

Hardwarová bezpečnost Eskalační protokoly



**Masarykova univerzita v Brně
Fakulta informatiky**

Jan Krhovják

Bezpečný hardware

- Zajištění (rychlé) bezpečné komunikace a bezpečného úložiště dat
 - Vznik bankovních sítí => nutnost zabezpečení bankovních transakcí
 - Certifikační authority => potřeba bezpečného úložiště + akcelerace
- Architektura vychází z klasického von Neumanna
 - Kryptografické koprocesory/akcelerátory/čipové karty/USB tokeny
 - Omezená funkčnost => snazší verifikovatelnost => vyšší bezpečnost
- Bezpečnostní kategorie
 - Fyzická bezpečnost – zabezpečení informace
 - Logická bezpečnost – zamezení neautorizovaného přístupu k datům
 - Bezpečnost prostředí – zabezpečení celého systému
 - Operační bezpečnost – bezpečnostní zásady při používání systému
- Bezpečný hardware negarantuje absolutní bezpečnost

Analýza bezpečnosti API

- Velký počet podporovaných standardů zajišťuje interoperabilitu, ale zapříčiňuje také vznik mnoha chyb
- Tři zásadní problémy kryptografických API
 - Nedostatečné zajištění integrity klíčů
 - Problémy ze zpětnou kompatibilitou (např. podpora DES či RC2)
 - Útoky: Meet in the Middle Attack, 3DES Key Binding Attack ...
 - Nedostatečná kontrola parametrů funkcí
 - Bankovní API a práce s PINy => PIN recovery attacks
 - Útoky: Decimalisation Table Attacks, ANSI X9.8 Attacks ...
 - Nedostatečné zajištění bezpečnostní politiky
 - PKCS #11 – pouze množina funkcí, navrženo pro jedinouživatelská hardwarová zařízení
- Bezpečnost současné generace (bankovních) API je nedostatečná

Eskalační protokoly

- Autentizované ustavení kvalitních kryptografických klíčů
- Založeny na použití dat s nízkou entropií (např. PINů či hesel)
- Odolné vůči off-line útokům hrubou silou (tedy i vůči slovníkovým útokům)
 - Klíč k symetrickému šifrování = heslo či PIN => šifrovaná data musí být nerozlišitelná od náhodných dat
 - Stále zranitelné on-line útoky ☹
- Na mezilehlých uzlech nevyžadují žádná perzistentní data
- Praktická aplikace
 - Kerberos; náhrada za zastaralé internetové protokoly
 - Vzdálený přístup k čipovým kartám; nový model pro sítě bankomatů
- Eskalační protokoly se stávají velmi oblíbenými
 - V současné době jsou v procesu standardizace (IEEE P1363.2)

Diffie-Hellman Encrypted Key Exchange (DHEKE)

- DHEKE je EKE založen na DH výměně klíčů
 - DH hodnoty jsou symetricky zašifrovány pomocí hesla P
 - $E_P(\alpha^x \bmod \beta)$ a $E_P(\alpha^y \bmod \beta)$
 - Není potřeba přenosu klíče K
 - K je odvozen z hodnoty $\alpha^{xy} \bmod \beta$
- Celý protokol (základ mnoha složitějších protokolů)
 - A->B: $E_P(\alpha^x \bmod \beta)$;
 - A<-B: $E_P(\alpha^y \bmod \beta)$, $E_K(R_B)$;
 - A->B: $E_K(R_A, R_B)$;
 - A<-B: $E_K(R_A)$;
- Velikost modulu β chráněného heslem může být menší 😊
- Kvalita klíčů nezávisí jen na délce klíče či návrhu EP
 - Základním požadavkem je náhodnost a nepředvídatelnost

Současně probíhající práce a otevřené problémy

- Probíhající práce
 - Analýza bezpečnosti API postavených na PKCS #11
 - Analýza bezpečnosti kryptografických eskalačních protokolů

- V jakých oblastech lze v budoucnu spolupracovat
 - Projekty související s autentizací uživatelů
 - Analýzy (případně návrh nových) autentizačních protokolů
 - Formální verifikace kryptografických (autentizačních) protokolů
 - Autentizační mechanismy založené na použití biometrik
 - Projekty zabývající se bezpečným hardwarem
 - Analýzy bezpečnosti (API, čipové karty, bezpečnostní politiky ...)
 - Vytváření bezpečných nosičů dat (USB tokeny ...)
 - Testování generátorů (pseudo)náhodných sekvencí