Tema nr.2 Controlul accesului în sistemele informaționale

1. Tipuri de control al accesului
2. Autentificare, autorizare, auditare (AAA)
3. Managementul parolelor

Lector univ. R.Bulai

1. Tipuri de control al accesului

- **Controalele sunt impuse pentru a diminua riscurile la care sunt expuse sisteme informaționale și pentru reducerea potențialelor pierderi.**

- **Controalele pot fi:**

1. Tipuri de control al accesului

- **1. Controale preventive** – au ca scop preîntîmpinarea apariției unor incidente în sistem;
- **2. Controale detective** – vizează descoperirea unor apariții ciudate în sistem;
- **3. Controale corective** – folosite pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

1. Tipuri de control al accesului

- **1. Controale administrative** – exercitate prin politici și proceduri, instruire, verificări (generale, la locul de muncă, în concediu) și o supraveghere exigentă;
- **2. Controale logice sau tehnice** – cuprind restricții de accesare a sistemului și măsurile prin care se asigură protecția informațiilor (sist de criptare, cardurile inteligente[crptare/decriptare, semnarea mesajelor, introducerea sist. de plăți electronice], protocoale de transmisie sau liste de control al accesului);
- **3. Controale fizice** – gărzile de protecție și pază, securitatea clădirilor (camere cu servere), protecția cablurilor, separarea atribuțiilor de serviciu.

1. Modele de control al accesului

- **1. Controlul obligatoriu al accesului** – autorizarea accesului unui subiect (entitate activă: persoană sau proces) la un obiect (entitate pasivă: fișier) depinde de **eticheta** care specifică nivelul de autorizare a subiectului, precum și de clasificare a obiectului [ex. dom.mil. documentele și utilizatorii lor sunt grupați în confidențial, secret și strict secret]. Controlul bazat pe reguli de acces
- **2. Controlul discreționar al accesului** – subiectul are autoritatea , în cadrul unor limite bine definite să specifice obiectele care pot fi accesibile, de ex. conform unei liste de control al accesului subiecților la obiectele sistemului;
- **3. Controlul nediscreționat al accesului** – o autoritatea centrală stabilește subiecții care pot să aibă acces la anumite obiecte, în funcție de politice de sec a organizației [de ex. controlul bazat pe **roluri** (rolul individual într-o orgaiz.) sau pe **sarcini** (responsabilitățile și sarcinile subiectului)].

Forme combinoate de cntrol

- Preventiv/administrativ
- Preventiv/tehnic (IntrusionPreventionSistem, protocoale, criptare, metode de acces etc.)
- Preventiv/fizic
- Detectiv/administrativ
- Detectiv/tehnic (IntrusionDetectionSistem)
- Detectiv/fizic (analiza a ceea ce oferă senzorii sau camerele)

2. Autentificare, autorizare, auditare (AAA)

- Controalele vizează responsabilizarea persoanelor care accesează informații sensibile.

- Responsabilizarea este înfăptuită prin **mecanisme de control al accesului** care exercită funcțiile de *identificare, autentificare, autorizare și auditare.*

Autentificare, Autorizare, Auditare (AAA)

Autentificare:

- Originea cuvantului in limba greaca cu sensul de real, veritabil
- Procesul de stabilire ca un obiect sau un subiect sunt adevarate, asa cum cineva pretinde, procesul de verificare a identitatii digitale

Exemplu: stabilirea identitatii unei persoane la ghiseul bancii cu un act de identitate.

Obs: autentificare si autorizare notiuni **diferite**

Autentificare, Autorizare, Auditare (AAA)

Autorizare:

- Procesul prin care unei entitati particulare i se acorda dreptul sa presteze o activitate, pe baza unor reguli, ca urmare a unei proprietati mostenite din procesul de autentificare
- Poate fi determinate de o gama de restrictii ca de ex: restrictii de timp, restrictii de locatie fizica, restrictii de acces multiplu la resursa.
- Exemplu: garantare accesului pentru citirea unui fisier specific de catre utilizatorul autentificat
- Tipuri de servicii: IP address filtering, address assignment, route assignment, Quality of Services, latime de banda etc.

Autentificare, Autorizare, Auditare (AAA) (3)

Auditare (Auditing sau Accounting):

- Urmarirea evenimentelor, de ex esecuri de autentificare si autorizare, resurse consumate de catre utilizatori.
- In afara aspectelor de securitate aceste informatii pot fi utilizate pentru management, planificare, facturare etc.
- Metode:
  - Real-time accounting, informatii interpretate in timp real
  - Batch accounting: informatiile sunt salvate si interpretate ulterior.
- Informatiile tipice stranse contin identitatea utilizatorului, natura serviciului furnizat, momentul la care serviciul a inceput si cand s-a terminat

Metode de autentificare

Metode bazate pe un singur factor:

- Autentificare bazata pe **ceea ce stii** (autentificarea cu username si parola)
  Ceva ce persoana știe ***Controlul accesului prin parole*** – o parolă de ex.

Avantaje:

- Nu necesita resurse importante de procesare
- Este o metoda de autentificare simpla
- Se pot transmite si alte informatii impreuna cu parola

Dezavantaje:

- Parola poate fi usor ghicita in multe cazuri
- De multe ori sunt stocate in clar pe un server (cine are acces la baza de date a serverului poate pretinde ca este alt utilizator).
- Chiar daca sunt stocate criptat pe server se pot transmite prin retele nesigure.
- Fiecare sistem detine o copie a informației de autentificare. Actualizarea parolele pe fiecare sistem duce la alegerea de parole simple (risc).
- Autentificarea nu este refolosibila, se autentifica pe fiecare sistem sau aplicatie. Exceptii: OpenID, OAuth
- Un sistem care impersoneaza sistemul real (prin *IP spoofing*), permite serverului impostor sa colecteze informatia personala ce va fi folosita pentru autentificare pe serverul real.

Metode de autentificare

Metode bazate pe un singur factor:

- Autentificare bazata pe **ceea ce ai** (PKI, ai o cheie privata)

  Ceva aflat în posesia persoanei ***Controlul accesului prin obiecte*** – cartele magnetice, cartele speciale [**carduri auexpirante**], echipamente de identificare personală sau jetoane;

- Autentificare bazata pe **ceea ce esti** (sisteme biometrice)

  Ceva care individualizează persoana ***Controlul accesului prin biometrie*** – identificările biometrice (amprente digitale, semnătură, voce, forma mîinii, imaginea retinei, imaginea feței etc.);[SUA dup 11.09 Congresul American a adoptat ca orice cetățean străin trebuie să posede un *document purtător de datele biometrice – recunoașterea feței și a amprentelor digitale, ulterior și recunoașterea irisului*]

Metode de autentificare

Metode bazate pe un singur factor:

- Autentificare bazata pe **locul unde esti** (autentificarea cu semnatura locatiei)

  Locul geografic ***Controlul geografic al accesului*** – unde este înregistrat calculatorul

  [Kaspersky punea problema legitimării persoanelor utilizatoare de servicii informatice și comunicații în spațiul global, tocmai pentru a se asigura responsabilizarea și conștientizarea participanților la noul trafic – el făcea asemănare cu sistemul de conducere a automobilelor…].

  [Corporația intern.Series Research din Colorado a realizat tehnologia autentificării locației *Cyber Locator.* Sistemul folosește semnale bazate pe microunde transmise de 24 sateliți GPS pentru calcularea și validarea unei **semnături a locației**. Fiecare utilizator al unui sistem protejat are un senzor al semnărurii locației **SSL**]

Metode de autentificare

- Metodele de control al accesului trebuie să se bazeze pe cel puțin două dintre cele 4 căi enumerate (cartelă-parolă, jeton-parolă tec.) sau să mai folosească și al treilea element – cel biometric.

Metoda bazate pe mai multi factori:

- autentificare cu doi factori combinatii **ceea ce ai/ceea ce sti** (token, smartcard) sau ceea ce esti/ceea ce stii.
- autentificare utilizand mai multi factori din categorii diferite

Exemple autentificare multi factor

- Smartcard pastreaza o cheie criptografica pe card ce este deblocata de utilizator cu keypair special. Utilizatorul introduce passphrase pentru a debloca cheia si sistemul face un schimb de chei criptografice cu serverul central pentru verificare

- Autentificare impartita intre doua persoane, ambele se autentifica

- **Autentificare centralizata:** utilizarea unui model centralizat ca autoritate centrala care autentifica utilizatorii remote la un mare numar de sisteme. Utilizeaza protocoale de autentificare remote ca RADIUS (Remote Access Dial-In User Service), TACACS (Terminal Access Controller Access-Control System), Kerberos, DIAMETER

- Tehnologia OTP

Zero-knowledge proofs

- Ofera posibilitatea ca o masina A sa convinga o alta masina B sa-I permita accesul fara a dezvalui o informatie secreta.
- Masinile ce folosesc o astfel de tehnica schimba mai multe informatii pentru a finaliza autentificarea.
- Clientul creaza o problema aleatoare si dificila de rezolvat pe care o rezolva cu informatiile pe care le detine.
- Clientul valideaza solutia utilizand o schema de validare si trimite solutia si problema serverului.
- Serverul cere clientului ca problema sa demonstreze ca aceasta este solutia.
- Clientul reactioneaza in conformitate cu cererea.
- De regula se ajunge la schimbarea a zeci de mesaje cu succes inainte ca autentificarea sa fie completa.

Rohos Logon Key

- **Soluția de autentificare prin 2 factori**

  convertește orice unitate USB în token de securitate pentru computerul Dvs. și permite accesul la Windows într-un mod sigur cu USB token, înlocuind Windows login

Rohos Logon Key

- Înlocuiește parola de autentificare de bază cu o cheie USB hardware (unitate flash USB sau card de memorie)
- Utilizează parola mare, care nu este necesar de memorizat
- Procesul de autentificare cu cheia USB este complet automat și rapid!
- Sistemul este protejat cu parolă însă nu este necesar să introduceți parola manual de fiecare dată cînd vă conectați sau deblocați Windows
- Autentificare asigurată prin 2-factori: Cheia USB + parola PIN
- Folosiți o singură cheie USB pentru a va conecta la computerul de acasa, laptop și de oficiu
- Acces limitat la computer bazat pe cheia USB
- Windows este protejat chiar și în Modul de Siguranță
- Stabilirea unei parole la contul Dvs. de utilizator ofera o protecție mai buna pentru computerul în hibernare.

Rohos Logon Key

- Logon de urgență vă va ajuta să accesați sistemul în caz că ați pierdut unitatea USB sau ați uitat codul PIN
- Codul PIN protejază cheia USB împotriva utilizării neautorizate pentru login (cu un numar limitat de încercări de accesare)

- Cu Modul de Siguranță – nimeni nu va putea evita cheia de securitate USB și deschide Windows în Safe Mode

- Rohos folosește principiile de securitate a datelor aprobate de NIST: parola nu este păstrata pe cheia USB în formă deschisă. Protecția la copiere a cheiei USB nu permite crearea neautorizată a duplicatelor. Toată informația de pe cheie este criptată cu AES-256 bit lungime cheie.

3. Managementul parolelor
(reguli de control al parolelor)

- Parolele trebuie schimbate cam la 6 luni, dar pentru datele deosebit de importante - termene și mai scurte;
- Parolele comune trebuie schimbate imediat ce o persoană părăsește grupul sau nu mai are dreptul utilizării;
- Parolele trebuie schimbate imediat ce se constată unnele bănuieli privind cunoașterea lor de alte persoane sau cînd trebuie dezvățuită pentru redresarea unei strări anormale temporale;
- Parolele trebuie ținute minte și nu scrise pe oriunde (cu excepția necesității intervenției de urgență / plic sigilat);
- Listele cu parole vor fi memorate în formă criptată;
- La introducere nu trebuie să se afle persoane străine prin preajmă;

3. Managementul parolelor
(reguli de control al parolelor)

- Cel puțin 14 caractere și nu 8 sunt destul de vulnerabile…
- Blocarea operațiunilor de încercare repetată;
- Dacă un terminal funcționează o perioadă lungă de timp / procesul de autentificare trebuie să aibă loc la intervale regulate de timp pentru a se asigura că nu folosește altcineva sistemul;

- Odată ce a pătruns în sistem, utilizatorul nu trebuie să i se permită să-și schimbe identitatea / să nu pătrundă în părțile altor utilizatori;
- La deschiderea unei noi sesiuni de lucru, userului trebuie să i se aducă la cunoștință ultimul timp de accesare a sist cu parola respectivă

Tehnologii de autentificare

- **One-time password**
- **Single Sign On (SSO)**
- **Password Manager**

One-time password

- Dezvoltata pentru a elimina problemele date de reutilizarea parolei
- Ideea a fost propusă de **Лесли Лампортом în anii 80**
- **Parola utilizata o singura data** (*one time password, OTP*) — este valida doar pentru o singura sesiune de autentificare sau poate fi limitata de un interval de timp
- **Avantajul:** parola nu poate fi reutilizabila
- **Dezavantaj:** se cere utilizarea tehnologiilor suplimentare (nu totdeauna poate preintimpina amenintarile **Man-in-the-Middle**)

One-time password

- Tipuri: parola provocare raspuns (*challenge-response*) si lista de parole

- *Provocare raspuns* raspunde cu o valoare de provocare dupa ce a primit id utilizator. Raspunsul este calculat fie din valoarea de răspuns cu dispozitive electronice sau selectat dintr-un tabel, pe baza provocarii.

  [Utilizarea algoritmilor matematici de creare a unei noi parole OTP pe baza unei cereri (de ex.un numar aleator, ales de server sau o parte dintr-un mesaj) si/sau contor]

- *Lista de parole*. Liste de parole utilizate secvential de persoana care doreste sa acceseze un sistem. Greu de calculat valorea urmatoare.

  [Utilizarea algoritmilor matematici de creare a unei noi parole OTP pe baza parolei precedente (parolele practic creaza un lant si trebuie sa fie utilizate intr-o anumita ordine]

- Autentificare bazata pe un token hardware care genereaza o parola conform unui algoritm care se bazeaza pe timp, verificata de serverul de autentificare

  [Sincronizarea in timp dintre server si client (parola este valida intr-un timp scurt)]

Exemple de OTP

- RSA SecurID utilizatorul poarta un token care este sincronizat in timp cu serverul central RSA. El genereaza numere de 6 digiti care se schimba la 60 secunde. La login se combina numarul de 6 digiti afisat de token cu PIN-ul personal pentru a crea one-time password. (http://www.youtube.com/watch?v=k_zpbJF9pmc)

- Tokenul ActivCard cere utilizatorului sa introduca PIN-ul si cu algoritmul special genereaza on-time password.

- Sistemul Secure Computing's SafeWord utilizeaza counter-based token care genereaza un simplu cod de sase digiti.

- Token software pastrate in sisteme separate ca PDA sau telefon ce genereaza parola.

- Sisteme challenge-based. Serverul central furnizeaza challenge (provocare) pe care utilizatorul il introduce in token si acesta genereaza parola

RSA SecurID
(server central de autentificare, agenţi software şi token-uri)

- **Agentul** este o aplicaţie software instalată pe o maşină ca: domain server, web server sau calculator personal, care facilitează comunicarea cu serverul central de autentificare. El cere fiecărui user care vrea să se logheze să introducă passcode-ul corect plus informaţiile de logare (user id şi network password)

- **Token**-ul este un dispozitiv hardware sau software care generează şi afişează un număr aleator (de 6 cifre) pentru a permite utilizatorilor să acceseze securizat resurse protejate din reţea. Numărul random se numeşte tokencode.

- În plus faţă de tokencode unele soluţii mai necesită un PIN, care poate fi creat de user sau generat de un server central de autentificare. Când utilizatorii doresc să acceseze acea resursa, pentru login, trebuie să introducă acest passcode (tokencode plus PIN).

- Fiecare token conţine un ceas şi un număr unic (seed number). La fiecare minut, un algoritm combină timpul curent şi acest număr rezultând afişajul de pe token, acele 6 cifre aleatoare.

În prealabil **serverul de autentificare** a fost configurat astfel**:**

- Seed number-urile au fost importate în sistem (seed number-urile sunt în nişte fişiere)
- Seed-urile din aceste fişiere sunt asigante token-urilor pentru a genera tokencode-ul când o cerere de autentificare este primită de la un agent.
- Se asignează token-uri utilizatorilor (înainte că un utilizator să se autentifice cu un token, acesta trebuie să fie recunoscut de server)
- Pentru a proteja împotriva furtului de passcode serverul verifică dacă acelaşi passcode a mai fost folosit într-o altă tentativă de autentificare.

RSA SecurID
(server central de autentificare, agenţi software şi token-uri)

În timpul procesului de autentificare serverul şi agentul lucrează în următorul mod:

1. Utilizatorul iniţiază o cerere de autentificare logându-se în sistem
2. Agentul cere utilizatorului să introducă un user id şi un passcode sau tokencode
3. Utilizatorul citeşte şi introduce tokencode-ul de pe token şi împreună cu PIN-ul creează passcode
4. Agentul software trimite datele introduse la server (pachetele trimise sunt criptate cu o shared key numită node secret care este stiută doar de server si de agent. Node secret este el însuşi criptat pe agent şi în bază de date)
5. Serverul primeşte datele şi caută un user record în bază de date
6. Serverul calculează valoarea corectă a passcode-ului accesând token record-ul asociat userului. Acest passcode este comparat cu cel primit de la utilizator
7. Serverul evaluează politicile date de administrator
8. Dacă passcode-ul este corect şi politicile permit accesul atunci userul are acces la aparatul protejat

One-time password. Standardizarea

- Sunt patentate foarte multe tehnologii OTP, ceea ce face ca standardizarea în acest domeniu sa fie greu de facut. Cu toate acestea există câteva standarde, precum RFC 2289[3] și RFC 4226 (HOTP).

- McAfee® One Time Password Server

Soluţia Single Sign On (SSO)

- Odată cu proliferarea serviciilor on-line a apărut şi nevoia firească de autentificare a consumatorilor acestor servicii.
- Astfel, s-a ajuns ca un individ să fie nevoit a memora mai multe zeci de parole, lucru care tinde să devină ineficient şi nesigur.
- Utilizatorii în general preferă să nu ia în calcul riscurile la care se expun şi pentru a evita notarea parolelor pe diverse suporturi aleg calea cea mai la îndemână, parola unică pentru toate serviciile.
- O soluţie la acest tip de probleme este adoptarea **sistemelor cu autentificare singulară**, numite Single Sign-On.
- **Un sistem SSO** permite ca un utilizator să fie autentificat automat fiecărui serviciu pe care îl accesează, cu condiţia autentificării iniţiale cu succes a clientului la sistemul SSO.

Soluţia Single Sign On (SSO)

- **OpenID** — este un sistem decentralizat care permite utilizatorilor să utilizaze un singur cont pentru a se autentifica pe mai multe site-uri, portaluri, bloguei sau forumuri care nu au vreo legatură comună.

- **Windows Live ID** (la început **Microsoft Wallet**, **Microsoft Passport**, **.NET Passport**,**Microsoft Passport Network**) — serviciu de identificare și autentificare de la Window Live. Se utilizează pentru o autentificare unică la toate serviciile de rețea de la Microsoft.

Password Manager

- Password Manager memorează numele de utilizator şi parolele asociate, astfel încât poţi dispune în acelaşi timp de mai multe parole diferite şi puternice, fără a fi necesară memorarea fiecăreia dintre ele

- Organizare şi stocare a tuturor parolelor într-o locaţie sigură
- Înregistrare pe site-uri şi aplicaţii printr-un singur click
- Acces şi securizare a tuturor parolelor prin intermediul unei parole unice
- Stocare a parolelor într-o bază de date criptată de pe PC
- Creare automată a unor parole puternice, unice
- Posibilitate de a stoca o versiune portabilă pe o unitate flash
- Completare automată a formularelor de înregistrare online

Password Manager

Managerii de parole pot fi clasificați în 3 categorii:

- Desktop — salvează parolele în managerul de parole instalat pe computer

- Mobile — păstrează parolele în managerul de parole instalat pe dispozitivul mobil sau pe suporturi mobile de memorie

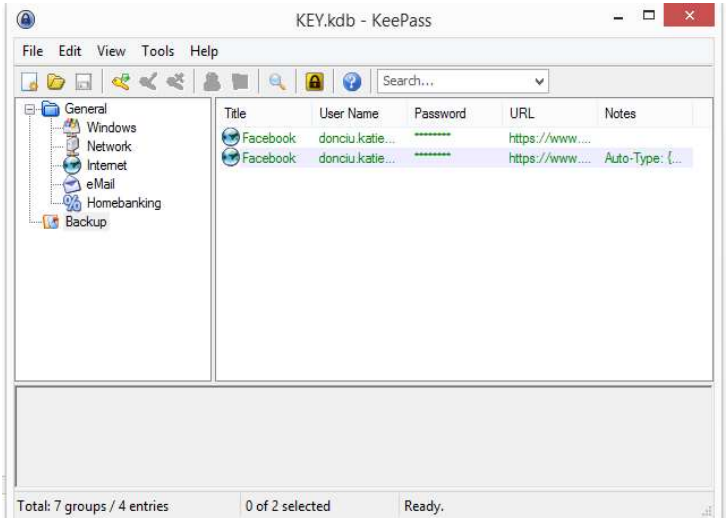
- De tețea — manageri de parole online, parolele fiind salvate pe site-urile provider-ilor

Cei mai populari manageri de parole:

- **KeePass, eWallet, LastPass, 1Password, RoboForm**
  (http://habrahabr.ru/post/125248/)

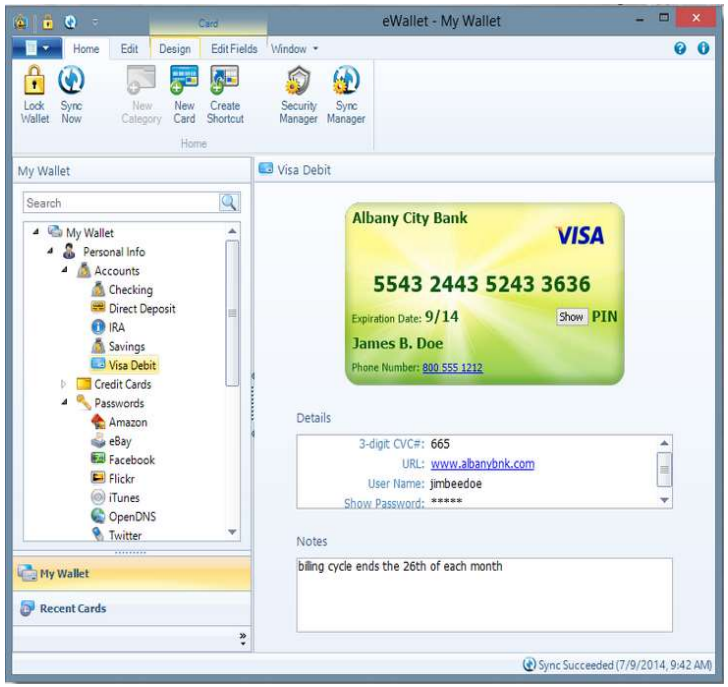
KeePass

KeePass este un soft de management a parolelor disponibil gratuit, pentru Microsoft Windows și versiuni neoficiale pentru Linux , MacOS , iOS, Android și Windows Phone. KeePass depozitează userame-urile, parolele și alte cîmpuri într-o bază de date criptată, protejată de o parolă și/sau file-cheie. Implicit baza de date este stocată local dar nu în cloud. Softul este dotat cu un generator de parole. Pentru criptare se utilizează algoritmii Advanced Encryption Standard (AES 256bit)



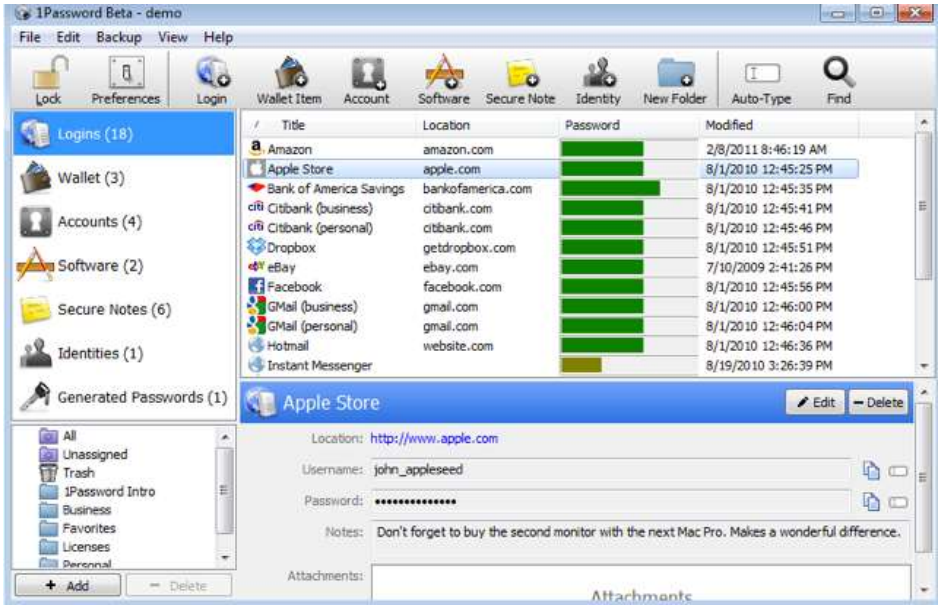
eWallet

eWallet este un produs al companiei Ilium Software. Softul permite stocarea informației confidențiale cum ar fi parole, username-uri, chei pentru produse soft ș.a. O trăsatură caracteristică a acestui soft este prezența șabloanelor pentru carduri credit ș.a. Deasemenea conținutul bazei de date poate fi sincronizat de pe diferite device-uri. Softul este dotat cu un generator de parole. Pentru criptarea informației se ultilizează algoritmul AES 256bit



1Password

1Password este este un manager de parole dezvoltat de AgileBits. Acest soft crează o bază de date protejată de o parolă-master, care servește ca parolă de acces la baza de date și ca cheie de criptare a informației, care se realizează prin algoritmul AES 128bit. 1Password poate crea o versiune mobilă a bazei de date în formă de html, un fișier care poate fi vizualizat în orice browser datorită funcției 1Password Anywhere. Pentru sporirea securității 1Password curățâ automat buffer-ul de schimb dacă în acesta a fost copiată o parolă, implicit acestă este timp de 90 de sec



RoboForm

Este un produs ce oferă stocarea informației confidențiale și completarea automată a formelor de autentificare pe web site-uri. Pot fi create mai multe “persoane”-seturi de date ce urmează a fi introduce pentru logare. Softul poate fi integrat cu Firefox, Netscape, SeaMonkey, Flock, Internet Explorer, Google Chrome, Maxthon ș.a. Pentru criptarea datelor se folosesc algoritmii AES, Blowfish, RC6, 3-DES, DES. La fel programul este dotat cu un generator de parole . Softul oferă posibilitatea de logare fără a folosi tastatura ceea ce prezinta un avantaj pentru securizarea datelor contra scurgerii lor prin intermediul keylogger-uri. Un dezavantaj al acestui program este codul închis ceea ce împiedică evaluarea obiectivă a algoritmilor de criptare a informației.

LastPass

LastPass este un produs disponibil în varianta free și premium a companiei LastPass. Aceasta este realizată în formă de plugin-uri pentru Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Maxthon și Apple Safari. Baza de date a informației este protejată de o parolă-master și este plasată local, avînd loc o sincronizare cu toate browserele . LastPass este dotat cu un generator de parole și poate crea un jurnal de evidență a autentificărilor pe unele site-uri