RFID a kouzlo Vánoc

Budou to už bezmála dva roky, kdy jsme se demonstrací útoku postranním kanálem na MIFARE Classic v ST 8/2009 v tomto seriálu naposledy věnovali bezpečnosti RFID. Nadešel čas k tématu vrátit a reflektovat významné události, které se od té doby staly.

Legic Prime

Čipem, který to odnesl hned po MIFARE Classic (dále jen MFC), byl Legic Prime, který v té době používalo například hamburské letiště [3]. Deklarované schopnosti tohoto čipu zhruba odpovídají MFC. Jedná se o paměťovou kartu s údajně kryptograficky řízeným přístupem. Její účel je však mnohem těsněji spojen s přístupovými systémy, což se odráží i na množině podporovaných funkcí. Více detailů zde bohužel uvést nemůžeme, neboť téměř vše kolem této technologie je přísně střeženým firemním tajemstvím. Dlužno podotknout, že v tomto směru Legic zdaleka překonává ostatní výrobce, neboť kolem svých produktů vytváří bezmála „sektu“. Existuje několik úrovní „zasvěcení“, přičemž bez příslušného iniciačního rituálu není možné koupit ani obyčejnou čtečku. Není proto divu, že chuť analytiků podívat se tomuto čarovnému hrnci pod pokličku byla opravdu velká. Její úspěšné nadzvednutí byla předvedeno o Vánocích roku 2009 na tradičním hackerském kongresu CCC [2]. Nyní už je jasné, že v hrnci Legic Prime se místo chutného pokrmu škvířil pěkný blaf.

Podstatu útoků velmi trefně shrnuje už samotný název práce [2], který je – stejně jako čip samotný – parodií na okřídlené „security in depth“. Použitým algoritmům by spíš seděl název klamavý kód, neboť jedinou tajnou informací byl popis tohoto kódu – ve schématu totiž žádné explicitní tajné klíče nejsou ani zavedeny! Úroveň bezpečnosti je tak ještě níže než u MFC. Praktickou stránku rizika podtrhuje fakt, že rádiové rozhranní těchto čipů, které se Legic údajně pokoušel standardizovat jako ISO 14443 F, se podobá spíš tzv. kartám s vazbou na dálku dle ISO 15693, což vede na oficiálně slibovanou komunikační vzdálenost až cca 70 cm. Za uvedených okolností se ovšem nejedná o příjemnou provozní vlastnost, nýbrž o markantní zvýšení rizika krádeže identity.

Výrobce přirozeně rychle přispěchal s tvrzením, že čipy řady Prime jsou už „samozřejmě“ zastaralé a že doporučuje přejít na řadu Advant. Bohužel však i zde je striktně aplikován naznačený přístup vrcholné exkluzivity okořeněný haldou mlžících marketingových pojmů. Je proto otázkou, zda se nejedná jen o další uplatnění techniky „obskurnost až do morku kostí“.

HID iClass

Nadělovalo se i o loňských Vánocích na 27. ročníku CCC. Tam to dostal čip HID iClass [1], což má být bezpečný nástupce již dříve prolomeného HID Prox. Připomeňme, že útok na HID Prox jsme nezávisle našli a publikovali v našem seriálu v ST 9/2008. Dnes se z napadání tohoto čipu stal už téměř folklór, což dokazují například webové stránky [5]. Vraťme se však k řadě iClass, jejímž slabinám výzkumníci věnovali rovnou celé webové stránky [4]. Zde popsaný útok je zajímavý tím, že přísně vzato nenapadá čip samotný, nýbrž jeho klíčové hospodářství. Za cíl útoku je přitom trefně vybrán nejslabší článek řetězu, kterým momentálně je – čtečka!

V takzvaném standardním režimu je přístup do čipu iClass chráněn továrními klíči, které jsou přirozeně uloženy v každé čtečce. Tu lze na rozdíl od Legicu koupit celkem volně v internetovém obchodě, čímž samozřejmě nechceme nijak bránit strategii tutlání slabých algoritmů. Analytici se konkrétně zaměřili na typ RW400, ale sehnat se dají i jiné. Jádrem čtečky RW400 je zástupce všeobecně oblíbených mikrořadičů rodiny PIC, konkrétně PIC18F452. K ochraně klíčů iClass jsou použity běžné mechanizmy tohoto procesoru, který umí po jednotlivých blocích chránit svou paměť programu a dat proti čtení přes ladicí rozhraní. Záměrně jsme zvýraznili ochranu aplikovanou po individuálních segmentech, neboť ta je právě tím místem, kde pašáci (tedy ti, kdož nepotřebují nic znát a jdou rovnou tvrdě na věc) ošklivě narazili. Chráněnou paměť sice lze odblokovat jen za podmínky jejího smazání, avšak zároveň je zde možnost pracovat nezávisle s jednotlivými bloky. Bez jakýchkoliv útočných technik tak lze přes definované vnější rozhraní dosáhnout toho, že odblokovány a smazány budou jen určité segmenty, zatímco ostatní zůstanou v původním stavu.

Je zajímavé, a pro vývojáře jistě poučné, projít si celý postup útoku [1], kdy analytici u procesoru čtečky nejprve obětovali blok zavaděče, který naplnili vlastním kódem. Ten potom přes běžné sériové rozhraní ochotně odeslal obsah zbývajících, dosud zablokovaných paměťových segmentů. Paměť, jakkoliv chráněná před čtením z vnějšího prostředí, byla totiž stále dostupná pro čtení programem běžícím uvnitř mikrořadiče. Samotný blok původního zavaděče byl následně získán z druhé čtečky, kde byly vhodně obětovány jiné, nyní již známé bloky. Ve finále tak analytici získali naprosto kompletní obsah programové a datové paměti čtečky RW400.

Prvním úlovkem byly samozřejmě klíče pro tzv. standardní režim, jehož bezpečnost tím okamžikem padla. Správně by nyní mělo dojít ke změně klíčů, sotva se nějaká čtečka dostane – byť jen na chvíli – mimo kontrolu. To je pochopitelně absurdní představa.

Slovo pašákům

Z jistých kauz kolem MFC lze soudit, že i pašáci čtou náš seriál, což nás těší. Bohužel mu však ne vždy rozumí, což nás mrzí. V diskusích zazněla otázka, jak vůbec můžeme říct křivého slova, když jsme přeci MFC v ST 2/2007 tak pěkně pochválili. Snad jde o větu ze závěru: …Pomineme-li délku klíče, neveřejný algoritmus a prakticky neznámé prvky ochrany proti postranním kanálům, jsou karty MIFARE robustním, snadno uchopitelným a aplikovatelným prostředkem, který právem nalézá svá dobrá uplatnění v bezpečnostních systémech „běžné spotřeby“. Dovolujeme si tímto připomenout, že každé tvrzení má v logice svou premisu, která uvádí podmínky implikující důsledek. Možná to zbortilo něčí představy o světě, ale ve skutečnosti se nestalo nic jiného, než že premisa byla vyvrácena. Prostě bylo ukázáno, že tyto aspekty nadále pomíjet nelze. Kvalitu bezpečnosti přitom mimo jiné dokládá právě schopnost pružně reagovat i v takových situacích. Pašáci, kteří zaspali dobu, se už mohou jen vztekat. Avšak nikoliv na naše tvrzení, jehož formulace navíc přesně odhadla, kde jsou potenciální slabá místa. Jak bylo ukázáno v ST 8/2009, nejrazantnější útok kombinuje právě krátkou délku klíče se slabinami tutlaného algoritmu a chybovým postranním kanálem!

Závěr

Během uplynulých dvou let byla jedna technologie odepsána, druhá vážně nahlodána. Útok na HID iClass lze označit jako přelomový, neboť místo karty si bere primárně na paškál ochranné mechanizmy čtečky. Najevo tak vyšly i některé proprietární kryptografické algoritmy, na kterých se už začalo pracovat. Uvidíme, co přinesou letošní Vánoce.

Vlastimil Klíma, Tomáš Rosa,
vlastimil.klima@knzsro.cz, tomas.rosa@rb.cz

LITERATURA

[1] Meriac, M. and Plötz, H.: Analyzing a modern cryptographic RFID system, 27C3, December 2010.

[2] Nohl, K. and Plötz, H.: Legic Prime: Obscurity in Depth, 26C3, December 2009.

[3] http://www.h-online.com/security/news/item/Chip-based-ID-cards-pose-security-risk-at-airports-905662.html.

[4] http://www.openpcd.org/HID_iClass_demystified.

[5] http://www.proxclone.com.