards, since the payment device (that is also the means of entry to the festival) would be worn on the guest's wrist. It could only be taken away by cutting the band – something that even Pozsi would notice.