Securitate email

Problematica uzuala:

- Ce se incearca protejat
- Impotriva cui

Ce se urmareste:

- Confidentialitate – pe email se trimit informatii private
- Autenticitate – cine trimite email in realitate
- Anti-spam
- Phishing

Strategii generale:

- Criptarea continutului mesajului cu o cheie simetrica, utilizand o cheie de trafic generata aleator
- Utilizarea criptografiei cu chei publice pentru criptarea pentru toti beneficiarii
- Semnatura digitala a mesajului

Probleme securitate email

- Nu toate sistemele de mail accepta toate caracterele intr-un set de caractere dat
- Transformarile criptografice nu implica doar schimbari minore;
- Codificare: EBCEDIC – ASCII? Unicode? Tab – blank?
- Solutie: codificare intreg email in base64 utilizand caracterele acceptate de toate sistemele A-Z, a-z, 0-9, +, /;
- Base64 converteste 3 caractere necodate, ex ASCII in 4 caractere codate ASCII. Ca rezultat se obtine un overhead de 33%. Se remarca codificarea diferita functie de pozitia in grupul celor 3 octeri ce sunt codificati pentru a produce 4 caractere;
- Numai aceste caractere au importanta, orice altceva este sters la receptie inclusiv spatiile albe.

Signing

Semnatura:

- Daca se semneaza plaintext si apoi se cripteaza, identitatea transmitatorului este ascunsa tuturor exceptand adevaratii receptori
- Daca se semneaza textul criptat, un gateway poate verifica semnatura – una dintre cele mai bune merode anti-spam si anti-phishing.

Headere:

- Headerele sunt schimbate in tranzit
- Valorile campurilor in header sunt in formar ASCII si nu poate fi codat base64
- Exemplu evident: Received: se adauga cate o linie
- Mai putin evident: adresele de mail sunt de multe ori rescrise pentru ascunderea masinilor interne si prezentarea de adrese clare in exterior
- In consecinta headerele nu pot fi protejate prin scheme de securizare email.

Criptare email – S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) este un standard pentru criptarea cu cheie publica si semnarea mesajelor de mail incapsulate MIME.

- S/MIME furnizeaza urmatoarele servicii criptografice pentru aplicatiile de mesagerie electronica:
  - Autentificare
  - Integritatea mesajului si nerepudierea originii (utilizand semnaturi digitale)
  - Caracterul privat si securitatea datelor (utilizand criptare)

- O practica buna este de a utiliza chei private si certificatele asociate separate pentru semnatura si pentru criptare. Asa se permite pastrarea in siguranta a cheii de criptare fara a compromite proprietatea de nerepudiere a cheii de semnatura.

Probleme - S/MIME

- Nu tot software-ul email manipuleaza S/MIME. Pentru compatibilizare se atasaza un fisier (devine confuz).
- S/MIME nu este propriu pentru clientii webmail. Probleme in browser, practica de securitate cere ca cheia privata sa fie accesibila utilizatorului, dar inaccesibila serverului de webmail. Metoda de securizare cu semnatura webmail cere ca browserul sa execute cod pentru a produce semnatura (bresa de securitate).
- S/MIME sunt dimensionate pentru securitate end to end. Nu se va cripta numai mesajul ci si malware. Daca mesajul este scanat oriunde in afara de punctul final, malware va fi distribuit cu succes.
- Solutii:
  - Realizarea scanarii malware la statia terminala dupa decriptare;
  - Pastrarea cheii private pe gateway server a.i. decriptarea sa se poata face inainte de scanare la gateway (are dezavantajul ca oricine cu acces la gateway server poate citi mailuri ale altor utilizatori).
  - Utilizarea scanerelor de continut capabile sa certifice continutul mesajelor criptate

Criptare email - Pretty Good Privacy

- Pretty Good Privacy (PGP) este un program care realizeaza criptare si autentificare. El este adesea utilizat pentru semnarea, criptarea si descriptarea email pentru a creste securitatea.
- Criptarea PGP utilizeaza criptarea cu cheie publica si include un sistem care leaga cheia publica de nume utilizator si/sau adresa email.
- In implementarile recente a fost adaugat X.509 care utilizeaza o abordare ierarhica bazata pe autoritate de certificare.
- PGP suporta autentificarea mesajelor si verificarea integritatii pentru determinarea alterarii mesajului si a autentificarii transmitatorului prin semnatura digitala.
- Semnatura digitala este creata fie cu algoritm RSA fie DSA. PGP calculeaza o cheie hash de la plaintext si creaza o semnatura digitala utilizand cheia privata a transmitatorului.
- PGP include un mod de revocare a certificatelor si suporta data expirare certificat.
- Calitatea securizarii. PGP este considerat unul dintre mecanismele sigure. Pe masura ce au fost descoperite vulnerabilitati acestea au fost remediate.

Criptare email - ID based

- ID-based cryptography (sau Identity-Based Encryption (IBE) sau identity-based cryptography) este un tip de criptografie cu cheie publica in care cheia publica a unui utilizator este o informatie unica despre identitatea sa (de ex. adresa email, numele sau numele domeniului sau adresa IP).
- Prima implementare bazata pe adresa de mail PKI introdusa de Adi Shamir si permite utilizatorilor sa verifice semnatura digitala utilizand numai o informatie publica (identificator utilizator).
- Identity-based systems permit oricarei parti sa genereze o cheie publica pornind de la o valoare a identitatii cunoscute ca un sir ASCII. O a treia parte, de incredere, numita si Private Key Generator (PKG), genereaza cheile private corespondente. Pentru operare PKG creaza master public key si pastreaza master private key corespunzatoare. Cu master public key orice parte poate calcula o cheie publica corespunzand identitatii (ID) prin combinarea master public key cu valoarea ID. Pentru a obtine o cheie privata corespondenta partea autorizata sa utilizeze identitatea ID contacteaza PKG care utilizeaza master private key pentru generarea cheii private pentru identitatea data ID.
- Ca rezultat partile pot cripta mesaje sau verifica identitati fara o distributie prealabila a cheilor intre diversi participanti individuali.

Criptare email - ID based

Avantaje:

- Numar finit de utilizatori, dupa ce toti utilizatorii au primit chei secretul de terta parte poate fi distrus
- IBE elimina necesitatea infrastructurii de distributie a cheilor publice
- Facilitati interesante prin posibilitatea de codificare a informatiilor aditionale (data de expirare mesaj, timestamp). Datele incapsulate in ID sunt similare cu deschiderea unui nou canal intre transmitator si PKG cu autenticitate garantata.

Dezavantaje:

- Deoarece PKG genereaza chei private pentru utilizatori el poate decripta si/sau semna orice mesaj fara autorizare
- Datorita abordarii centralizate pentru PKG, criptografia IB nu este utilizabila in super-retele
- Necesita un canal sigur intre utilizator si PKG pentru transmiterea cheii private la intrarea in sistem. O solutie fezabila este o conexiune SSL.

Phishing

Definitie: Este un proces fraudulos prin care se incearca obtinerea de informatii sensibile cum sunt: nume utilizatori, parole si informatii detaliate pentru carti de credit prin deghizarea ca o entitate de incredere intr-o comunicatie electronica.

- Falsifica transmitatorul e-mail ca fiind de la o institutie financiara sau de la web site-uri cunoscute.
- Redirecteaza utilizatorii pentru introducerea de detalii pe un site pirat care arata aproape identic cu cel original
- De regula cere intreruperea legaturii active, daca aceasta exista, si revalidarea contului
- Chiar cand se utilizeaza autentificarea, utilizatorul trebuie sa fie experimentat pentru a detecta ca site-ul este fals
- Adesea pretinde ca a fost suspendat contul si cere reintroducerea datelor
- Este un exemplu de tehnica de manipulare pentru a pacali utilizatorii si a exploata cunostintele precare in securitate web

Phishing

Tehnici pe care se bazeaza:

- Social Engineering (Manipulare sociologica) – bazata pe reactia oamenilor la lucruri ce au importanta pentru ei. Subiectele genereaza panica si cer actiune imediata "to restore access to your bank account"
- Link manipulation – utilizarea unor forme prin care se creaza un link in email la un site web falsificat.
- Filter evasion – Atacatorii utilizeaza imagini in loc de text pentru a face dificila detectarea atacului de filtrele anti-phishing.
- Website forgery – utilizare de JavaScript pentru alterare continut bara de adrese, utilizare de cross-site scripting, man-in-the-middle. Se poate utiliza si Flash.
- Phone phishing – atac ce nu necesita in site fals. Mesajul care aparent vine de la banca cere utilizatorilor sa sune la un numar pentru problemele relative la cont. Se invita utilizatorul sa introduca contul si pinul. Voice phishing (Vishing) poate utiliza un caller ID fals pentru a crea aparenta apelului de la o organizatie de incredere.

Combatere phishing

- Social responses – pregatirea populatiei pentru a recunoaste atentatele phishing. In 2004, intr-un experiment cu un astfel de atac, 80% dintre studentii uneia dintre academiile militare a raspuns cu date personale. Este necesara certificarea in prealabil fara a introduce date.

- Technical responses – implementarea de masuri de combatere in browsere. Printre masuri se pot enumera: utilizarea SSL pentru autentificare server, utilizarea autoritatilor de certificare, includerea de filtre anti phishing, introducerea de parole numai arunci cand se justifica (ex, la Bank of America se cere utilizatorului sa introduca parola numai dupa ce banca a afisat o imagine proprie utilizatorului).

- Legal responses – adaptarea legislatiei la conditiile actuale de utilizare IT.