KIVFS: Zabezpečení, šifrování a ověření identity

Marek Pivnička

vedoucí práce: Ing. Luboš Matějka

Západočeská univerzita v Plzni
Fakulta aplikovanných věd
Katedra informatiky a výpočetní techniky

25. června 2009

Návrh bezpečnostního modelu

- Poskytnout uživatelům KIVFS odpovídající zabezpečení prokázání identity a ochranu přenášených dat.
- Toho docílíme procesy autorizace, autentizace a šifrováním přenosu.
- Poskytnout transparentně data pro nižší vrstvy.
- Umožnit použití KIVFS pouze určitým uživatelům.

Bezpečnostní model

- Na základě teoretických poznatků byla vybrána vhodná kombinace protokolů.
- Pro autorizaci, autentizaci a správu účtů uživatelů je použit protokol Kerberos.
- Pro šifrování přenosu je použit protokol SSL.

Ochrana přenášených dat

KIVFS obsahuje několik druhů přenášených dat:

- Autentizace: šifrování komunikace zajišťuje protokol Kerberos.
- Autorizace: šifrování komunikace také zajišťuje protokol Kerberos.
- Řídící data aplikace: šifrování komunikace realizováno pomocí protokolu SSL.
- Přenášené soubory: nešifrujeme z důvodu vyšší režie.

Protokol Kerberos

- Při šifrování autentizace a autorizace je užito symetrické šifrování.
- Používáme vlastní Kerberos server implementace Heimdal.
- Kerberos server autorizuje jak uživatele, tak i službu na serveru - oboustranná autorizace.
- Pokud nelze ověřit identitu přes Kerberos, je komunikace ukončena.
- Původní myšlenka bylo použít pouze Heimdal. Nenabízí knihovny pro Windows, ty používáme od MIT.

Protokol SSL

- Pro šifrování použita volná implementace OpenSSL.
- Pro předání symetrického šifrovacího klíče je použit SSL Handshake.
- SSL Handshake používá algoritmus RSA z asymetrického šifrování.
- Veřejný klíč je obsažen v certifikátu, který server pošle klientovi. Klient šifruje komunikace pomocí tohoto klíče.
- Po SSL Handshake je bezpečně vyměněn symetrický šifrovací klíč pouze mezi klientem a serverem.
- Pro šifrování používáme šifru AES s délkou klíče 256 bitů.
- Na základě měření šifer byl vybrán vhodný kompromis mezi rychlostí šifry a zátěží serveru.

Realizace Kerberos

- TGT a tikety jsou uloženy v RAM, při skončení práce jsou zničeny.
- Je kontrolován čas, potřeba synchronizace klientů přes protokol ntp.
- Máme klienta pro OS Windows a OS Windows Mobile.

Realizace SSL

- Změřili jsme dostupné symetrické šifry s ohledem na přenosovou rychlost, vytížení klienta a vytížení serveru.
- Protokol SSLv3 nám nabízí pomalejší přenosovou rychlost, ale mamé vytížení serveru.
- U protokolu TLSv1 je průměrně 3x vyšší rychlost, ale velké zatížení serveru.
- Na základě naměřených hodnot vybrána šifra AES s délkou bloku 256 bitů, protokol SSLv3.
- Nabízí vysokou bezpečnost přenášených dat spolu s dobrou přenosovou rychlostí.

Závěr

- Bezpečnostní model je úspěšně implementován v projektu KIVFS.
- Zatím není dostupné šifrování souborů.
- Do budoucna je snadné přejít na použití ZČU Kerberos.
- Dalším krokem bezpečnosti uživatelských dat je šifrovaný oddíl na pevném disku.

Závěr

- Děkuji za pozornost.
- Vaše dotazy.