Radiofrekvenční identifikace

Kočka s počítačovým virem

Rádiové visačky na zboží, rádiové čipy ve zvířatech. A nyní i první virus. Podívejme se, čím vším by nás technika RFID – kromě bolení hlavy – mohla v budoucnu obdařit.

Text: Manfred Flohr, *autor@chip.cz*

Označuje se jím skot, nosí jej v sobě psi a kočky: RFID čip. Jako elektronická „ušní známka“ užitkových zvířat střeží celou jejich životní pouť – či spíše „cestu masa“ – z odchovného zařízení až na jatka. Zaběhlá domácí zvířata lze díky čipu pod kůží identifikovat podle patnáctimístného rozpoznávacího čísla. Avšak praktickému využívání RFID také brání závažná bezpečnostní rizika.

Aby upozornili na potenciální nebezpečí, zvolili vědci z amsterdamské Vrije Universiteit jako demonstrační objekt obyčejnou domácí kočku. „Je vaše kočka infikována počítačovým virem?“ zněla pak otázka pracovní skupiny profesora Andrewa Tanenbauma při vědecké prezentaci. Badatelé z Computer Systems Group na ní předvedli, jak může RFID čip zaútočit na počítačovou databanku.

Teoreticky možný scénář napadení prostřednictvím kočky líčí Tanenbaum takto: Hacker zvířeti implantuje zmanipulovaný rádiový čip a přivede je ke zvěrolékaři. Identifikační systém v ordinaci se začne chovat podivně, neboť do centrální databanky se přenesou falešná data. O pár hodin později systém vymaže údaje z RFID čipů ve zvířatech. A nakonec přijde to nejzáhadnější: displej identifikačního systému zamrzne se zlověstnou zprávou „Všechna vaše zvířata patří nám!“.

Všeobecná důvěra vkládaná do RFID tagů (jak se těmto čipům také říká) není namístě, varují vědci kolem Tanenbauma. Doposud se vycházelo z toho, že útokem pomocí RFID je možné jenom zfalšovat data. „Ve skutečnosti však hackeři mohou napadnout databanku pomocí SQL Injektion nebo Buffer Overflow,“ tvrdí Tanenbaum. Touto cestou by virová programátoři mohli šířit i malware, viry a červy využívající RFID.

Ačkoliv možné bezpečnostní mezery nelze připsat k tíži rádiovým čipům, nýbrž programátorům databank, lobby RFID cítí ohrožení. Její zájmové sdružení AIM proto obratem zveřejnilo stanovisko pod titulem „Vaše kočka je bezpečná“. Argumentuje hlavně tím, že Tanenbaumova skupina vykonstruovala systém se slabým místem a jen tuto vestavěnou „Achillovu patu“ využila; RFID tagy používané pro zvířata by totiž nemělo být možné přepsat.

V tom má AIM pravdu. Ostatně Computer Systems Group v Amsterdamu se také ve svých studiích kočkou jako možným nositelem virů přestala zabývat. Místo toho se pro svůj vlastní test soustředila na scénář, v němž bude RFID napříště hrát ještě mnohem větší roli – simulovala počítač v budoucím samoobslužném obchodě.

Jak zanést virus do supermarketu

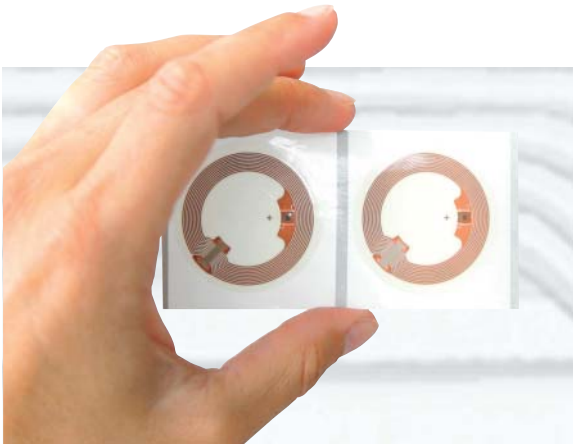
Není to tak složité. Útočník nejprve v obchodě zcela regulérně zakoupí zboží opatřené RFID tagem. Doma pak elektronickou etiketu vymění za jinou – „bianco“ tagy a vhodná zapisovací zařízení jsou komerčně dostupné. Teď stačí propašovat zboží zpět do obchodu – prodavačka u pokladny pak naskenuje falešnou etiketu. Ve svém testu zapsal Tanenbaum na čip tzv. „quine“ – program, který reprodukuje svůj vlastní zdrojový text. Cílem útoku byla databanka Oracle. ➔

MANIPULACE S RFID A JEJICH MOŽNÉ ÚČELY

	Špionáž	Podvody	Denial of Service	Ochrana soukromé sféry
Falšování obsahu		X		
Falšování identity: tag		X		
Deaktivace		X	X	X
Odlepení		X		X
Odposlech	X			
Blokování		X	X	X
Rušení		X	X	X
Falšování identity: čtečka	X			
Viry		X	X	

Blamáž: Bezpečnostní studie BSI sice uvádí přehled o možných nebezpečích při nasazení RFID čipů – poslední řádek tabulky ovšem chybí...

RFID při tankování: Bezhotovostní čerpání paliva s použitím radiofrekvenčních čipů.



Infikované: Do těchto čipů vložili vědci z Amsterdamu první RFID viry.

Zaregistrován: Metro Group v Neussu testuje RFID etikety pro supermarket budoucnosti.

Než budou pokladny v supermarketech skutečně načítat RFID tagy, ještě pár let uplyne. Obchodní řetězec Metro Group tuto techniku právě zkouší na úsecích logistiky zboží a zákaznického servisu. Předpokládá přitom, že ceny etiket během příštích cca deseti let poklesnou natolik, že je bude možné nalepit na každý obal. Kontejnery a palety nesou elektronické označení částečně už dnes – tu a tam dokonce s přepisovatelnými čipy.

„Bereme to opravdu velmi vážně," komentuje varování amsterdamských vědců Harald Kelter ze Spolkového úřadu pro bezpečnost v informační technice (BSI). O „RFID virech" však odmítá hovořit: „Jsou to obyčejné počítačové viry – také nemluvíme o ‚disketových' virech jen proto, že je škůdce zapsán na disketě." Scénář útoku prostřednictvím SQL Injektion není v podstatě nic nového, využívá jen dlouho známou bezpečnostní mezeru. „Nový je zde jenom přenosový kanál," říká Kelter.

Studie BSI nazvaná „Rizika a šance nasazení systémů RFID" prozrazuje, že bezpečnostní experti vůbec nevzali v úvahu virové napadení prostřednictvím RFID. Průzkum se detailně zaměřil na různé způsoby útoku (viz tabulka) – viry se mezi nimi však vůbec nevyskytují. „Tohle nebezpečí jsme při zpracovávání studie před téměř dvěma lety neuvážili," připouští Harald Kelter. Také laboratorní pokus s nechráněnou databankou vypadá hodně vykonstruovaně. „Na to nejsou tyto jednoduché etikety dostatečně komplexní," říká Kelter. Tím však téma RFID malwaru nezmizelo ze stolu. V Tanenbaumových testech každopádně sloužily RFID tagy jen jako „doručovatelé". Samotné zboží v supermarketu – a samozřejmě ani kočka – virem infikovány pochopitelně nebyly.

Neznámé riziko: RFID na šekových kartách

Napínavé by to mohlo být u jiných variant RFID, které šifrují data a přímo na čipu provádějí výpočty. Jako duální rozhraní jsou nasazovány například na „smartcards" s funkcí šekové karty nebo při vstupní kontrole osob. „Bylo by zajímavé vědět, zda nejen databanky, ale i RFID čipy samotné mohou být napadeny," přemítá Kelter.

Co může nastat, nejsou-li RFID čipy dostatečně zašifrovány, poznali před rokem někteří výrobci automobilů: jejich blokovací zařízení založené na RFID bylo prolomeno. Data na transpondéru (RFID tagu) firmy Texas Instruments byla chráněna klíčem o délce pouhých 40 bitů. Na zjištění tohoto klíče stačila bezpečnostním specialistům krátká doba: celých 15 minut. Odtud už k elektronickému paklíči vede jen krátká cesta. ■ ■ ■

ODKAZY

Prezentace výzkumníků z Amsterdamu:
www.rfidvirus.org/papers/percom.06.pdf
RFID u Metro Group:
www.future-store.org