PASTI PRI VGRADNJI KRIPTOGRAFIJE V APLIKACIJSKI SVET

MARKO HÖLBL, BOŠTJAN BRUMEN

KRIPTOGRAFIJA

- Zgoščevalne funkcije (hash functions)
  - Prilagojene (dedicated)
- Šifrirni algoritmi (encryption algorithms)
  - Simetrične šifre (symmetric ciphers)
  - Asimetrične šifre (asymmetric cipers)
- Digitalni podpisi (digital signatures)
- Kriptografija javnega ključa (public key cryptography)

KRIPTOGRAFIJA

- ECB
- CBC
- OFB

- .cer, .crt, .der
- .p7b, .p7c
- .p12
- .pfx

NALOGE KRIPTOGRAFIJE

- Zaupnost
- Celovitost
- Overjanje
- Ne-zanikanje

PROBLEM?

- Algoritmi
- Implementacija

NA KRATKO

- Zgoščevalne funkcije (hash functions)
  - MD5, SHA1
- Šifrirni algoritmi (encryption algorithms)
  - Simetrične šifre (symmetric ciphers)
    - Blokovne
      - DES, AES
    - Tokovne
      - RC4
  - Asimetrične šifre (asymmetric cipers)
    - RSA
- Digitalni podpisi (digital signatures)
  - RSA
  - DSS

NA KRATKO

Asimetrična kriptografija

=

Kriptografija javnega ključa

PASTI

- V teoriji težko razbiti
- Napake pri implementaciji in rabi
- Najbolj pogoste ranljivosti in napake

NAPAČNA RABA ALGORITMOV

- Zastareli / ranljivi algoritmi
- Pravilna dolžina ključa
  - Vsaj 128 bitov pri simetričnih algoritmih
  - Vsaj 1024 bitov pri asimetričnih
- Daljši ključ = počasnejše delovanje

NEPRAVILNOSTI POVEZANE S KLJUČI (IN DIGITALNIMI POTRDILI)

- nepravilno shranjevanje in zaščita ključev in digitalnih potrdil
  - Močno geslo
  - hranjenje na zunanjem varnem nosilcu (pametna kartica)
- Neustrezno:
  - Ključ zakodirati v prog. Kodi
- Prenos preko varnih kanalov
- Socialno inženirstvo

NEVARNOST POVEZANE Z IMPLEMENTACIJO ALGORITMOV

- **Zelo** pogosta vrzel
- posegamo po uveljavljenih implementacijah
  - incident z OpenSSL knjižnico
- Bližnjica
  - Dostop do ključev - shranjevati najmanjšo možno mero podatkov, ki jih potrebujemo
- Temeljito testiranje
- Tudi pri uveljavljenih implementacijah so možne ranljivosti

PASTI POVEZANE Z NEOZAVEŠČENOSTJO IN POMANJKLJIVIM ZNANJEM

- Razumevanje konceptov
- Tudi končni uporabniki
- Napačna raba = varnostna luknja
- Priporočljivo vpeljati standardne procedure

TEŽAVA NAKLJUČNIH ŠTEVIL

- Zelo pomembna
- Preizkušene implementacije
- Ranljivosti v implementacijah

SMERNICE

- Povzete po OWASP in NIST priporočilih
  1. Pazite na napake pri prehodu v produkcijo
  2. Uporaba uveljavljenih implementacij
  3. Hranite samo podatke, ki jih resnično potrebujete
  4. Bodite pazljivi pri uporabi generatorjev psevdonaključnih števil
  5. Uporabite močne načine šifrirnih algoritmov [14] (načini OFB, CFB ali CBC).
  6. Dobra dokumentacija in redno izobraževanje
  7. Kriptografski ključi naj bodo pravilno in zadostno varovani
  8. Varnostno kritične hranite na zunanjih varnih nosilcih
  9. Ključi in digitalna potrdila morajo imeti omejen čas veljavnosti, ki je odvisen od njihove pomembnosti

SMERNICE

10. Varujte centralna ali jedrna digitalna potrdila in ključe
11. Arhiviranje digitalni potrdil in ključev
12. Zavedanje uporabnikov o odgovornosti
13. Šifrirajte in/ali digitalno podpišite vse pomembne podatke
14. Varujte dele programske kode, ki so zadolženi za kriptografijo
15. Gesla shranjujete v obliki izvlečkov s soljo

SKLEP

- Izobraževanje in zavedanje
- Spremljanje dogodkov

- Človek = najšibkejši člen