

# Bezpečnostní analýza ostatních projektů

Ivan Dendis, Martin Krivosudský, Lubomír Viluda – Hrochokobry

1.

Problem identification: A\_x(security architecture)

Severity: middle

Practicability: easy (directly by external attacker)

Description of the problem: Pokud se útočník dostane mezi klienta a certifikační autoritu může převzít identitu klienta a sledovat jeho komunikaci aniž by to klient poznal, jelikož ve specifikaci není napsáno, že by se veřejný klíč klienta něčím šifroval při tom, když se posílá do certifikační autority.

Proposed solution: šifrovat veřejným klíčem certifikační autority aby veřejný klíč klienta nebyl při přihlášení do CA jen tak dostupný.

2.

Není zde napsána délka klíčů jaké architektura používá.

3.

Není zde popsána hashovací funkce která je zde použita.

4.

Problem identification: A\_x(security architecture)

Severity: middle

Practicability: easy (directly by external attacker)

Description of the problem: Celá komunikace před ustanovením spojení mezi klienty probíhá nešifrovaně, čili kdokoli může odposlouchat kdo s kým komunikuje.

Proposed solution: Šifrovat veškerou komunikaci mezi jednotlivými entitami.

## Himanshu Karnatak, Ravibabu M., Mainak Garai – Sapiens

1. Není zde napsána délka klíčů jaké architektura používá. Ani vlastně jaké algoritmy jsou zde použity pro asymetrickou šifru.
2.
  - Problem identification: A\_x(security architecture)
  - Severity: low
  - Practicability: easy (directly by external attacker)
  - Description of the problem: Při zneplatnění nebo obnově certifikátu u CA se nijak neověřuje zda je to opravdu vlastník původního certifikátu. Takto by mohl kdokoli komukoli změnit public key.
  - Proposed solution: -
3.
  - Problem identification: A\_x(security architecture)
  - Severity: low
  - Practicability: easy (directly by external attacker)
  - Description of the problem: Problém je u serveru když se někdo chce odregistrovat. Nevím jak je řešeno aby nějaký klient nepřeregistroval jiného aniž by to tom původní klient věděl.
  - Proposed solution: -
4.
  - Není zde popsáno jak se kontroluje integrita zprávy. Jestli nějakou hashovací funkci nebo to řeší SSL samo nevím.

## Matěj Plch, Lukáš Toldy, Maroš Valter – Team

1.

Problem identification: A\_x(security architecture)

Severity: middle

Practicability: easy (directly by external attacker)

Description of the problem: Pokud se útočník dostane mezi klienta a server při přihlašování klienta může převzít identitu klienta a sledovat jeho komunikaci aniž by to klient poznal. Není zde napsáno, že se komunikace nějak šifruje, když se posílá veřejný klíč klienta na server.

Proposed solution: šifrovat veřejným klíčem serveru aby veřejný klíč klienta nebyl při přihlášení na server jen tak dostupný.

2.

Použité algoritmy pro šifrování chybí délka klíče.

3.

Není zde popsáno jak se kontroluje integrita zprávy.

Ve všech architekturách fyzický přístup ke klientskému zařízení zapříčiní kompromitaci bezpečnosti systému.