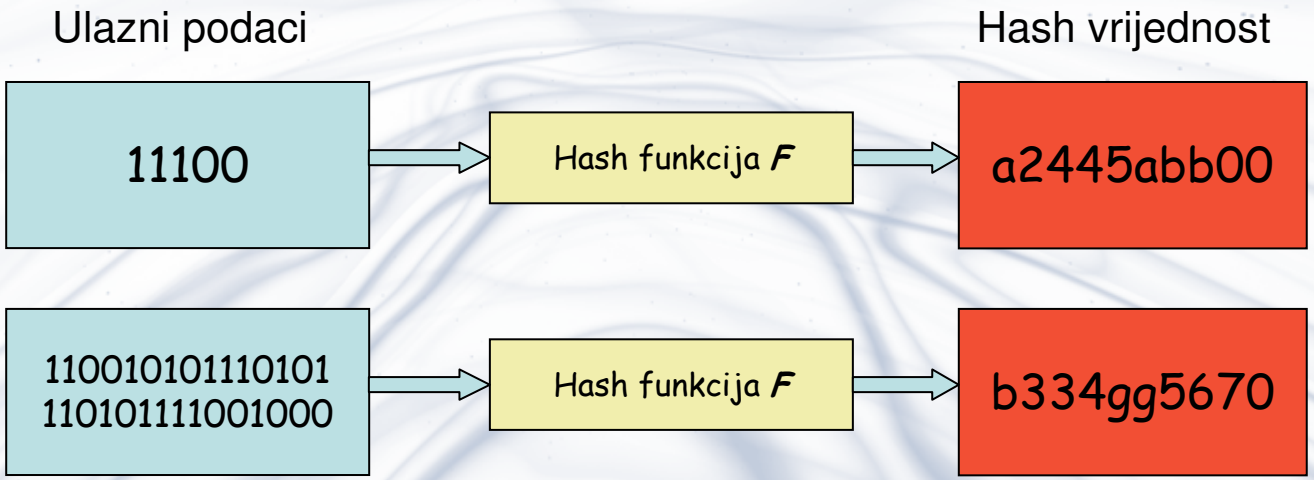
Tehnologije za provjeru integriteta datoteka

Branko Mažar, dipl.ing.
CARNet CERT

Sažetkovne (*engl.* hash) vrijednosti

- Iz ulaznog niza podataka proizvoljne duljine izračunava se sažetak fiksne duljine

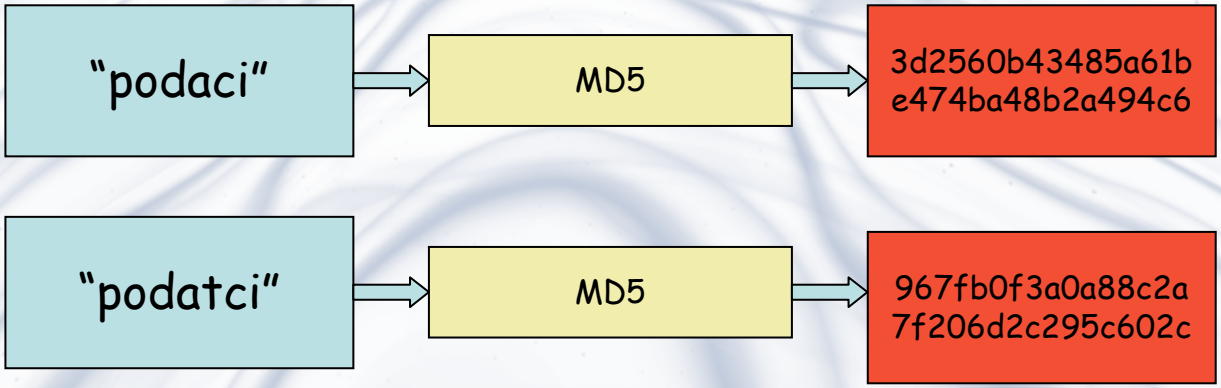


Hash funkcije

- Svaka hash funkcija primjenjuje neki hash algoritam za računanje sažetaka
- Obilježja hash funkcija:
  - Hash funkcije računaju sažetke fiksne duljine iz ulaznog niza podataka proizvoljne duljine
  - Funkcije za računanje sažetaka su ireverzibilne, tj. iz sažetka se ne može izračunati izvorni niz podataka
  - Postoji mogućnost kolizija – zbog fiksne duljine sažetaka dva različita ulazna niza podataka mogu rezultirati istim sažetkovnim vrijednostima
  - Kako bi se izbjegle predvidive kolizije, podaci koji se malo razlikuju rezultiraju potpuno različitm sažetkovnim vrijednostima – tzv. “efekt lavine”
- Vjerojatnost pojave kolizije predstavlja bitnu mjeru kvalitete pojedine hash funkcije. Stoga je kvaliteta hash funkcije usko povezana s duljinom rezultirajućeg sažetka

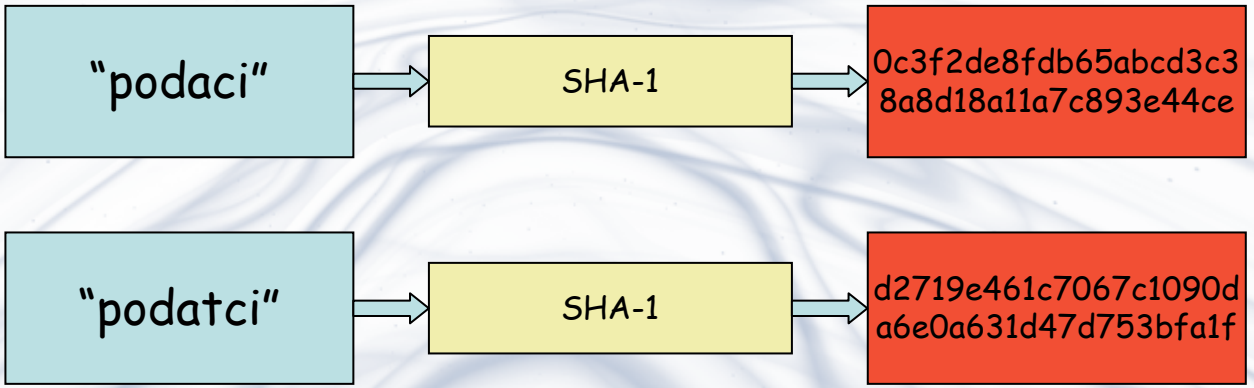
Kriptografski algoritmi za računanje sažetaka

- Temeljna karakteristika ovih algoritama je da su izvedeni s visokom razinom zaštite od napada
- Najrašireniji su MD5 i SHA-1
- MD5:
  - Razvio ga je Ronald Rivest 1991. godine
  - 128-bitni sažetak



Kriptografski algoritmi

- SHA-1:
  - Razvijen od strane NSA (*National Security Agency*)
  - 160-bitni sažetak



Primjene sažetaka u kriptografiji

- Autentikacija
  - Pohranjivanje i usporedba sažetaka lozinki
- Provjera ispravnosti podataka
  - Provjera autentičnosti e-mail poruka
    - u sklopu poruke se šalje i njezin sažetak što omogućuje provjeru originalnosti poruke
  - Provjera integriteta datoteka
    - pohranjuju se sažeci datoteka te se u određenom trenutku uspoređuju pohranjeni i trenutni sažeci

Provjera integriteta datotečnog sustava

- Princip provjere integriteta datotečnog sustava:
  - Izračunavaju se sažeci sistemskih datoteka odmah po instalaciji sustava, prije njegovog priključivanja na mrežu
  - Sažeci se pohranjuju na siguran medij (CD, DVD) ili neko drugo sigurno računalo
  - Za uvid u integritet sustava uspoređuju se sažeci trenutnog stanja sustava s pohranjenim sažecima

Sažeci datoteka

- Datoteke proizvoljne veličine sažimaju se u sažetke fiksne duljine:
  - Nekoliko MB -> 128 ili 160 bita
  - Sažetak nije kriptirana datoteka
  - Sažetak predstavlja digitalni “otisak prsta” datoteke (*engl.* digital fingerprint)
- Svaka promjena na datoteci rezultira drugačijim sažetkom
- Puno je jednostavnije uspoređivati 128-bitne ili 160-bitne sažetke nego sadržaje datoteka

Provjera integriteta datotečnog sustava

- Smisleno je računati i pohranjivati sažetke sistemskih datoteka koje nisu predviđene za često mijenjanje
- Računanjem sažetaka često mijenjanih (npr. korisničkih) datoteka ne bi se dobio uvid u integritet sustava
- Izmjene na sistemskim datotekama najčešće su uzrokovane:
  - Nadogradnjom operacijskog sustava i aplikacija
  - Djelovanjem zlonamjernih programa: virusa, crva, spywarea, rootkita i dr.
  - Neovlaštenim pristupom
- Ovim načinom ne može se utvrditi uzrok promjena već samo postojanje promjena, no dobiva se početna točka za daljnju analizu sustava

AIDE

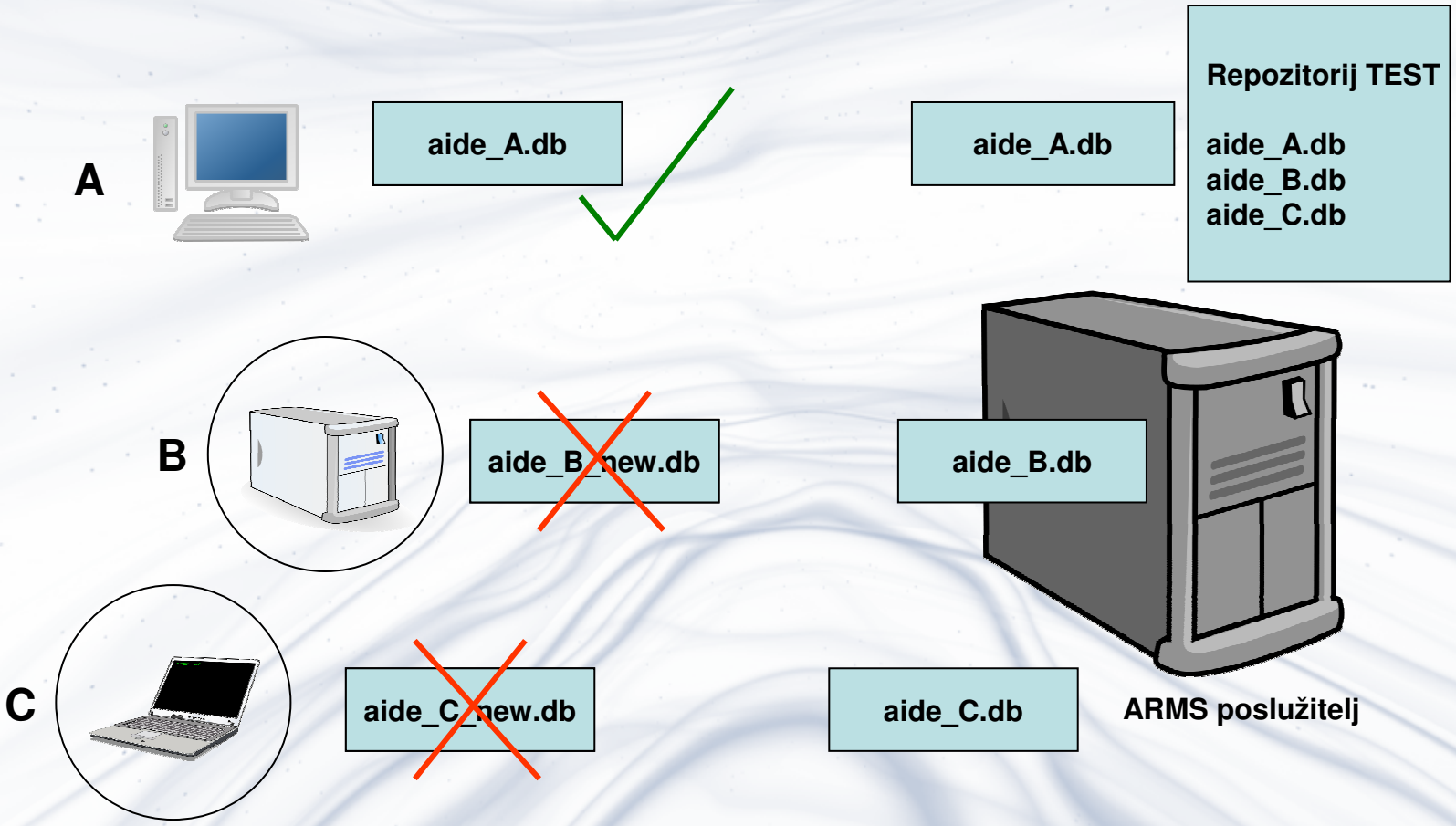
- AIDE – *open source* alat namijenjen provjeri integriteta datotečnog sustava
- AIDE generira sažetke odabranih datoteka sustava te ih pohranjuje u tzv. “bazu sažetaka”
- U svakom trenutku moguće je usporediti trenutno stanje sustava sa sažecima u referentnoj bazi
- AIDE se može preuzeti na stranici:

  http://sourceforge.net/projects/aide

ARMS usluga

- AIDE Repository Management Suite - ARMS, usluga razvijena u suradnji CARNeta i Srca
- Omogućuje pohranjivanje AIDE baza na **siguran** centralni ARMS poslužitelj te dohvaćanje istih korištenjem mrežne infrastrukture
- Elementi sustava:
  - Centralni ARMS poslužitelj
  - ARMS klijent koji se ugrađuje lokalno na ciljano računalo
- ARMS klijent omogućuje:
  - Stvaranje repozitorija na centralnom ARMS poslužitelju
  - Pohranjivanje AIDE baza na centralni ARMS poslužitelj
  - Pregled i dohvat pojedinih baza s poslužitelja

ARMS usluga - prikaz



Dva računala s izmijenjenim sistemskim datotekama!

CERT.hr

Što nakon provjere?

- Nakon provjere imamo točan popis izmijenjenih datoteka na računalima B i C
- Sada možemo početi analizu računala u potrazi za uzrokom promjena
- Ukoliko nije obavljena nadogradnja sustava niti instalacija novih aplikacija, imamo čvrstu indikaciju prisustva nepoželjnog softvera u sustavu
- U slučaju svjesno učinjenih izmjena generiramo AIDE bazu novog stanja sustava i pohranimo je na ARMS poslužitelj
- Periodičkim ispitivanjem sustava na ovaj način dobivamo kontinuirani uvid u njegov integritet

Kraj!

Zahvaljujem na pažnji!

CARNet CERT

http://www.cert.hr

ccert@cert.hr