Uvod v računalništvo (UvR)

Informacijska varnost

Danijel Skočaj
Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Literatura: Invitation to Computer Science, poglavje 8

v1.0
Št. leto 2013/14

Cilji predavanja

- Poznati ukrepe za povečanje informacijske varnosti
- Razložiti kako so gesla šifrirana z zgoščevalno funkcijo
- Opisati različne načine napadov iz omrežja
- Šifrirati in dešifrirati sporočila z enostavno Cezarjevo kodo ter bločno kodo
- Poznati šifriranje z algoritmom DES
- Primerjati simetrično in nesimetrično šifriranje
- Opisati proces pri šifriranju z algoritmom RSA
- Razumeti delovanje protokolov SSL in TLS

Uvod

- Informacijska varnost
  - zavaruj informacijo
  - dostop do informacij naj imajo samo avtorizirane osebe
- Fizična varnost
  - fizične prepreke pri dostopu do računalnikov (npr. zakljenena soba)
  - nadzor nad napravami
- Online (spletna, internetna) varnost
  - varen zbirni jezik
  - varen operacijski sistem
  - varno omrežje

Avtentikacija

- Avtentikacija: ugotavljanje identitete
  - Običajno z uporabniškim imenom in geslom
  - Datoteka z gesli je šifrirana
    - zgoščevalna funkcija
  - Pri prijavi:
    - preberi uporabniško ime in geslo
    - poišči up. ime v datoteki z gesli
    - izvedi zgoščevalno funkcijo na geslu in primerjaj
  - Še bolj varno
    - zapomni si čas kreiranja gesla in ga dodaj k geslu bred uporabo zgoščevalne funkcije
    - identični gesli se ne bosta enako šifrirali
  - Napadi na gesla
    - ugani geslo (groba sila ali s poznavanjem uporabnika)
    - ukradi datoteko z gesli in uporabi program za odkrivanje gesel
    - socialno inženirstvo – pripravi osebo, da izda geslo
  - Druge metode za avtentikacijo
    - odgovori na dodatna osebna vprašanja
    - biometrična informacija (prstni odtisi)

Avtorizacija

- Z avtorizacijo upravljamo kaj lahko avtenticiran uporabnik počne
  - množica dovoljenih akcij za vsakega uporabnika
- Operacijski sistem dovoli samo avtorizirane posege oz. dostope do virov

- Datoteke in direktoriji imajo sezname dovoljenih posegov:
  - beri datoteko (R)
  - dodaj novo informacijo v datoteko (A)
  - spremeni trenutno informacijo (C)
  - izbriši datoteko (D)
- Administrator ima univerzalen dostop in postavi avtorizacijske pravice drugim uporabnikom

File: GRADES

Name	*Permitted Operations*
Smith	R (R = Read only)
Jones	RA (A = Append)
Adams	RAC (C = Change)
Doe	RACD (D = Delete)

Grožnje iz omrežja

- Zlonamerna programska oprema (Malware)
  - virus: program vdelan v drugi program, se razmnožuje in razširja po omrežju, ko je program pognan (npr. v datotekah pripetih sporočilom elektronske pošte)
  - črv: se lahko replicira in razširja sam, ne da bi bil posredovan v okuženem programu
  - Trojanski konj: program, ki zgleda koristen, a vsebuje skrito zlonamerno kodo
- Napad DOS (Denial of Service) – onemogočanje storitve
  - veliko računalnikov skuša hkrati dostopati do istega URL
  - DDOS – porazdeljen DOS, armada zombijev (botnet)
- Spletno ribarjenje (phishing) – poizkus pridobitve osebnih občutljivih podatkov s socialnim inženiringom
  - el. sporočila s pozivom za osvežitev gesla na bančnem računu ipd.

Zaščita pred grožnjami iz omrežja

- Protivirusna programska oprema (antivirus software)
  - detektira in odstrani črve, viruse, Trojanske konje
  - redno osveževanje!
- Požarni zid (firewall software)
  - blokira komunikacijo, ki ni dovoljena
- Protivohunska programska oprema (antispyware)
  - detektira zlonamerno vohunsko programsko opremo
- Vedno namesti zadnje varnostne programske popravke (security patches)
- Ne odpiraj pripetih datotek iz neznanih virov
- Ne nalagaj programske opreme iz neznanih virov
- Ne pošiljaj osebnih ali bančnih podatkov neznancem

Šifriranje

- Kriptografija - veda, ki se ukvarja s skrivanjem vsebine sporočila z uporabo šifriranja in dešifriranja
- Šifriranje – pretvori originalno sporočilo v šifrirano sporočilo
- Dešifriranje- pretvori šifrirano sporočilo nazaj v originalno obliko

- Simetrični šifrirni algoritem
  - isti ključ je uporabljen za šifriranje in dešifriranje
  - problem: varna dostava ključa
- Asimetrični šifrirni algoritem (javni ključ)
  - dva ključa: javni in zasebni
  - javni (splošno znani) za šifriranje
  - zasebni (ga pozna samo prejemnik) za dešifriranje
  - relacija med javnim in zasebnim ključem mora biti kompleksna

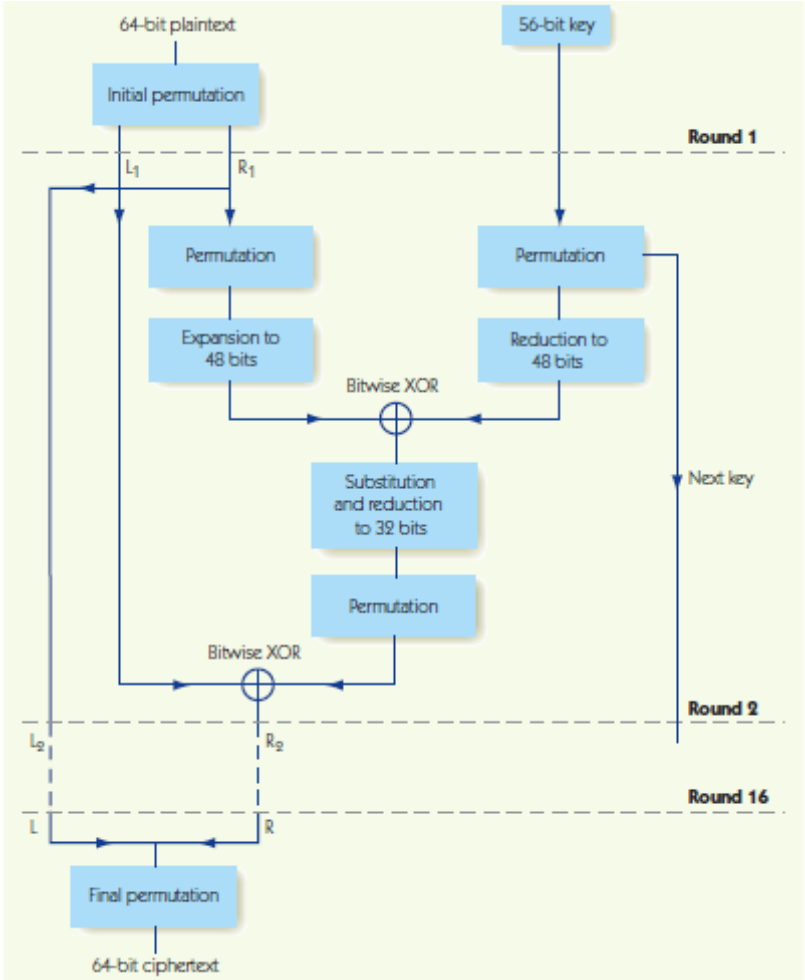
Enostavni šifrirni algoritmi

- Cezarjeva šifra
  - preslikaj posamezne znake v znake oddaljene za določeno razdaljo v abecedi
  - samo 25 ključev
  - Substitucijsko šifriranje (substitution cipher)
    - drugi (bolj splošni) načini preslikav
    - možen vdor z analizo frekvenc pojavnosti in sopojavnosti posameznih znakov
  - Pretočno šifriranje (stream cipher)
    - šifrira en znak naenkrat

- Bločno šifriranje
  - šifrirajo se bloki in ne posamični znaki
  - vsak znak prispeva k šifriranju več znakov
  - matrična bločna šifra

Šifriranje DES

- DES - Data Encryption Standard
- simetrični šifrirni algoritem
- načrtovan za digitalne podatke – binarno originalno sporočilo
- 64 (56) bitni binarni ključ
- 16 krogov manipulacij s sporočilom
- hiter in učinkovit
- zahteva skupni ključ
- 56 bitni ključ premalo za moderno tehnologijo
- AES (Advanced Encryption Standard)
  - podoben pristop
  - daljši ključ



Šifriranje z javnim ključem

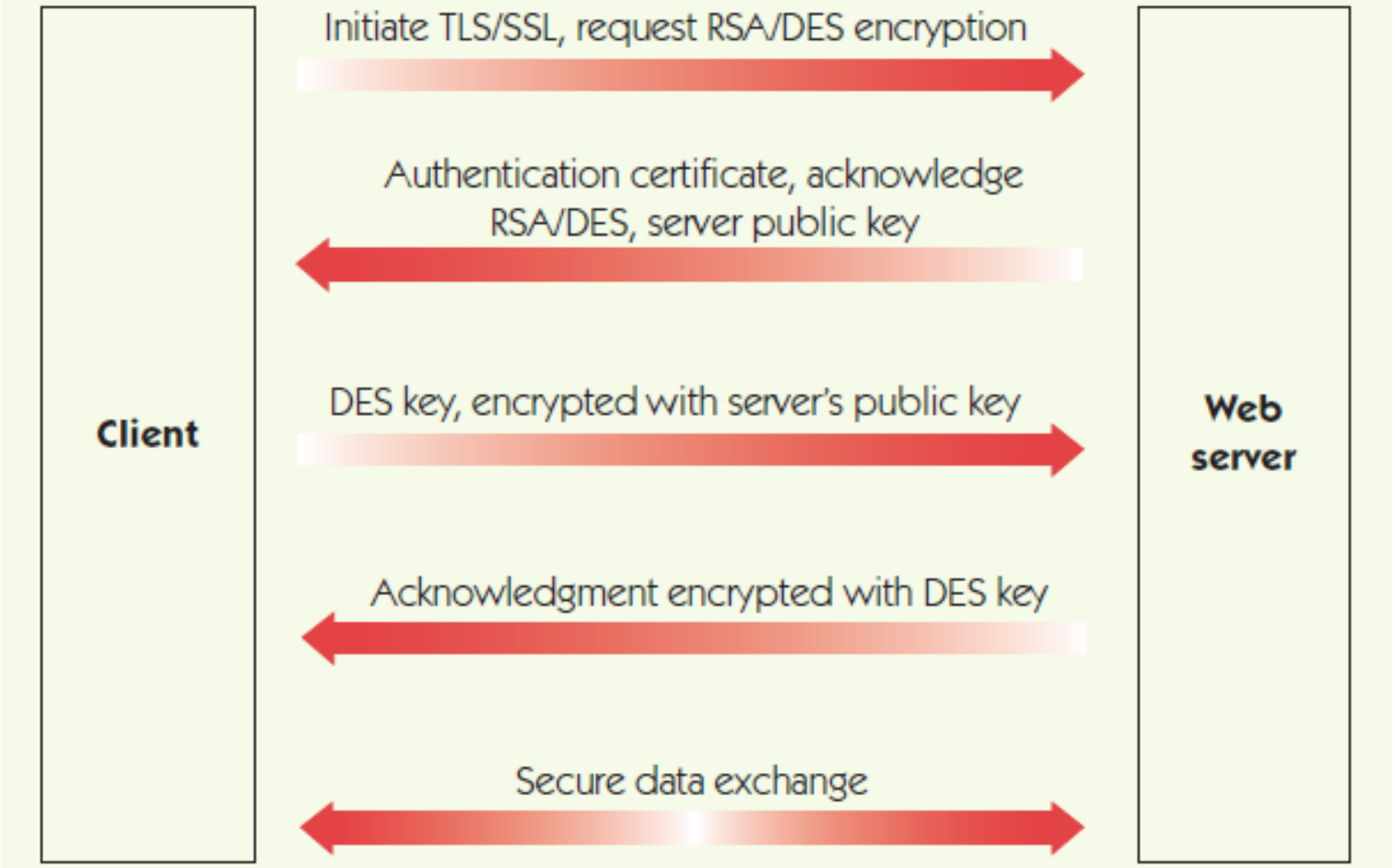
- RSA šifriranje
  - javni ključ poznan vsem, zasebni ključ samo prejemniku
- Kreiranje ključev:
  1. Izberi dve veliki praštevili p in q
  2. Izračunaj $n=p \cdot q$ in $m = (p-1) \cdot (q-1)$
  3. Naključno izberi veliko število e, tako, da e in m nimata skupnih deliteljev (razen 1)
  4. Najdi enolično število d med 0 in m, tako, da je $(e \cdot d) \bmod m = 1$
  5. Javni ključ = (n,e); Zasebni ključ = d
- Šifriranje (z javnim ključem (n,e))
  - Spremeni sporočilo v število P
  - Izračunaj $C = P^e \bmod n$
- Dešifriranje (z zasebnim ključem d)
  - Izračunaj $M = C^d \bmod n$

Varen prenos preko spleta

- Elektronsko poslovanje zahteva varen prenos osebnih podatkov, gesel, številk kreditnih kartic
- Varnostni spletni protokoli
  - SSL (Secure Sockets Layer)
  - TLS (Transport Layer Security)
- Uporabljata RSA in DES
  - deluje po principu odjemalec/strežnik
  - strežnik pošlje avtentikacijski certifikat in svoj javni ključ
  - odjemalec pošlje svoj DES ključ šifriran po RSA
  - nato se podatki pošiljajo preko (skupnega) DES ključa
- Rokovanje (handshaking) na začetku inicializira varen prenos
  - RSA je računsko zahteven zato se z njim na varen način prenese samo simetrični ključ
  - DES je zelo hiter, zato se z njim nato prenese celotno sporočilo

Varen prenos preko spleta

- Seja TLS/SSL



Varnost v vgrajenih računalnikih

- Vgrajeni računalniki (embedded computers)
  - avtomobili, hišni aparati, alarmni sistemi, telefoni, digitalne ure, PM3 predvajalnik, igralne konzole, digitalna kamera, kreditne kartice, mikrovalovna pečica, navigacijski sistemi, krmilni sistemi v avtomobilih, avtopilot, bančni avtomati, medicinske naprave,…
- Nov trend: povezava vgrajenih računalnikov na mrežo
  - pošiljajo podatke, se nadgrajujejo
  - Internet stvari (Internet of things)
  - večja nevarnost zlorab
- Napadi na vgrajene računalnike lahko povzročijo kaos
- Potrebna velika previdnost!

Povzetek

- Internet in svetovni splet sta namenjena širjenju informacij, zato je težko zagotoviti informacijsko varnost
- Grožnje iz omrežja: virusi, črvi, Trojanski konji, napadi z ohromitvijo storitve, spletno ribarjenje,…
- Informacijska varnost zajema šifriranje občutljivih podatkov pred pošiljanjem oz. shranjevanjem
- Simetrično šifriranje zahteva skupni ključ
  - Cezarjeva koda, bločna koda
  - DES, AES
- Asimetrično šifriranje zahteva javni in zasebni ključ
  - RSA
- Protokoli za varno prenašanje informacij preko spleta
  - SSL/TLS
- Problem varnosti v vgrajenih sistemih