

Červí díry v RFID

Výrazem *červí díra* označujeme v oblasti RFID každý postup umožňující nežádoucí komunikaci mezi terminálem (čtečkou) a transpondérem, který by za běžných okolností byl mimo aktivní dosah tohoto terminálu. Setkáme se také s pojmem přepojovací kanál, který označuje totéž, jen ve svém názvu více odráží technický *princip* realizace takového postupu. Bezpečnostní specialisté však v poslední době dávají přednost právě pojmu červí díra, který si pochopitelně pouze vypůjčili z teoretické fyziky. Snad je vhodné zdůraznit, že o konstrukci, dosud hypotetických, „zkratek“ v časoprostoru zde rozhodně neusilujeme. Alespoň prozatím. Nicméně pojem sám už jen svým názvem velmi dobře ilustruje často poněkud překvapivý *dopad* takového postupu, a to zejména právě na bezpečnost.

Pokud legitimní držitel jednoho či rovnou více důležitých transpondérů RFID vstoupí spolu s nimi do šikovně nastražené červí díry (tj. ocitne se v aktivním dosahu antény útočníka), potom může – ke svému nemalému úžasu – například vpustit útočníka do své kanceláře, bytu či garáže, zaplatit mu dobrý hotel a restauraci, nechat ho pracovat na svém počítačovém účtu, odjet svým autem nebo snad dokonce nechat projít hranice na „svůj“ pas. Vidíme, že to rozhodně není málo, a tak lze jistě prominout ten provokující název. Provokace je totiž s ohledem na riziko realizace takové červí díry bezesporu na místě.

Hlavní pozornost bude v přednášce věnována bezkontaktním smart kartám dle ISO 14443, které už začaly postupně nahrazovat klasické „kontaktní“ karty, přičemž jejich význam stále rychle roste. Spolu s ním roste pochopitelně i zájem akademiků a výrobců hledat a vyvíjet vhodné technologie a nástroje pro jejich podporu. Téměř každá technologie a technika se však dá nejen využít, ale i zneužít. Naznačené úsilí tak zároveň nevyhnutelně podporuje i útočníky – například právě v oblasti prakticky schůdné realizace červích děr. Za všechny zmiňme především platformu NFC (Near Field Communication), která umožňuje, zjednodušeně řečeno, aby se například mobilní telefon choval jednak jako čtečka, jednak i jako transpondér RFID. Dáme-li tuto novou pozoruhodnou schopnost telefonu dohromady s jeho přirozenou podporou přenosových kanálů GSM/UMTS, Bluetooth, Wi-Fi, atp., vyjde nám velice slušný základ pro robustní červí díru.

Z předchozího by snadno mohl vzniknout dojem, že je žádoucí, aby vývojové firmy poněkud přibrzdily a omezily svůj výrobní program. Dokonce se s tímto názorem v praxi skutečně setkáme, avšak z hlediska bezpečnosti je takový přístup naprosto pomýlený. Šlo by jen o další převlek všeobecně zprofanované bezpečnosti skrze obskurnost! Účinná opatření je nutné hledat zejména v návrhu bezkontaktních aplikací samotných. Například je záhodno revidovat zaběhnutý princip, podle kterého je již samotná přítomnost transpondéru v poli čtečky chápána jako postačující projev vůle legitimního držitele čipu vstoupit do nějaké místnosti, zaplatit oběd, nastartovat auto, atp. Dále je vhodné podporovat snahu kryptologů o hledání tzv. protokolů omezujících vzdálenost (distance bounding protocols), kteréžto úsilí je zatím vývojáři RFID přijímáno nanejvýš vlažně. Rozšíření stávajících schémat je přitom nevyhnutelné, má-li si kryptografie i zde udržet punc základního stavebního kamene bezpečnosti. Klasická schémata orientovaná na zajišťování důvěrnosti a integrity přenášených dat jsou totiž obecně zcela bezzubá proti červí díře, která nechce nic špehovat ani měnit – jen přenést data z jednoho konce na druhý a obráceně. Přednáška si klade za cíl upozornit i na tento aspekt a ukázat, že spolehlivá bezpečnostní opatření je opravdu nutné hledat jinde, než ve škrcení výroby radičů NFC a jim podobných obvodů. Jejich existence má naopak na bezpečnost RFID jednoznačně pozitivní dlouhodobý dopad, neboť nutí vývojáře aplikací brát existenci červích děr skutečně vážně.