I s hloupým čipem lze hrát chytré divadlo

Václav Šamša

vsamsa@tdp.cz

Proč se zabýváme hloupým čipem?

- Přišel zákazník a chtěl, abychom se o to pokusili (je v sále …)
- Jsme mu za to vděční, protože to byl a je úžasný nápad
- První aplikaci s chytrými čipy jsme udělali v roce 2002 pro Komoditní Burzu Kladno, kde se poprvé kotovaly ceny elektřiny v ČR
- Takže se nestydíme za to, že se zabýváme i hloupými čipy ☺
- Pracujeme pro zákazníky, kteří nevybírají daně ani bankovní poplatky a zajímá je poměr cena /výkon

Čím se vlastně zabýváme?

- Autentizací uživatelů v lokálním prostředí
- Aplikační důvěrou – jak dlouho může konkrétní systém věřit, že před obrazovkou se nachází stále ten, který se na začátku pracovní doby autentizoval?
- Chováním a motivací uživatelů - tedy efektivitou a pohodlím – náš zákazník chtěl a chce, aby “to” bylo bezpečnější a zároveň jednodušší a pohodlnější – a to dva přídavné zámky na dveřích do domu nejsou

Hloupý čip z našeho pohledu

- Unikátní ID
- Bezkontaktní
- Nízká cena čipu i čtečky, obrovské množsví variant
- Masivní rozšíření pro velmi mnoho uživatelských aplikací: vjezdy, vstupy, docházkové systémy, tisk/kopírování, stravování (objednání/vyzvednutí), interní kreditní systémy
- Vysoká unifikace – dostupné čtečky zvládnou většinu typů čipů

Chytrý čip z našeho pohledu

- Podepisování
- Paměť
- Chráněn PIN (heslem)
- Unikátní ID
- Kontaktní/bezkontaktní
- Vyšší cena čipu a bezkontaktní čtečky
- Kontaktní čtečka levná – cena podle počtu vložení

Chytrý čip z našeho pohledu

- Aplikace – podepisování, podepisování a podepisování
- Využití ID jako u hloupých čipů – ovšem omezeno cenou a variabilitou čteček
- Není problém na chytrém čipu postavit disertační práci ☺

Bezpečnost

- Asi všichni v tomto sále a mnoho dalších ví, že hloupé čipy nejsou bezpečné
- Zkopírovat je může ten, komu je půjčíte a pak váš nepřítel - správce
- Přesto lze i ve finančních institucích vstoupit do serverovny s hloupým čipem nebo jen s ID chytrého čipu
- Kdo by také u čtečky na dveřích zadával PIN a čekal a čekal …
- I když i to se v praxi děje, abychom byli upřímní

Bezpečnost

- Čip je bezpečný, pokud dokážeme motivovat uživatele, aby ho nikomu nepůjčoval, nenechával ve čtečce apod
- To lze docílit jen tak, že s čipem bude spojena nějaká aplikace, kterou uživatel považuje za významnou
- Autentizace to není. Bohužel. A to ani do registru vozidel na služebně městské policie s kartou s kvalifikovaným podpisem

Motivace

- Důležitá aplikace je možnost vrátit se z toalety do kanceláře a samozřejmě vyzvednutí oběda a kredit na kávu a na kopírku
- V žádné zemi na světě (ověřeno) si uživatel nedovede představit, že by si “na něj” někdo dal kávu
- Při jednání kdekoliv se podívejte, co si lidé u stolu položí před sebe. To je důležité. Bývá to hloupá karta a mobilní telefon. Nebývá to občanský průkaz ani když má chytrý čip. Platí i v USA.

Autentizace

- Pro autentizaci není hloupý čip sám o sobě dostatečně bezpečný
- Tak jsme ho spojili s přihlášením do adresáře (eDIR, AD ..)
- Uživatel musí prokázat, že má předmět a že zná heslo účtu, ke kterému je předmět přiřazen
- Útočníkovi nestačí znát jen heslo nebo mít jen čip. Musí mít oboje. Na tom není nic objevného. Až na to, že to umíme s hloupým čipem.

Prostředí Microsoft a MicroFocus

- Do obou prostředí se ze přihlásit s chytrým čipem.
- NMAS je lepší ale to neznamená, že MS nefunguje
- Pokud se uživatel přihlásí do domény nebo k eDIR, převezmeme jeho identitu a zkontrolujeme, zda přikládá svůj čip
- Čip hraje stejnou roli jako na předchozím slide
- Věříme, že fakt, že je uživatel autentizován znamená, že použil své, dostatečně bezpečné, heslo

Popelka - odhlášení

- Odhlašování je pro bezpečnost více kritické než samo přihlášení
- Protože většina útočníků jsou vaši kolegové
- Kolega - útočník si může sednout k vašemu počítači když odejdete na oběd, schůzku, cigaretu nebo toaletu
- Ovládejte odhlašování předmětem
- Odejdu s hloupým čipem, zamkne se mi počítač a mnou používané systémy dostanou notifikaci

Popelka - odhlášení

- Pozor na to, že dnes se uživatelé neodhlašují. Oni to prostě vypnou, uspí, zavřou apod
- Odhlašování, kterého se má účastnit třeba browser uživatele, je pak na nic. Úplně.
- Ale může to zvládnout server, který zjistí, co uživatel udělal
- Jen to musí používané informační systémy podporovat

Informační systémy

- Většinou ignorují informace, které mohou od prostředí (IdP) získat
- Neřeší jak, kdy a na jakém zařízení se uživatel autentizoval, stačí jim, že dostanou ticket s jeho identitou. To usnadňuje útoky. Velmi. A snižuje efektivitu investice do chytrých čipů.
- V mnoha případech podporují jen jméno a heslo a nebrání se použití různých „Credential managers“

Praktická ukázka

- Nemocniční prostředí (a mnohá jiná) nezapadá do konceptu Microsoft, ve kterém má každý “svůj” počítač, ráno se přihlásí a večer se odhlásí (pokud)
- Uživatelé přecházejí z pracoviště na pracoviště, střídají se u jednoho počítače a absolvují až desítky autentizací za směnu
- Rychlost a efektivita autentizace a způsob odhlášení jsou zcela kritické

Q & A

Václav Šamša

TDP sro

vsamsa@tdp.cz