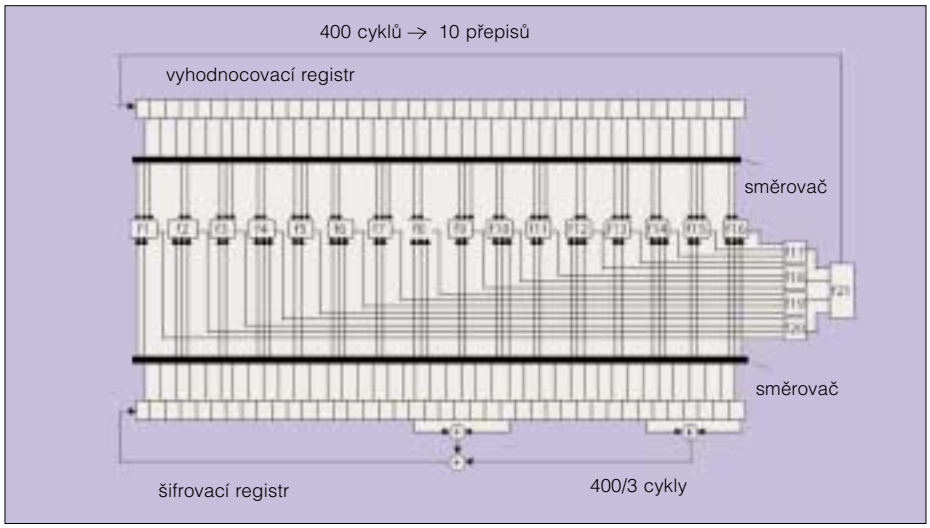
O bezpečnosti imobilizérů

Na jednom příkladu si ukážeme některé problémy doprovázející bezpečnost nejen imobilizérů, ale i obecných málo výkonných pasivních kryptografických předmětů. Sem patří zejména moduly, sloužící pro bezkontaktní rádiovou identifikaci (Radio-Frequency IDentification –RFID), které se napájí na principu elektromagnetické indukce, vyvolané zářením ze čtecího zařízení.



Obr. 1 Původní publikované schéma DST40 s chybami [1]

Tato malá bezdrátová zařízení jsou často založena na velmi levných a mechanicky odolných technologiích. Jejich velká budoucnost se očekává v identifikaci zboží, kdy budou působit jako čárové kódy za cenu 5 centů za kus. Kvalitativně vyšší jsou RFID, které zajišťují nejen identifikaci, ale i autentizaci (pojmy viz ST

Obr. 2 ExxonMobile a SpeedPass, oba s přiloženými vypreparovanými čipy

9/2004). Jeden z nejznámějších je Digital Signature Transponder od Texas Instruments (dále jen TIDST). Pro autentizaci by se hodily například standardní blokové šifry, ale ty jsou spolu s dalšími vhodnými kryptografickými funkcemi (HMAC) příliš složité pro realizaci v RFID. Výrobci se proto vydali cestou proprietárních šifer, které jsou jednodušší, avšak bohužel také slabší. Tuto nevýhodu se snaží vyrovnat tím, že popis použité techniky tají. To je známý princip „bezpečnosti pomocí zamlžení“ (security through obscurity), který se už mnohokrát nevyplatil. Vyplatil by se tehdy, pokud by existoval předpoklad, že se o danou techniku nebude nikdo zajímat. To však není případ imobilizérů. Používá se jich přes 150 miliónů a je jich celá škála od jednoduchých identifikátorů po kryptografické předměty. Zmíněný TIDST používají například letošní modely automobilů Ford. TIDST umožňuje také rychlé placení pohonných hmot, a to pouhým přiložením RFID na stojan, kde je platební terminál. Platí se tak i mýtné na dálnicích. Ukážeme si, jak byl tento modul prolomen týmem z Hopkinsovy univerzity a RSA (dále jen tým Hopkins-RSA) [3].

Autentizace

TIDST slouží k autentizaci vůči terminálu (čtečce), s níž sdílí svůj tajný klíč *Ks*. Čtečky nepoužívají *Ks*, ale odvozují si ho pro každý TIDST pomocí jeho identifikátoru a hlavního klíče. K autentizaci se používá proprietární symetrický kryptografický algoritmus „DST40“, který nebyl publikován. Z veřejně dostupných informací [1] a [2] byla známa pouze základní struktura algoritmu, do níž byly (úmyslně nebo neúmyslně) zaneseny chyby.

Autentizační protokol TIDST má následující fáze:
- TIDST vysílá 24 b identifikátor,
- čtečka vysílá 40 b náhodnou výzvu *C*,
- TIDST zašifruje výzvu *C* svým klíčem Ks, zkrátí výsledný šifrový text na 24 b a zašle jej čtečce (hodnota *R*) k ověření.

Pokud *R* odpovídá výzvě *C*, považuje čtečka TIDST za autentizovaný.

Publikované informace o DST40

Jádro DST40 je založeno na konečném automatu s lineární strukturou a vnitřní pamětí 80 b. Paměť je rozdělena na dvě části po 40 b. První je posuvný registr o 40 b (Input Register, *IR*), který se naplňuje výzvou *C*. Druhou částí je lineární posuvný registr se zpětnou vazbou (Linear Feedback Shift Register – *LFSR*), který se naplňuje klíčem *Ks*. Poté následuje 400 cyklů automatu (ve skutečnosti 200), během nichž je obsah registrů zpracován nelineárním filtrem s průběžným ukládáním výsledku do vstupního registru *IR*. Finální výsledek *R* pak tvoří 24 b registru *IR*.

Výsledky útoku na TIDST

Výsledkem zkoumání bezpečnosti TIDST týmem Hopkins-RSA je:
- odhalení přesného popisu algoritmu DST40, odlišného od publikovaných informací;
- odhalení základních bezpečnostních slabin algoritmu DST40;
- konstrukce lusticího zařízení;
- reálná ukázka útoku vyrobením kopie automobilového imobilizéru a nákupu benzínu.

Postup útoku na TIDST

Tým Hopkins-RSA použil pouze logické vstupy a výstupy TIDST a možnosti programovat jeho klíče. Na základě volby klíče *Ks* a vstupů (výzev *C*) potom analýzou výstupů *R* odvodili chybějící detaily schématu TIDST. Upozorněme, že zde může být i mnohem jednodušší cesta, jak získat popis algoritmu, a to reverzním inženýrstvím obslužného SW dodávaného výrobcem. Toto riziko se týká většiny transpondérů typu RFID. Nicméně fakt, že algoritmus šlo získat pouhou analýzou dat, sám o sobě dokládá míru rizika, a to i pro jiné systémy. Bylo zjištěno, že skutečný algoritmus se liší podstatným způsobem v časování, výstupu i vnitřním uspořádání schématu. Oproti veřejnému popisu:
- se některé bity výzvy *C* xorují na výstup;
- výstup není jednobitový, ale dvoubitový;
- vnitřní vedení bitů klíče a výzvy jsou odlišná od publikovaného schématu;

Obr. 3 Nákup benzínu pomocí duplikátu TIDST

– zpětná vazba do registru *R* není jeden bit, ale dva bity, apod.

Byl zjištěn neznámý obsah 21 logických funkcí (tzv. *f*-boxů), použitých v DST40 a identifikováno jaké bity registrů *IR* a *LFSR* vedou do jakých *f*-boxů. Dále bylo odhaleno zpracování klíče v *LFSR*. Ukázalo se, že vstupem do zpětné vazby jsou jiné bity, a že řízení registru s klíčem bylo jiné, než na publikovaném obrázku. Všechny tyto detaily byly nakonec rekonstruovány. Původní domněnka, že publikování nepřesných a zavádějících informací o schématu může zmást útočníka, se ukázala jako mylná. Naopak publikací některých detailů (jako je základní struktura schématu) se útoku velmi napomohlo.

Základní chyby

Poznamenejme, že všechny RFID musí mít z principu jednoduché schéma. Analytici využili faktu, že schéma umožňuje použít nulový klíč. Tento klíč pak eliminuje složitost části schématu, což urychluje jeho analýzu. Dále využili faktu, že klíč je možné libovolně volit a naprogramovat do TIDST prostřednictvím RF-příkazu. Metody, které použili, jsou obecně využitelné i pro jiná schémata, která jsou založená na posuvných registrech. K luštění klíče je zapotřebí zachytit pouze dva páry výzva-odpověď. Ty je možné získat například čtečkou, umístěnou v kapse obleku a přisednutím k člověku, který má svůj imobilizér v kapse.

Klíč *Ks* je určován vyzkoušením všech 2^{40} hodnot. Poté je možné zkonstruovat duplikát TIDST. I přes to, že 40 b je dnes považováno za absolutně nedostatečné, pro vyluštění 40bitového klíče *Ks* by bylo potřeba 10 PC po dobu 2 týdnů. Aby se tato doba zkrátila, byla tato úloha řešena paralelně pomocí programovatelných polí (FPGA). Za cenu asi 200 USD za materiál bylo pořízeno FPGA ověřující naráz paralelně 32 klíčů. Při taktování na frekvenci 100 MHz bylo možné celý 40bitový klíč najít za něco málo přes 10 hodin. S využitím 16 FPGA pak byly během 2 hodin zjištěny všechny klíče k pěti TIDST oficiální zapůjčenými firmou TI.

V analýze se pokračuje, a sice využitím Hellmanovy strategie typu time-memory trade-off. V tomto případě se využijí tabulky o velikosti 10 GB, které je nutno předem sestavit. Poté bude vyhledání správného klíče trvat na běžném PC asi jednu minutu. Samotný algoritmus TIDST však vykazuje slabosti, které mohou být využity k čistě kryptoanalytickému útoku, čímž by bylo možné dobu luštění podstatně zkrátit oproti útoku hrubou silou. Uvedené slabiny ukazují také okamžitý a jednoduchý návod k nápravě: nepoužívat „domácí samoděla“, ale kvalitní, odborně implementované standardy.

Závěr

DST40 je proprietární algoritmus z devadesátých let minulého století. 40bitový klíč je zcela nedostatečný, proto bezpečnost TIDST závisela pouze na utajení algoritmu. To je princip, který patří do historické kryptografie a opět se potvrdilo, že už není vhodné se jím řídit (podobný osud prodělaly původně neveřejné algoritmy A38 a A5/i v GSM, apod.). Připomeňme si, že základní ideu, tj. to, že útočníkovi je umožněna volná komunikace s „černou skříňkou“, jsme v roce 2003 využili k významnému útoku na protokol SSL [4]. Tehdy jsme pouze z hodnot výzvy a odpovědi od serveru SSL dokázali rozšifrovat jakoukoliv zachycenou komunikaci s tímto serverem, chráněnou protokolem SSL se silnými šiframi (RSA-1024, TripleDES-168). Navíc jsme od serveru nepotřebovali získávat žádná přesná data jako v případě TIDST, ale pouze chybové hlášení typu ano-ne. Útoky na špatně navržené černé skříňky, ať už pomocí postranních kanálů nebo přes jiné slabiny v jejich schématech, jsou v současné době nejefektivnějšími kryptoanalytickými útoky vůbec.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Kaiser U.: Universal immobilizer crypto engine. In 4th Conference on the Advanced Encryption Standard (AES), 2004. Guest presentation, http://www.aes4.org/english/events/aes4/program.html

[2] Gordon J., Kaiser U., Sabetti T.: A low cost transponder for high security vehicle immobilizers. In 29th ISATA Automotive Symposium, 3th–6th of June 1996

[3] Bono S., Green M., Stubblefield A., Juels A., Rubin A., Szydlo M.: Security Analysis of a Cryptographically-Enabled RFID Device, http://www.rfidanalysis.org/DSTbreak.pdf

[4] Klíma V., xPokorný V., Rosa T.: Attacking RSA-based Sessions in SSL/TLS, In Proc. of CHESS 2003, pp. 426–440, Springer-Verlag, 2003, http://eprint.iacr.org/2003/052.pdf

[5] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz

E-learning v praxi

Aktivní zvládnutí cizí řeči klasickým postupem v rozumné době a přiměřené kvalitě může být pro některé starší, ryze technicky orientované specialisty docela obtížný úkol. Co paměť historiků sahá, mnozí v dávné minulosti naivně očekávaly objev zázračného lektvaru (nebo funkčního norimberského trychtýře), který by donutil příslušná paměťová místa v lidském mozku udržet (a v případě potřeby zase vymazat) informaci po vzoru kdejaké polovodičové struktury. Protože však dosud bohužel nic takového objeveno nebylo, a pravděpodobně ani v budoucnu nebude, nejrozšířenější metodou učení stále zůstává memorování slovíček s procvičováním gramatických pravidel z učebnice, nejlépe pod dozorem rodilého mluvčího. Kvalitního učitele však dneska může s úspěchem nahradit počítač s příslušným programovým vybavením, jak svými úspěšnými produkty dokazuje např. firma LangMaster, která se tvorbou výukového software v nejširším měřítku zabývá už mnoho let.

K hlavním výhodám multimediálních internetových kurzů (nejen jazykových) patří z pohledu studujícího zejména možnost dokonalého přizpůsobení intenzity studia osobním potřebám, časovým rezervám a aktuálním schopnostem vstřebávat plynule rostoucí kvantum znalostí. Kromě toho vertebrální algoritmus kurzu (jehož základem je obvykle metoda Re-Wise) automaticky v zastoupení zkušeného pedagoga sleduje pokroky studenta, pamatuje si jeho slabší místa, a partie, v nichž opakovaně registruje chyby, procvičuje neúnavně s nepříjemnou důsledností naprogramovaného stroje. Biologická paměť v mozku člověka totiž vykazuje vlastnosti, které v technických systémech nelze tolerovat. Například, jak ostatně každý z nás ví z vlastní zkušenosti, i přes opakované pokusy o trvalé zapamatování konkrétní informace nelze u většiny jedinců garantovat, že při následném pokusu o její bezprostřední aktivaci bude ta pravá zpráva nalezena a zůstane nezkreslena. V delších časových intervalech může být dokonce obsah některých paměťových buněk trvale vymazán a nezávisle na vůli svého nositele navždy zapomenut, případně přepsán jinou, aktuálnější zprávou. Proto není důležité učit se jen to, co ještě mozek neuložil do dlouhodobé paměti, ale také včas a efektivně kontrolovat správný obsah zapamatované informace. Proces plnění dlouhodobé paměti obsahem s minimálním počtem opakování optimalizuje už zmiňovaná metoda Re-Wise, která vznikla ve spolupráci s odborníky zabývajícími se výzkumem učení a matematickým modelováním procesů zapamatování a zapomínání. V principu se využívá se toho, že časový interval, po který informaci v paměti udržíme, se opakováním prodlužuje. Další podrobnosti k formě i obsahu širokého výběru profesionálně sestavených jazykových kurzů lze zjistit na www.langmaster.cz.