Latvian student found a security hole in Estonian bank links

September 27, 2012 04:30

Hans Lõugas
Eesti Päevaleht

It is possible to assume false identity even when logging into mobile operator self-service environment. Authentication via online bank has not been regulated and security is lacking in almost all online services. According to banks, e-service providers are to be blamed, but still the former have decided to assemble a Banking Association workgroup.

Arnis Paršovs
Foto: Lauri Kulpsoo

Just last week Freedom House declared Estonia to be the country with the freest internet where a large number of people use the internet for their daily actions. It is true that almost every respectful enterprise in Estonia offers the possibility to use their services online. Estonians can obtain call statements in online mobile operators' self-service environments, purchase insurance, pay for utilities, purchase bus tickets or parking operators' parking permits. For all these one must identify themselves on the internet which is safest using an ID-card. What if you have forgotten the passwords, lost the ID-card reader or, as it often happens, the software malfunctions?

All the service providers listed above allow authentication via an online bank using a password card or PIN-calculator. The young Latvian computer scientist Arnis Paršovs refers to this method in his master's thesis as "highly unsafe in reality".

For example, a citizen would like to log in on AS Ühisteenused parking site parkimine.ee to check whether their parking permit is valid or they have to pay a fine. They choose Swedbank bank link for authentication where they enter their user name, password or a PIN-calculator code.

The risk arises in the next step: an ordinary user reaches again the site parkimine.ee after having completed the authentication process in Swedbank, whereas an attacker with bad intentions may skip the whole bank authentication process and access the parking site directly.

Personal data one click away

In order to find evidence for his thesis, Paršovs made videos where he impersonates such an attacker. The method portrayed in the video will seem terrifyingly simple to a technically competent viewer. Paršovs shows how he is without bank authentication suddenly logged in on Credit Register site E-safe, Elisa and Tele2 self-service centres, paperless Estonian Motor Vehicle Registration Centre, pilet.ee site, Ühisteenused parkimine.ee environment.

The largest security hole was discovered in parkimine.ee: in the video, Paršovs exchanges his personal identification code for his fellow scientist's one and gains access to the parking site with their identity. The other citizen's address in the population register is a few clicks away....

The flaw can be attributed to the fact that service providers trust bank link data too much. In theory, a person's information authenticated via a bank link should be checked thoroughly, and made sure that it is not expired and that the person used the bank link authentication for this particular merchant. At the moment, personal information authenticated via a bank link may be used with all merchants, often also days or weeks later after the person used the authentication.

Paršovs who graduated from Tartu University and Tallinn University of Technology cybersecurity joint curriculum in summer, notified Estonian CERT of his findings. CERT, which works with Estonian Information System's Authority and identifies and solves security incidents in Estonian computer networks, corroborated that the security holes discovered by the Latvian student are genuine.

"Paršovs describes real vulnerabilities and problems of authentication protocol," confirmed Toomas Lepik, an information security expert of Estonian Information System's Authority. "The video is like a textbook for a programmer on what should be done differently and be checked."

Lepik said that if the weaknesses described in the thesis accumulate and combine with other programming flaws, it may create a security hole on a webpage, as it already has happened with several Estonian websites. CERT which has said that national services (for example eesti.ee) are absolutely secure, notified technical staff in banks asking them to notify their partners who use such authentication service.

Users prefer banks

Although such a security hole could be avoided when using an ID-card, most people still prefer to log in to e-services via bank links. For instance, according to the statistics of the national portal eesti.ee (which does not contain this security flaw), 60 % of log-ins are done via bank links, 37 % using ID-cards and 3 % with Mobile-ID.

According to Paršovs, the security hole on parkimine.ee is just a simple example of taking on a stranger's identity. "Another security risk exists. It is more difficult to understand this one, but I have tried it out," he said. This is the possibility for an e-service provider to steal unhindered its clients' identities and use these for other services by impersonating a stranger. The reason is that [once personal information has been authenticated using a bank link] it does not have a notation of which service provider it is meant for. Thus, when someone has acquired authentication, they can become a user in all other environments" explained Paršovs.

A possible scenario is forcing access to a website where a criminal will find data that allow them to impersonate the clients of this site. Whereas Paršovs used a truly spiteful service provider as an example of security risk who takes advantage of unsafe authentication of a person. "Most people shrug and say that this is such a theoretical possibility – but as no one checks the authentication methods of banks, these are serious risks."

But let us not forget that the security hole that Paršovs discovered pertains to stealing another person's identity or impersonating them with merchants or service providers, but not to bank transactions or logging

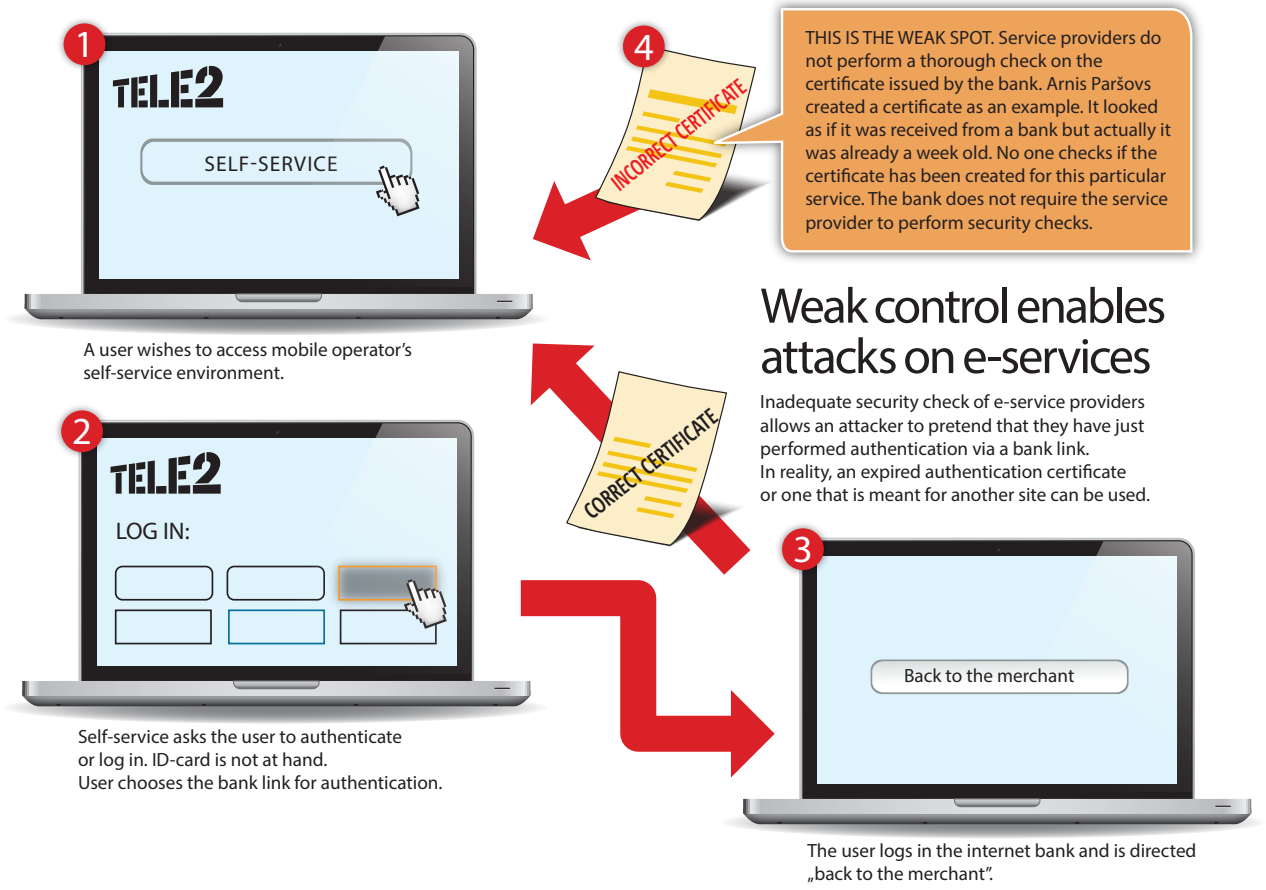
in to online banks. However, banks could eliminate the security risk by demanding that service providers perform checks more frequently.

Banking Association takes action

According to Estonian Information System's Authority, the e-service provides who have a negligent attitude to bank authentication are to blame here. "The described weaknesses are the problem of webpages that use bank authentication and the responsibility of the careless site owner," said Toomas Lepik from Estonian Information System's Authority.

The largest banks corroborate this. "The threats described in the thesis do not result mainly from an unsafe Swedbank link, but the merchant's possible weak implementation of the link," observed Arno Pae, the Head of E-Channels Department at Swedbank. According to Silver Vohu, the Communication Manager at SEB, a Banking Association working group has been assembled in order to solve "the arisen issue". "A solution has been found and technically speaking, it is not very complicated, whereas it requires all service providers to make changes in their systems, and therefore the implementation of the solution takes time," said Vohu.

According to Paršovs, the importance of the discovered security holes will be downplayed. "All parties claim that these threats are hypothetical and not feasible in reality," he said. "It is clear that if banks should improve their authentication of persons, it would require banks to undertake tremendous programming work and the same applies also to each e-service provider. Authentication of persons in online banks has never been audited [in Estonia] and only one foreign student had the idea to study how one of the most widespread methods has been created".



Used with permission of Eesti Päevaleht

Websites which contained higher or lower security risks

Banks:

- Krediidipank
- Nordea
- Sampo
- SEB
- Swedbank

Environments:

- arved.ee
- arvekeskus.ee
- compensalife.ee
- eesti.ee
- elion.ee
- elisa.ee
- emta.ee
- emt.ee
- energia.ee
- eparkimine.ee
- e-register.ee
- ergo.ee
- e-seif.ee
- ettevotjaportaal.rik.ee
- g4s.ee
- gaas.ee
- iizi.net
- kindlustus.ee
- kinnistusraamat.rik.ee
- korteriyhistu.net
- lkf.ee
- mandatumlife.ee
- paberivaba.ark.ee
- parkimine.ee
- partnercard.net
- pensionikeskus.ee
- pilet.ee
- stat.ee
- stv.ee
- tallinnavesi.ee
- tallinn.ee
- tele2.ee

Supervisor: the hole may have been neglected for years

Peeter Laud

Director of Research at Information Security Research Institute, PhD

In his thesis, Arnis has drawn attention to several weak spots. One of them is the classical man-in-the-middle attack: when user U contacts service provider S who happens to have bad intentions, then S may log in to some other service provider and pose as U.

The second issue is the expiration of authentication notifications sent to service providers by banks. As in some protocols these notifications do not have "best before" periods, it might be possible to use an expired authentication notification to log in. This is not really a weakness, but in case of some more complicated attacks (should the user not have complete control of their computer) it might be applied.

The third issue is protocol implementation flaws with service providers. Some signature verification or other check may have not been performed.

All these flaws are serious. Whereas fixing these is not complicated as the ecosystem is small – fewer than ten banks and tens of service providers. New version of protocol must be applied and necessary controls introduced in implementations. Coordinated action should not be impossible among such a small number of players. This will of course not guarantee that new flaws cannot exist. This is more a question of education.

I believe that scientists have not taken a personal interest in studying the security of authentication via Estonian bank links before. Scientifically speaking, we are dealing with protocols which do/achieve "boring" things as opposed to Mobile-ID. In this sense it is very good that cybersecurity has brought to us students who are interested in such issues.

It is possible that such a hole may have been neglected over the years. I think there are two reasons. One of these is the fact that the mentioned ecosystem is so small: it should be possible to keep an eye on each other and have an idea whether some service provider has bad

intentions. The second reason is that authentication via bank links has been a method without future for the past 10 years as the primary authentication device is the ID-card.

What is the problem?
Authentication via bank links is an activity that is technically as well as legally unregulated. If one merchant decides to offer its clients the possibility to authenticate online via a bank link, no one will check if this is safe for the client. Banks assume that the merchant who is their partner performs all checks to avoid client identity being stolen. A merchant expects a bank to provide full service. The client loses.

Arnis Paršovs says that such authentication via bank links should quickly be made impossible. "I strongly support the ID-card as a more secure method has not been created yet".

Hence do not log in to a service providers site using a bank link, but if possible, perform the authentication using the ID-card and you will have done everything that is possible to protect your personal information.

Master's thesis made a bank in Latvia improve its systems
Arnis Paršovs' master's thesis indicated a security risk in Estonian as well as Latvian bank and e-service systems. In addition, Latvian national computer security unit CERT confirmed in Latvian TV3 programme *Nothing personal* that Paršovs' analysis is well-founded and the threat is real. The analysis highlighted that the means of authentication were least checked in Swedbank and Citadele banks in Latvia. At the beginning of September, spokesperson for Citadele bank said to TV3 in Latvia that although the means of authentication is not really unsafe, they have begun improving it and this should be completed in a month. Latvian Swedbank said in the programme that the flaw is theoretical and unlikely to occur in real life.

In Latvia where the use of ID-card on the internet is not so widespread yet, most e-services offer the possibility of authentication via bank links. The representatives of public and private e-services who commented on the programme did not hasten to fix the systems, but expected the banks to show initiative.