

-- Domande per argomento ==

Velocità di cifratura

Proprietà teoriche di sicurezza

TCP SYN flooding

risp: SYN Cookie (djb) implementato su Linux e Solaris

- spiegare meccanismo di pagamento nel commercio elettronico
- One time password: spiegare il concetto. Che attacco elimina? --> sniffing.

Hash per calcolare la password partendo da un seme.

Autenticazione Accesso in Rete

- autenticazione per accesso in rete, radius, ...
- EAP: a cosa serve, differenze rispetto a PAP e CHAP. --> EAP È un framework, permette di avere sotto qualsiasi canale.
- (Aime) Radius e quando si usa nelle reti wireless. Problemi di sicurezza in una piccola rete aziendale: che tecnologie adottare?

IPsec

- cos'È e quali servizi di sicurezza offre; proprietà (sempre - mai - opzionalmente) su: autenticazione del server, del client, autenticità dei dati, non ripudio (mai), protezione da replay, cancellazione
- (Aime) Ipsec...
- Funzionalità di sicurezza offerte da Ipsec. Cosa autentica? Come si fa l'autenticazione dei dati?

Firewall

- dove si può piazzare in una grossa rete aziendale?
risp: tra reti a livelli di sicurezza diversi
- classificazioni livelli dei firewall e controlli da fare a ogni livello; differenza packet filter e proxy di circuito (fa controlli sul sequence number, x' meno potente di qlo a livello applicativo)
- dove vanno messi e che funzioni hanno ai vari livelli?
- Architettura dei firewall (con schema), eventuali miglioramenti.

IDS

- attivo (contro: falsi allarmi e non riconosce tutti gli attacchi, perché si basa su statistiche)
 - passivo (pro: riconosce solo attacchi certi, amministratore non deve cambiare la configurazione; contro: È sempre in ritardo: prima si scoprono gli attacchi e poi li riconosce)
 - rete
 - host (controlla traffico CPU, pacchetti che girano,...)
 - Cos'È IDS? Controlla l'utente? Che dati guarda? Meglio host, net, entrambi?
- Fare schema. Come si fa a fare partire? Bisogna impostare dei parametri? Es. 5 processi che girano su un host, come si fa a capire se c'È un attacco? (dipende se È statico o dinamico --> dire pro e contro).

SSL/TLS

- Parlare di SSL. Come si fa autenticazione del server? Se manda certificato qcn puó copiarlo: come si verifica associazione chiave pubblica - server
- giusto? --> si manda una sfida.

X.509

- certificati X.509, attributi (obbligatoriosi o no), ...
- revoca dei certificati X.509, da chi È richiesta (utente o CA), cosa succede se ti rubano il certificato? (mi sono persa la risposta...)
- CRL
- (Aime) Certificato X.509, campi e loro scopo. Revoca. Come si usano le info del certificato? CRL... Come si verifica una firma digitale?
- Revoca certificato: in cosa consiste e perchÈ si deve fare? Chi lo chiede?
- Come si invalida un certificato? Chi garantisce affidabilit  della CRL?

Firma digitale

- cos'È e quali sono le propriet  (risp: autenticit  dei dati, non ripudio, integrit ); se tolgo digest quali rimangono? (risp: tutte, perchÈ serve solo a non dover cifrare tutto il documento)
- differenza tra firma digitale (integrit  e autenticazione) e firma autografa (solo autenticazione)
- Parlare della firma digitale; confronto con firma autografa.

Posta elettronica

- sicurezza a livello di messaggi
- sicurezza della posta elettronica e S-MIME; attributi di sicurezza (qli di prima)
- tipi di messaggio (firmato, cifrato, firmato e cifrato, in chiaro + firma --> qto È leggibile anche da chi non ha SMIME)
- problema dello spamming di posta elettronica: cos'È e come si evita (usare canale sicuro, SMTPS)

-- Domande per sessione d'esame ==

5 minuti per due domande scritte (totale 10 punti, +0.5 giusta, -0.5 sbagliata, 0 non data):

- 1 - confrontare velocit  di cifratura simmetrica - asimmetrica - digest - digest con chiave (matrice in cui mettere +, -, =).
- 2 - propriet  teoriche della sicurezza: dire per cosa sono verificate (sempre - mai - opzionalmente).

Federica 8.50 - 9.00

1 - parlare del firewall; dove si può piazzare in una grossa rete aziendale?

(risp: tra reti a livelli di sicurezza diversi)

2 - firma digitale: cos'è e quali sono le proprietà (risp: autenticità dei dati, non ripudio, integrità); se tolgo digest quali rimangono? (risp: tutte,

perché serve solo a non dover cifrare tutto il documento).

Tizio di mondovì 9.05 - 9.15

1 - classificazioni livelli dei firewall e controlli da fare a ogni livello;

differenza packet filter e proxy di circuito (fa controlli sul sequence number, xú meno potente di qlo a livello applicativo)

2 - Syn attack e metodi per contenerli (non tenere la tabella in memoria, usato da SO Linux e Solaris).

Massari 9.20 - 9.40

1 - IDS: attivo (contro: falsi allarmi e non riconosce tutti gli attacchi, perché si basa su statistiche) - passivo (pro: riconosce solo attacchi certi,

amministratore non deve cambiare la configurazione; contro: È sempre in ritardo: prima si scoprono gli attacchi e poi li riconosce), livello rete - host (controlla traffico CPU, pacchetti che girano,...)

2 - posta elettronica sicura a livello di messaggi

3 - (perché era indeciso sul voto) differenza tra firma digitale (integrità e autenticazione) e firma autografa (solo autenticazione)

Paolo 9.43 - 10.10

1 - IPsec: cos'è e quali servizi di sicurezza offre; proprietà (sempre - mai - opzionalmente) su: autenticazione del server, del client, autenticità dei dati, non ripudio (mai), protezione da reply, cancellazione

2 - sicurezza della posta elettronica (visto che qlo di prima non l'aveva saputo) e S-MIME; attributi di sicurezza (qli di prima); tipi di mex (firmato,

cifrato, firmato e cifrato, in chiaro + firma --> qto È leggibile anche da chi non ha SMIME)

Sconosciuto 10.13 - 10.30

1 - problema dello spamming di posta elettronica: cos'è e come si evita (usare canale sicuro, SMTPS)

2 - spiegare meccanismo di pagamento nel commercio elettronico

3 - certificati X.509, attributi (obbligatori o no), ...

Simone 10.33 - 10.50

1 - revoca dei certificati X.509, da chi È richiesta (utente o CA), cosa succede se ti rubano il certificato? (mi sono persa la risposta...)

2 - CRL

3 - autenticazione per accesso in rete, radius, ...

Amico di Silvio

- 1 - Firewall: dove vanno messi e che funzioni hanno ai vari livelli?
 - 2 - Parlare della firma digitale; confronto con firma autografa.
 - 3 - Cos'è IDS? Controlla l'utente? Che dati guarda? Meglio host, net, entrambi?
- Fare schema. Come si fa a fare partire? Bisogna impostare dei parametri?
Es. 5 processi che girano su un host, come si fa a capire se c'è un attacco?
(dipende se è statico o dinamico --> dire pro e contro).

Regis

- 1 -(Aime) Certificato X.509, campi e loro scopo. Revoca. Come si usano le info del certificato? CRL... Come si verifica una firma digitale?
- 2 - Parlare di SSL. Come si fa autenticazione del server? Se manda certificato
qcn può copiarlo: come si verifica associazione chiave pubblica - server giusto? --> si manda una sfida.
- 3 - EAP: a cosa serve, differenze rispetto a PAP e CHAP. --> EAP è un framework,
permette di avere sotto qualsiasi canale.

Scavarda

- 1 - Architettura dei firewall (con schema), eventuali miglioramenti.
- 2 - One time password: spiegare il concetto. Che attacco elimina? --> sniffing.
Hash per calcolare la password partendo da un seme.
- 3 -(Aime) Ipsec...

Simone

- 1 - Revoca certificato: in cosa consiste e perché si deve fare? Chi lo chiede?
Come si invalida un certificato? Chi garantisce affidabilità della CRL?
- 2 - Funzionalità di sicurezza offerte da Ipsec. Cosa autentica? Come si fa l'autenticazione dei dati?
- 3 -(Aime) Radius e quando si usa nelle reti wireless. Problemi di sicurezza in una piccola rete aziendale: che tecnologie adottare?

--- DA AGGIUNGERE ---

1) Funzionamento del PGP seguito da una domanda di rara stupidità del tipo "Ma perché alla gente non piace? (la risposta corretta a quest'ultima domanda era del tipo: "Perché usa i certificati")"

2) Poi gli ha chiesto Diffie seguito dalla solita domanda stronzina di rito del tipo "Perché viene preferito a RSA?" . La risposta corretta è "Perché lo usa l'esercito"

DOMANDE LIOY VENERDI' - SCRITTO:

[tre domande per il primo turno (A), tre per il secondo (B)]

1A)

quali algoritmi si possono usare per scambiare chiavi segrete?

DES, AES, DSA, ... no

DH, RSA, OOB, ... sÌ

1B)

quali algoritmi si possono usare per comunicare una certa chiave segreta a una controparte?

DES, AES, DSA, DH ... no

DH, RSA, OOB, ... sÌ

NdApi: DH puro serve per concordare una chiave, non per comunicare una chiave giÙ scelta, ma È possibile concordare una chiave K1 con cui cifrare la la chiave scelta per mandarla al partner.

2A)

proprietÙ di sicurezza di IPsec (mai, sempre, parziale)
(lista)

2B)

proprietÙ di sicurezza di SSL (mai, sempre, opzionale)
(lista) non me le ricordo...

3A e 3B)

differenze e somiglianze tra packet filter e circuit gateway? da quali attacchi difendono?

DOMANDE LIOY VENERDI' - ORALI:

[non le ho segnate tutte...]

- PGP: perchÈ non si È diffuso? (non usa certificati, scambio chiavi OOB ai party!)

- da cosa protegge il circuit gateway? (da attacchi sulle intestazioni TCP/IP, SYN, flag, seq num...)

- Spam: cause? rimedi? (Open Mail Relay, autenticazione con SMTP-Auth e/o SSL)

- Posta elettronica sicura: formati dei messaggi? differenze? (signed, clear-signed, ecc.)

- lunghezza delle chiavi simmetriche: trade-off? (prestazioni, valore del segreto, DES 56 bit scarso,...)

- SET: schema e funzionamento, si usa? perchÈ? (no perchÈ il SET wallet da installare richiede supporto e assistenza agli utenti, usare browser...)

- voglio autenticazione, integritÙ, velocitÙ e NON non-ripudio? (keyed-digest, perchÈ... schema)

- IPsec: SA, IKE?

- SSL: come È trattato il messaggio? (record, MAC, ...)

- SSL: scambio messaggi? (schema generale, senza dettagli di ogni singolo messaggio, importante dire che i certificati, se presentati, sono controllati con una sfida!)

- Commercio elettronico...

- WEP: cosa avrebbe dovuto garantire? perchÈ non lo garantisce? cosa hanno fatto per risolvere il problema? (attacchi a WEP, nuovi algoritmi, ...)

- PAP, CHAP, EAP: varie...

- RADIUS: dove si usa, come funziona...
- Revoca dei certificati X.509: meccanismi...
- e molte molte altre...

- shadow server
- protezione della mail
- tipi di vpn
- denial of service: esempio e come combatterlo
- diffie-hellman

- per le seguenti tecnologie dire cosa offrono
 - . identificazione
 - . segretezza
 - . etc

- per i seguenti algoritmi dire per cosa sono utili
 - . firma
 - . crittaz dati
 - . hash

1. Spiegare lo shadow server attack, come può essere messo in atto e quali possono essere le contromisure.
2. Spiegare il concetto di Basic VPN, i suoi vantaggi e svantaggi, i suoi problemi critici e le possibili contromisure.
3. Descrivere l'HMAC, senza entrare nei dettagli degli algoritmi e le proprietà di sicurezza che offre.
4. Un client vuole scaricare le mail dal MS. Quali sono i rischi di questa interazione e quali tecniche possono essere utilizzate per la sicurezza sia lato client che lato server?
5. Descrivere il canale TLS, quali sono le proprietà di sicurezza offerte, quali sono gli algoritmi di crittografia e se questi sono opzionali o obbligatori, quante sono le chiavi utilizzate e come vengono gestite.