**Penetrační testy RFID – aneb když pravda je horší než lež**

Penetrační testování je v oblasti informační bezpečnosti již notoricky známo coby technika umožňující simulovaným útokem prověřit reálnou odolnost konkrétní aplikace vůči napadení. V mnoha případech je to díky nedostatečné analytické, vývojové a provozní dokumentaci jediná cesta, jak se o bezpečnosti vybrané aplikace (například internetového obchodu) něco smysluplného dozvědět. V sesterské oblasti zvané fyzická bezpečnosti jsou počítačové obvody sice dnes už stejně důležité jako ocel, avšak penetrační testování se zde příliš nepoužívá. Na jednu stranu je fakt, že vůči testování bankovní pobočky rotou vojáků asi budou oprávněné výhrady, avšak proč se nezaměřit právě na zmíněné prvky IT? Jejich zranitelnosti jsou v zásadě stejné bez ohledu na místo a účel použití. Přednáška si klade za cíl předat praktické zkušenosti získané při penetračním testování přístupových systémů fyzické bezpečnosti založených na čipech RFID. Otázkou k prověření bylo, zda a za jakých podmínek lze vytvořením „falešné“ karty získat přístup do chráněných oblastí. Dodejme, že úspěšnost byla zatím, bohužel, stoprocentní.

Jakkoliv může téma radiofrekvenční identifikace (RFID – Radio Frequency IDentification) snad ještě někomu znít nově, jedná se o oblast nejméně tak starou, jako je radiofrekvenční lokalizace (RADAR – RAdio Detection And Ranging). Jakmile totiž nějaký objekt zaměříme, vzniká zcela přirozená potřeba jej také identifikovat. Připomeneme-li, že RADAR se hyperaktivně rozvíjí už od 2. světové války (existují například RADARy zaměřené na lokalizaci živých tvorů), lze si udělat hrubou představu, jak rozsáhlá je dnes také oblast RFID. S ohledem na tuto skutečnost musíme záběr přednášky razantně omezit jen na ty technologie, které se pro přístupové systémy používají nejčastěji. Zde se jedná o pasivní čipy s induktivní vazbou mezi čtecím zařízením (terminálem) a kartou pracující na frekvencích dlouhých až krátkých rádiových vln. Čipy nejsou vybaveny žádným autonomním zdrojem energie, jejich napájení probíhá přes vysokofrekvenční transformátorovou vazbu s terminálem. Tou samou cestou také probíhá obousměrná datová komunikace. Elementární principy tohoto mechanizmu budeme v úvodu přednášky rekapitulovat v rozsahu nutném pro pochopení dále popisovaných útoků.

Zastavme se ještě u nadpisu přednášky, který možná zní poněkud divně. Vzhledem k tomu ovšem, že techniky vysvětlené v prezentaci dokáží položit na lopatky drtivou většinu současných přístupových systémů na bázi RFID, nelze se v duchu nezeptat, zda je skutečně vhodné toto téma takto veřejně otevírat. Více či méně zjevně si tuto otázku kladli také všichni zlomení uživatelé zlomených aplikací, se kterými se autor měl tu čest setkat. Pokud by současná technologická základna neumožňovala dosáhnout řádově vyšší bezpečnosti, než jaká byla při testech prakticky zjištěna, pak by se nutně i sám autor nehledě na všechny své ideály musel klonit k názoru, že jakákoliv publikace je krajně nevhodná. Ale tak to není – nedávná a tím spíš i aktuální součástková základna totiž postavit několikanásobně bezpečnější aplikace umožňuje! Přitom nedochází ani k dramatickému navýšení ceny ani k neúnosnému zesložitění provozních postupů, jak se nám obchodníci často snaží namluvit. Vlastně jediné, co je skutečně třeba, je hned na začátku vědět, jaké vlastnosti nový systém mít rozhodně nemá. Toto je pak ještě v pilotní fázi vhodné prověřit alespoň základním penetračním testem. Ano ovšem, to vše se týká především nových systémů, neboť změna stávajících instalací je často díky jejich rozsáhlosti prakticky nemožná. A právě proto – v zájmu ušetření mnoha milionů korun vyhozených za neopravitelně špatně postavený přístupový systém – padlo rozhodnutí prezentovat techniky umožňující odhalit zásadní slabiny hned na začátku, často jen na základě poskytnutého vzorku přístupové karty.