SYSTEMS LABORATORY

Cursul #09

Securitatea sistemului

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.

Eugene H. Spafford

Suport de curs

- Capitolul 12 – Securitatea sistemului
  - https://github.com/systems-cs-pub-ro/carte-uso/releases

Atacuri din 2020

- Twitter social engineering attack – Înșelătoria a vizat conturile a 130.000 de persoane publice, atacatorii putând reseta parolele conturilor.
  - https://securityboulevard.com/2020/07/biggest-twitter-breach-accounts-of-us-high-profiles-hacked-in-bitcoin-scam/
- Zoom data breach – 500000 de conturi zoom vândute pe dark web
  - https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
- Nintendo data breach – 160.000 - 300000 de conturi de utilizator au fost compromise într-un singur atac
  - https://www.forbes.com/sites/daveywinder/2020/06/12/300000-nintendo-users-hacked-what-gamers-need-to-know-switch-gamers-account-passwords/
- Easy Jet – Atacul cibernetic a expus detaliile a 9M de clienților
  - https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card

Problematica securității

- protecția informațiilor prețioase (companii, instituții) sau private (persoane)
- Ce este un sistem sigur?
  - resursele sale sunt utilizate și accesate în orice împrejurare așa cum se dorește
- Se poate obține un sistem sigur?
  - Da. Complet izolat de lumea exterioară.
  - nu este util, nici flexibil
- Ce înseamnă securizarea unui sistem de calcul?
  - folosirea de metode de protecție **suficient** de puternice
  - un potențial atacator va fi **descurajat**
  - compromiterea sistemului este **greu** de realizat
- Securitatea este un proces nu o finalitate

Ce urmărește un atacator?

- bani și/sau faimă
- steal
  - furt de informații (information disclosure)
  - sunt vândute sau se cere răscumpărare
- cripple
  - sistemul merge prost
  - Denial of Service (DoS)
  - sabotaj
- control
  - de acolo se pot fura informații (sau ransomware)
  - se poate extinde la cripple (DoS)
  - se pot folosi resursele (bitcoin mining, trimis SMS-uri)

Fundamentele securității

Obiectivele securității

- confidențialitate
- integritate
- disponibilitate
- robustețe
- protejarea vieții private (privacy)

- discutăm în continuare cum atingem obiectivele

Definiții

- Defect (bug)
- Vulnerabilitate
- Exploatare
- Atac, vector de atac
- Suprafață de atac
- Măsuri defensive
  - preventive
  - reactive

Principii de securitate

- principiul celui mai mic privilegiu (leastprivilege)
- principiul separării privilegiilor (privilege separation)
- securitythroughobscurityvs. securitybydesign
- cea mai slabă verigă
- simplitate (feature creep)
- Bruce Schneier: Complexityis theworstenemyof security.
- defense in depth
- securitate vs. utilizabilitate

Modelul subiect-obiect

- subiect sau agent efectuează acțiunea
  - de exemplu un proces
- obiect sau resursă este ținta acțiunii
  - de exemplu un fișier
- permisiuni specifice dictează accesul subiectului la obiect
  - de exemplu permisiuni în sistemul de fișiere
- o entitate specializată (reference monitor) verifică permisiunile
  - de obicei sistemul de operare

Autentificare

- accesul unui utilizator în sistem
- acesta poate crea procese
- pe baza unui identificator și token de autentificare (de exemplu parolă)
  - parolă
  - biometric
  - cheie publică (SSH)
  - one-time password

Autorizare

- bază de date de permisiuni
- adăugarea unei noi permisiuni înseamnă autorizarea unui subiect la un obiect
- chmod, chown

Controlul accesului

- verificarea permisiunilor în baza de date de autorizare
- făcut de reference monitor la accesul unui obiect de un subiect
- la comenzi precum ls, cat, vim

Securitatea datelor

Atacuri pe date

- furtul datelor
- modificarea datelor pentru a le face neutilizabile
- criptarea datelor pentru a fi răscumpărate (ransomware)

Protejarea datelor

- autentificare (pentru a limita accesul)
- criptare (pentru confidențialitate)
- algoritmi de message digest / message authentication (pentru integritate)

Permisiuni pe date

- asociate cu autorizare
- în general read și write
- întâlnite în sistemul de fișiere
  - uzual permisiunile sunt atașate fișierului
  - pot fi schimbate (chmod)

Criptarea datelor

- confidențialitate

- mesaj de intrare (MI)
- cheie de criptare (K)
- algoritm de criptare (A)
- mesaj de ieșire (MO)

- MO = A(K, MI)

Chei simetrice și asimetrice

- chei simetrice
  - aceeași cheie la transmițător și receptor
  - problematic dacă este interceptată
  - problematic să fie distribuită
  - criptare rapidă
  - AES
- chei asimetrice
  - cheie privată și cheie publică legate matematic
  - cheia publică criptează, cheia privată decriptează
  - fără probleme de distribuție
  - criptare greoaie
  - RSA

Integritatea datelor

- modificarea datelor este detectată
- algoritmi de hashing / message digest
  - se creează o sumă de control
  - se verifică dacă se păstrează suma de control
  - MD5, SHA

Securitatea accesului

Forme de autentificare

- parole (cea mai răspândită)
- biometric: retină, amprentă
- token hardware (one type password)
- cheie publică
- alt canal (SMS)

Multi-factor authentication

- mai multe forme de autentificare
  - parolă și SMS
  - parolă și cod de autentificare
- uzual altă formă este un dispozitiv pe care îl are utilizatorul în posesie
- 2FA, 3FA

Recomandări de gestiune a parolelor

- cel puțin 10-12 caractere
- să nu fie parole comune
- passphrase: parolă din cuvinte
- caractere speciale
- folosirea unui password manager
- schimbarea periodică a parolelor

- https://howsecureismypassword.net

Gestiunea parolelor în Linux

- Datele publice în /etc/passwd
- Informațiile de parole în /etc/shadow
  - /etc/shadow accesat doar de root
- Parolele se țin într-o formă hashed (MD5, SHA)
  - funcție one-way
  - e ușor să creezi dintr-o parolă hash-ul
  - e foarte dificil să inversezi procesul

Securitatea transferului

Securitatea transferului

- Cum ne autentificăm peste rețea?
- Cum protejăm datele (integritate + confidențialitate) transmise pe rețea de atacatori?

- Un model descentralizat, în care cele două entități comunicante își stabilesc identitatea (SSH)
- Un model descentralizat în care există autorități de certificare (CA)

Man in the Middle

- traficul poate fi interceptat
  - switch, ruter
  - atacuri de redirectare
- un atacator poate investiga și modifica pachetele de rețea
- un atacator poate impersona celălalt capăt al conversației

Firewall

- protejarea sistemului local de anumite pachete din rețea
- pot fi selectate pe bază de adresă IP, port, conținut, proces
- util pentru protejarea la atacuri de tip DoS (denial of service)
    - numite și flood

SSH pentru autentificare

- traficul este criptat
- se deschide la distanță uzual un shell autentificat
- SSH este un protocol
  - poate fi folosit pentru securizarea/criptarea și altor tipuri de trafic
  - spunem că tunelăm trafic prin SSH

Autentificare cu chei publice

- se generează pe client o pereche cheie privată-cheie publică
- cheia publică este adăugată pe server
- cheia privată semnează un mesaj
- mesajul poate fi verificat cu cheia publică
- dacă este prezentă cheia publică, atunci clientul este autentificat: are acces în sistem
- recomandat pentru SSH, simultan cu dezactivarea autentificării pe bază de parole

Securitatea protocoalelor

- conexiunile HTTP, IMAP, POP3, FTP, LDAP sunt implicit nesigure
- există variante sigure HTTPS, IMAPS, POP3S, FTPS, LDAPS
- se folosesc de TLS (Transport Layer Security)
    - criptarea traficului
    - verificarea identității serverului

Certificate digitale

- folosite de TLS
- un certificat este:
  - o cheie publică
  - o identitate
  - o semnătură digitală care le asociază pe cele două
- semnătura este realizată de cheia privată a unei autorități recunoscute (CA: Certification Authority)
- clientul are cheia publică a CA-ului
- poate verifica semnătura din certificatul serverului și valida, astfel, identitatea

Concluzie

Obiective atacator

- bani și/sau faimă
- steal
  - furt de informații (information disclosure)
  - sunt vândute sau se cere răscumpărare
- cripple
  - sistemul merge prost
  - Denial of Service (DoS)
  - sabotaj
- control
  - de acolo se pot fura informații (sau ransomware)
  - se poate extinde la cripple (DoS)
  - se pot folosi resursele (bitcoin mining, trimis SMS-uri)

Principii de securitate

- principiul celui mai mic privilegiu (leastprivilege)
- principiul separării privilegiilor (privilege separation)
- securitythroughobscurityvs. securitybydesign
- cea mai slabă verigă
- simplitate (feature creep)
  - Bruce Schneier: Complexityis theworstenemyof security.
- defense in depth
- securitate vs. utilizabilitate

Componente în securitatea sistemului

- securitatea datelor
- securitatea accesului
- securitatea transferului

RSA

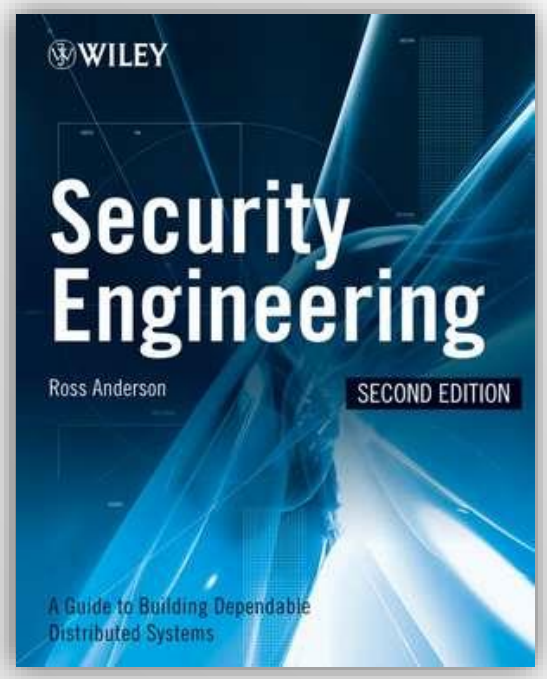
- numele de la fondatorii: Ron Rivest, Adi Shamir, Led Adleman
- inființată în 1982
- algoritmul de criptare cu chei publice RSA
- token-uri de autentificare (RSA SecurID security tokens)
- RSA Factoring Challenge

AES

- Advanced Encryption Standard
- adoptat de guvernul US ca standard de criptare în noiembrie 2001
- inițial denumit Rijndael după numele unuia dintre inventatori
- înlocuiește algoritmul DES (Data Encryption Standard) din 1977
- procesul de alegere a avut loc între 1997 și 2000 - destinat comunității criptografice
  - inițial aleși 15 algoritmi, apoi 5 finaliști, apoi doar 1 (Rijndael)

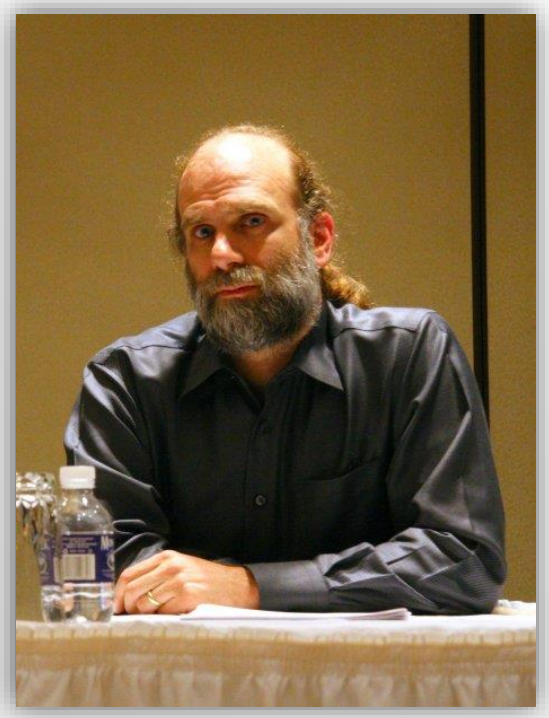
Security Engineering

- Ross Anderson
- 2nd Edition, 2008
- toate capitolele disponibile: https://www.cl.cam.ac.uk/~rja14/book.html
- o privire în ansamblu a securității sistemelor și rețelelor
- atacuri și apărare
- bogată în povestiri reale
- ușor de citit
- conține formalisme, dar insistă pe aspecte practice



Bruce Schneier

- autorul mai multor cărți de securitate
- algoritmi de criptografie
- Bruce Schneier on security (blog:) http://www.schneier.com
- Bruce Schneier Facts



BitDefender

- fondată în 2001 de Florin și Măriuca Talpeș
- companie românească producătoare de soluții de securitate cibernetică
- 38% dintre soluțiile de securitate de pe piața internațională
- sediu lângă Regie

Resurse pentru securitate aplicată

- OWASP (Open Web Application Security Project}): https://www.owasp.org/index.php/Main_Page
- wargames and challenge sites
  - http://www.wechall.net/
  - http://overthewire.org/wargames/
  - http://captf.com/practice-ctf/
  - https://w3challs.com/
- CTF (Capture the Flag) security contests
  - https://ctftime.org/
- Stack Exchange
  - http://security.stackexchange.com/
  - http://crypto.stackexchange.com/
  - http://reverseengineering.stackexchange.com/

Resurse utile

- http://www.unixtools.com/security.html
- http://insecure.org/
- http://www.linuxsecurity.com/
- http://www.schneierfacts.com/

Cuvinte cheie

- atacator
- vulnerabilitate
- exploatare
- vector de atac
- suprafață de atac
- confidențialitate
- integritate
- disponibilitate
- privacy
- subiect-obiect
- autentificare
- autorizare
- controlul accesului
- criptare
- chei simetrice
- chei asimetrice
- funcții hash
- AES
- RSA
- multi-factor
- parole
- password manager
- /etc/shadow
- SSH
- man in the middle
- firewall
- SSH
- TLS/SSL
- certificat digital