Zdroj: http://ceskavedadosveta.cz/vedci-z-muni-nasli-dalsi-problem-v-cipech-tyka-se-elektronickych-podpisu/

Vědci z MUNI našli další problém v čipech. Týká se elektronických podpisů

Informatici z Masarykovy univerzity přišli před časem na zranitelnost, kvůli které se muselo měnit mimo jiné zabezpečení čipů slovenských občanských průkazů. Teď přišli na další slabé místo, které se uplatňuje především při elektronickém podepisování. Jejich objev znovu dokazuje, jak důležitá je důsledná analýza bezpečnostních systémů.

Při zabezpečení elektronických operací se v současnosti používají dva základní algoritmy asymetrické kryptografie – RSA a ECC. V případě prvního objevu informatiků z roku 2017 se chyba objevila v implementaci algoritmu RSA. U toho aktuálního pak v implementaci toho druhého, v současnosti široce používaného algoritmu ECC. Objev se týká čipů s vysokou bezpečnostní certifikací i několika široce používaných softwarových knihoven, které využívají vývojáři z nejrůznějších koutů světa.

„Rámcově jde o to, že na matematické úrovni se oba zmíněné algoritmy považují za bezpečné. Potíž je v tom, že tento matematický algoritmus je potřeba i bezpečně naimplementovat v konkrétních systémech a právě při implementaci se chyby objevují," uvádí problém Petr Švenda, vedoucí týmu informatiků.

Spolu s kolegy se právě ze zmíněného důvodu dlouhodobě zabývají bezpečností čipových karet, které postupně testují a sledují je z různých úhlů.

Karty, na kterých jsou bezpečnostní klíče, fungují tak, že uživatel požádá o digitální podpis a ona mu ho bezpečnou formou vypočítá a poskytne. „Uživatel pošle požadavek a karta mu podpis za určitou krátkou dobu odešle zpět. V tomto našem konkrétním případě ale problém spočíval v tom, že si kolega Ján Jančár všiml, že doba vydání podpisu je u různých požadavků různě dlouhá. Právě tato závislost dává určitou malou informaci, kterou lze při patřičném množství opakování využít k zisku celého tajného klíče," vysvětluje Švenda.

Podezřelé závislosti si Jančár, který je Švendův student, všiml v březnu. Červeným praporkem pro něj byla už jenom existence takové časové závislosti. Ve výsledku to ale ještě nemusí vždy znamenat problém. „Někdy můžeme později zjistit, že se ke zranitelnému místu nedokážeme dostat. Další úroveň je, že i když se k němu dostaneme, nemusíme najít cestu, jak zaútočit a tajný klíč získat. A když ji třeba i najdeme, můžeme zjistit, že útok je prakticky neproveditelný, protože vyžaduje například miliony pokusů a nelze jej provést v rozumném čase," naznačuje Jančár komplikovanost problému. V tomto případě ale nakonec bohužel pro výrobce všechno zmíněné možné bylo.

Jančárovi zabralo několik týdnů času, než přišel na způsob, jakým na slabinu zaútočit. Když pak vytvořil nástroj, kterým klíč získal, přišlo se na to, že napadení by útočníkovi zabralo jen dvacet minut a zvládl by to na běžném počítači.

Upozornění výrobce

Společně s dalším kolegou Vladimírem Sedláčkem zranitelnost dále analyzovali a poslali oznámení o problému výrobci karty a konkrétního čipu, který by měl zjednat nápravu. Do jaké míry se to skutečně stalo, je otázka. Původní výrobce karty už dnes totiž neexistuje a ani objevitelé sami netuší, kam všude se čip mohl dostat a používá se. Navíc vědí, že

v případě některých použití nebude možné problém vyřešit jinak než fyzickou výměnou čipu. Zveřejnili také nástroj, který umožňuje přítomnost zranitelnosti otestovat.

„Čip je certifikován pro použití americkými vládními institucemi a byl i certifikován pro použití v Evropě například pro klasický elektronický podpis pro úřady nebo různé přihlašování do systémů," naznačuje Švenda, který ale zároveň uklidňuje, že koncového uživatele se problém pravděpodobně masově nedotkne.

Zpráva pro komunitu vývojářů

Jedna část úkolu, který na sebe výzkumníci Fakulty informatiky MU vzali, bylo informovat výrobce čipových karet. Druhou částí bylo poslat zprávu do celého vývojářského světa, protože obdobný problém s implementací algoritmu našli i ve čtyřech kryptografických knihovnách. Vývojáři si z nich berou kousky hotových programů, aby je nemuseli dělat sami znovu a zbytečně opakovat chyby, které už někdo vyřešil.

„Pro představu, kdyby si člověk napsal program sám, může udělat chyb třeba padesát. Když použije knihovnu, bude tam chyb jen pár a časem jich bude ubývat. Proto se opravdu nedoporučuje dělat si v těchto případech vlastní řešení. Neznamená to ale, že sdílené řešení je dokonale bezpečné," říká Švenda a odkazuje tak na systémový problém, který se v oboru řeší.

Výzkum čipových karet, který s kolegy dělají, má proto mimo jiné za cíl šířit v oboru výzvu a praktické postupy, jak výrobu a testování čipů udělat víc otevřenou včetně transparentnějšího bezpečnostního testování. Aby bylo jasnější, na jaké problémy se produkty testovaly a kde by ještě mohly díry zůstat.

Autor: Martina Fojtů
Zdroj: MUNI
Úvodní foto: pixabay.com