Universiteti i Prishtinës "Hasan Prishtina" Kosovë

Programimi i distribuar

Pjesa 7 – Siguria

Prof. Asoc. Dr. Ermir Rogova

Përmbajtja

- Problemi i Sigurisë
- Kontrolla e qasjes (Access Control)
- Kriptografia
- Autentifikimi

Problemi i Sigurisë

- Kufizimi i aksesit në informacion dhe burime vetëm për ata që kanë qasje të autorizuar!
- Klasa të kërcënimeve:
  - Rrjedhje/ Leakage (përvetësimi i paautorizuar i informacionit)
  - Ngatërrime/ Tampering (ndryshimi i paautorizuar i informacionit)
  - Vandalizmi (ndërhyrje me funksionimin e sistemit)

Problemi i Sigurisë

- Kanali i komunikimit veçanërisht është i ndjeshëm ndaj sulmit:
  - Përgjimi (marrja e kopjes pa autorizim)
  - Maskimi (duke përdorur identitetin e tjetrit pa autorizim)
  - Cenimi i Mesazhit, ngatërrimi (sulmi njeriu në mes)
  - Replaying
  - Mohimi i Shërbimit

Supozimet e sigurisë

- Ndërfaqet/interfaces janë të ekspozuar: Hakerat mund të dërgojnë mesazh në çdo proces komunikimi.
- Rrjetet janë të pasigurtë: Adresat mund të jenë fallso.
- Algoritmet janë në dispozicion të hakerëve: Fshehtësia varet më shumë nga fshehtësia e çelsit sesa nga algoritmi.
- Sulmuesit kanë qasje në burimet të mëdha: fuqia kompjuterike nuk do të jetë një problem për hakerat gjatë jetës së sistemit.

Access Control / Kontrolli i qasjes

- Operacionet
  - Kërkesat në sistemet e shpërndara janë zakonisht të formës:

    <op, principal, resource>
- Mbrojtja e domain-eve / Protection Domains
  - Mjedisi i Ekzekutimit ndahet nga proceset.
  - Set i çiftit <resource, rights> - e ngarkuar në mënyrë tipike me hyrje me emrin përkatës.

Access Control / Kontrolli i qasjes

- Aftësitë
- Set i aftësive të mbahet nga çdo proces sipas domen-it të saj.
  - <identifikimi i burimeve, operacionet, kodi i vertetimit apo autentikimit>
  - <resource identifier, operations, authentication code>
- Kodi për autentikim bën të pamundur falsifikimin.
- Kërkesat e klientit janë të formuluara
  - <op, userid, aftësi/ capability >
- Disavantazhet : mund të vidhen, çelësat mund të kenë nevojë të revokohen apo anulohen, tërhiqen.

Kriptografia

- 2 klasa
  - Simetrike (çelës të përbashkët sekret)
  - Asimetrik (çelës publik / privat në çift/pair)
- 2 Role:
  - Fshehtësia dhe integriteti
  - Autentikimi
- Konsiderohen:
  - Skenarët
  - Algoritmet

Nocioni i Kriptografisë

Alice	First participant
Bob	Second participant
Carol	Participant in three- and four-party protocols
Dave	Participant in four-party protocols
Eve	Eavesdropper
Mallory	Malicious attacker
Sara	A server

Nocioni i Kriptografisë

K_A	Alice's secret key
K_B	Bob's secret key
K_{AB}	Secret key shared between Alice and Bob
K_{Apriv}	Alice's private key (known only to Alice)
K_{Apub}	Alice's public key (published by Alice for all to read)
$\{M\}^K$	Message M encrypted with key K
$[M]_K$	Message M signed with key K

Skenari 1

- Alice dëshiron ti dërgoj disa informacione sekrete Bob-it. Alice dhe Bob ndajnë një çelës të fshehtë Kab.
- Alice enkripton M duke përdorur algoritmin për enkriptim të rënë dakord E (Kab, M) dhe çelësin e përbashkët Kab duke prodhuar {Mi} Kab.
- Bob dekripton me algoritmin për dekriptim D (Kab, M)
- Problemet:
  - Si Alice dhe Bob shkëmbejnë çelësat?
  - Si Bob e di se {Mi} nuk është një përsëritje e një mesazhi të mëparshëm?

Skenari 2

- Alice dëshiron qasje në file-et të ruajtura nga Bob (një file server).
- Sara është një server i autentifikimit/vërtetimit të menaxhuar në mënyrë të sigurtë.
- Sara merret me çështjet e përdoruesit me fjalëkalime dhe mban çelësat e fshehtë për të gjithë pjesëmarrësit e sistemit që ajo i shërben.
- Sara e di çelësin Ka të Alice dhe çelësin Kb të Bob.

Skenari 2

- Alice i dërgon një mesazh Sarës duke kërkuar qasje te Bob-i.
- Sara i dërgon një mesazh të enkriptuar Alice-ës me Ka të përbërë nga një Biletë * dhe një çelës të ri të fshehtë për komunikim me Bob - Kab - kështu që mesazhi i plotë është {{Bileta} Kb, Kab} Ka
  - Bileta e enkriptuar/koduar përmban identitetin e Alice dhe çelësin e përbashkët Kab dmth {Alice, Kab}
- Alice dekripton përgjigjen e dhënë {Bileta} Kb dhe Kab
- Alice dërgon një kërkesë R deri tek Bob. Kërkesa është {Bileta} Kb, Alice, R
- Bob dekripton biletën, duke i dhënë atij identitetin e Alice-ës dhe çelësin sekret të përbashkët. Kab është përdorur tashmë nga Alice dhe Bob për kohëzgjatjen e sesionit.

Skenari 3

- Bob gjeneron një çelës publik / privat në çift
- Grupi asimetrik i çelësave ku dekriptohet një mesazh i enkriptuar nga tjetri
- Çelësat janë Kbpub dhe Kb Kbpriv
- Alice dëshiron të komunikojë me Bob duke përdorur një çelës sekret të përbashkët Kab.

Skenari 3

- Alice i qaset një shërbimi të rëndësishëm të shpërndarjes për të marrë një certifikatë të rëndësishëm publike duke i dhënë çelësin publik Bob-it (Kbpub)
  - certifikata e nënshkruar nga një autoritet i besuar - një palë e tretë e besueshme dhe mirë e njohur.
- Alice krijon një çelës të ri sekret Kab dhe enkripton/kodon atë me Kbpub dhe i dërgon një mesazh Bob-it - duke përfshirë një identifikues për çelësin e përdorur për të enkriptuar.
  - Në rast se Bob kishte më shumë se një -
  - Keyname, {Kab} Kbpub
- Bob zgjedh/selecton KBpriv nga keystore i tij lokal dhe dekripton Kab.

Skenari 4

- Alice dëshiron të nënshkruajë një dokument M në mënyrë që çdo marrës i mëvonshëm mund të verifikojë se ajo është iniciator i saj.
- Procesi:
  - Alice llogarit një digest (hash) të gjatësisë fikse të dokumentit Digest (M)
  - Alice enkripton/kodon hashin duke përdorur çelësin e saj privat dhe bashkangjet atë në M-në e dhënë.
- M, {Digest (M)} KApriv - Bob merr mesazhin, ekstrakton M dhe llogarit Digest (M)
- - Bob dekripton {Digest (M)} Kapriv duke përdorur KApub dhe krahason rezultatet me llogaritjen/ kompjuterizimin Digest(M)
- M, {Digest (M)} Kapriv përfaqëson një nënshkrim dixhital.

Skenari 5

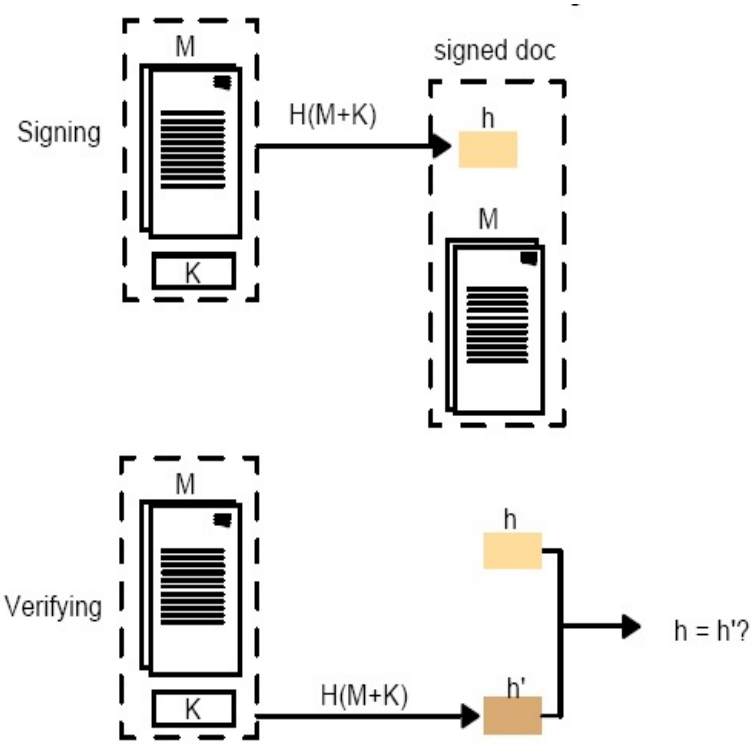
- Bob është një bankë.
- Alice ka nevojë për një çertifikatë nga Bob cili thotë se ajo ka një llogari me Bob.
- Carol mund të pranojë certifikatën kur Alice-ës i janë ngarkuar artikuj në llogarinë e saj me Bob.
- Carol ka nevojë për një çertifikatë nga një palë e tretë e njohur dhe e besuar (Fred) duke deklaruar vlerën e çelësit publik të Bob-it, në mënyrë që Alice nuk jep vlera të çelësit të Bob-it në një certifikatë të rreme apo fallso.
- Carol atëherë, megjithatë, duhet të vërtetoj apo autentikojë.
- Certifikata e Fred-it - autentikim rekursiv

Algoritmet kriptografike

- Symmetric Encryption
  - Encryption Function
  - Decryption Function
  - Shared Secret Key
- Asymmetric Encryption
  - Encryption Function
  - Decryption Function
  - Encryption Key
  - Decryption Key

Nënshkrimet dixhitale

- Kërkesat
  - Autentik
  - Unforgeable (e pamundshme për të falsifikuar)
  - Non-repudiable (e pakundërshtueshme)



Secure channels / Kanalet e sigurta

- Një kanal i sigurt mbron dërguesit dhe marrësit nga:
  - Fabrikimi/falsifikimi
  - Modifikimi.
  - Përgjimi.
- Për të pasur një komunikim të sigurtë ne duhet të kemi:
  - Një autentifikim/vërtetim nga palët e komunikimit.
  - Sigurim apo garantim i integritetit të të dhënave dhe konfidencialitet.

Autentifikimi / vërtetimi

- Merret me verifikimin e identitetit të përdoruesve para se ti lejojë ata të hyjnë/aksesohen në një burim.
- Ky mekanizëm parandalon përdoruesit e paautorizuar tu qasen burimeve të sistemit.

Autentifikimi

- Identifikimi: është procesi i kërkimit të pohimit të një identiteti të caktuar nga një përdorues.
- Verifikimi: është procesi i verifikimit të identitetit të pohimit të përdoruesit.
- Autentifikimi në sistem të shpërndarë mund të kategorizohet si në vijim:
  - User login autentifikimi
  - One-way vertetim apo autentifikim të entiteteve të komunikimit
  - Two-way vertetim i entiteteve të komunikimit.

Autentifikimi me User login

- Merret me verifikimin e identitetit të përdoruesit apo user-it nga sistemi përderisa logohet(logging in).
- Identifikimi i saktë i përdoruesit gjatë hyrjes-login bëhet e domosdoshme prej kur të gjitha vendimet e kontrollit të qasjes dhe funksionet e llogaritjes varen në këtë identitet.
- Për garantimin e sigurisë, një sistemin e autentifikimit i bazuar në fjalëkalime/password duhet të kenë mekanizmat e mëposhtme:
  - Të ruajnë fshehtësinë e fjalëkalimeve
  - Bëni fjalëkalimet e vështira për tu supozuar
  - Kufizojnë dëmin për shkak të një fjalëkalimi të kompromentuar

Autentifikimi në një drejtim (One way)

- Një entitet A dëshiron të komunikojë me entitetin B, B mund të dëshirojë të verifikojë identitetin e A-së para fillimit të komunikimit.
- Ky protokoll i vërtetimit apo autentifikimit drejtpërdrejt përdor kriptosistem të cilat kategorizohen në:
  - Protokollet e bazuara në kriptosistem simetrik
  - Protokollet e bazuara në kriptosystem asimetrik

Kriptosistemi simetrik

- Njohja e çelësit të përbashkët lejon enkriptim dhe dekriptim të mesazheve.
- Shembull: Përdoruesi apo user-i A dëshiron të komunikojë me përdoruesin B:
- A enkripton ID e tij duke përdorur K merr tekstin e koduar (cipher-text), dhe ia dërgon këtë mesazh përdoruesit B.
- User B dekripton duke përdorur K dhe krahason rezultatet me ID e mesazhit.
- Në rast se ato përputhen, përdoruesi A pranohet; në të kundërtën refuzohet.

Kriptosistemi asimetrik

- Çelësi publik i çdo përdoruesi publikohet, ndërsa çelësi i fshehtë i çdo përdoruesi është i njohur vetëm për përdoruesin.
- Shembull: Një përdorues dëshiron të komunikojë me përdoruesin B:
- A i dërgon ID e saj në formë plaintext B-së.
- B merr mesazhin dhe dërgon një numër të rastit/random për A në formë plaintext.
- Përdoruesi A merr këtë mesazh, enkripton çelsin e rastit duke përdorur çelësin e saj sekret merr shifër/cipher-tekst dhe ja dërgojn atë B-së.
- Përdoruesi B merr mesazhin, dekripton shifrën/cipher-tekst duke përdorur çelësin publik të përdoruesit A.
- Krahason rezultatin me numrin fillestar të rastit nëse ata janë të barabartë atëherë përdoruesi A pranohet; në të kundërtën refuzohet.

Autentifikimi në dy drejtime (Two-way)

- Protokolli me dy rrugë apo Two-way siguron që të dy proceset, dërguesi edhe marrësi të identifikojnë njëri-tjetrin para vendosjes së një kanali të sigurtë logjik të komunikimit mes tyre.
- Autentikimi i ndërsjellë apo i përbashkët mund të bëhet edhe duke kryer një rrugë apo one-way të vërtetuar apo autentifikuar dy herë.

Pyetje???