ANALÝZA NFC RELAY ÚTOKU

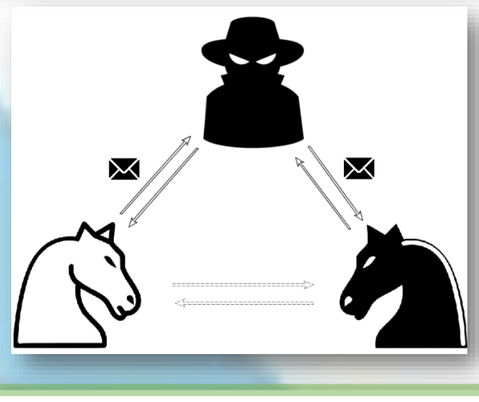
Petr Holubec

Příspěvek 20

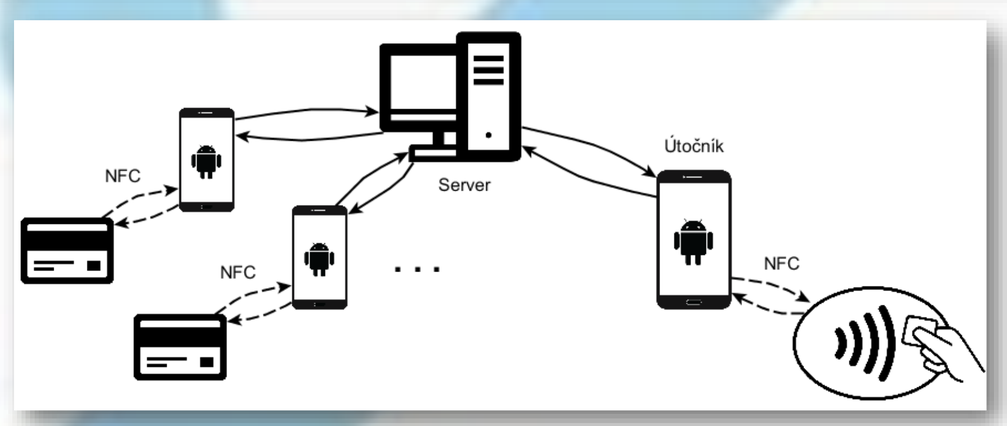
- **Platíte bezkontaktně?**
  - **Víte, co lze provést s Androidem a internetem?**
    - **Nebojíte se?**

S rostoucí pohodlností lidí se zvyšuje i **riziko zneužití** technologií. Stále diskutovanější je proto i bezpečnost bezkontaktních plateb, která se týká většiny z nás. Pro nechtěné zaplacení cizího nákupu totiž stačí chytrý telefon s Androidem a rychlé připojení k internetu.

Princip relay útoku lze demonstrovat na problematice hráče šachů, který chce vyhrát proti šachovému mistrovi, popsané J. H. Conwayem. Šachista – amatér hraje na dálku dvě partie šachů se dvěma různými šachovými mistry, kdy v každé partii má jinou barvu. Svému protihráči vždy přeposílá tahy protivníka ze druhé partie, dokud hry neskončí. To mu zajistí výhru v jedné partii, aniž by musel nad hrou přemýšlet. Šachoví mistři totiž hrají navzájem proti sobě, aniž by tušili podvod.



Pro NFC relay útok potřebujeme dvě zařízení pod kontrolou útočníka. První z nich bude sloužit jako **falešná čtečka** bezkontaktní karty, druhé využijeme pro **emulaci karty**. Mezi těmito dvěma zařízeními je nutné vytvořit spolehlivý a především rychlý komunikační kanál bez zbytečných zpoždění. Dále už jen potřebujeme bezkontaktní kartu oběti a terminál, který chceme obelstít naší emulovanou kartou. Vzhledem k limitu 500 Kč pro platbu bez zadání kódu PIN, uvažujeme pouze částky do tohoto limitu.



Celý systém je **navržen** s ohledem na maximální škálovatelnost. Cílem není dosáhnout pouze ad-hoc spojení mezi dvěma zařízeními, nýbrž vytvořit centralizovaný systém, ve kterém bude moci figurovat teoreticky neomezené množství platebních karet. Útočník si poté pouze vybere, kterou z aktivních karet využije k platbě.

Zdroj: http://www.resurrectionmission.org/

Reálný útok může vypadat následovně. Útočník přiblíží telefon ke kabelce či kapse oběti například v prostředcích MHD, kině apod., zatímco druhý útočník bude jinde platit vybranou kartou za zboží, aniž by oběť cokoli tušila.
Nebezpečnější variantou by byla již rozsáhlá síť útočníků, případně zařízení vhodně rozmístěných po městě či v prostředcích MHD, kteří by zajišťovali komunikaci s kartami obětí. Mezitím by další skupina útočníků prováděla platební transakce aktuálně dostupnými kartami.

Ptáte se, jak se můžete proti tomuto zneužití Vaší platební karty **bránit**? V reálných podmínkách postačí, když v peněžence budete mít vedle platební karty i další bezkontaktní karty (např. další platební kartu nebo elektronické peněženky různých dopravců), které se navzájem vyruší a znemožní tak komunikaci s jednotlivými kartami. Nebo si můžete zakoupit speciální pouzdro na platební kartu, které dokáže odstínit pokusy o komunikaci s bezkontaktní kartou.

Zdroj: http://cdr.cz/clanek/bezpecnost-bezkontaktnich-platebnich-karet-kopiruje-je-nekdo-v-mhd-se-cteckou

Excel@FIT 2016