UNIT - V

E-Mail, IP & Web - security

E-mail security : - (2)

Security services for E-mail attacks possible through email - (2)

- (3)

Establishing keys & Privacy - (4)

Authentication of the source - (6)

Message Integrity - (8)

Non-repudiation - (9)

Pretty Good Privacy - (10)

S/MIME - (15)

IP Security: overview of IPsec - (17)

IP and IPv6, Authentication Header - (21)

Encapsulation Security Payload ESP - (24) (26)

Internet key Exchange (Phases of IKE, ISAKMP/IKE Encoding) - (27) (29)

Web security: SSL/TLS Basic Protocol - (31)

computing the keys - (35)

client authentication - (36)

PKI as deployed by SSL - (36)

Attacks fixed in V3 - (35)

Email attacks
Possible through email — (2)
— (3)
key & Privacy — (4)
Authentication of the source — (6)
Message Integrity — (8)
Non-repudiation — (9)
Pretty Good Privacy — (10)
S/MIME — (15)
IP Security: overview of IPsec — (17)
IP and IPv6, Authentication Header — (21)
Encapsulation Security Payload ESP (24) — (26)
Internet key Exchange (Phases of IKE, ISAKMP/IKE Encoding) (29) — (27)
Web security: SSL/TLS Basic Protocol — (31)
computing the keys — (35)
client authentication — (36)
PKI as deployed by SSL — (36)
Attacks fixed in V3
Exportability — (38) Encoding — (39)
SET — (40)

UNIT-V

E-mail, IP and web-Security

E-mail Security : Security services for E-mail:-

*. For Security, some features are vided for the electronic mail systems, are as follows;

* Privacy
* Authentication
* Integrity
* Non-repudiation
* Proof of submission
* Proof-of-delivery
* Msg flow of confidentiality
* Anonymity
* Containment
* Audit
* Accounting
* Self-destruct
* Msg sequence integrity.

Attacks possible through E-mail :-

* E-mail hacking is the illegal access to (or) manipulation of an E-mail account

  * SPAM
  * VIRUS
  * PHISHING

SPAM :-

* Spam is created by attackers who send bulk E-mail.

* Spammers attempt to find new ways around the increased legislation and policies governing unsolicited emails.

VIRUS :-

* A virus incorporates email as a means of transportation. This type of virus is called a warm - the sobig virus is an example.

* This virus creates a spamming framework by taking over unwilling participating PCs.

PHISHING:-

* It is a type of attack that involves e-mails that appear to be from legitimate businesses that we usa associated with.

* Phishing msgs look authentic, with all the corporate logos & formats similar to that of official emails.

> An account no
> A pwd (or)
> A date-of-birth.

Establishing keys privacy:-

Establishing keys:-

* Security services are provided by cryptography requires keys.

Establishing secret keys:-

* Two parties establish a shared secret key for e-mail in some other means of private comm.

Privacy:-

*. Electronic mail is private but there are many ways to read that msgs.

End-to-End Privacy:-

*. Alice want to send a msg to Bob that only Bob can read it. She can't depend on the nlw keeping the msg secret, but she can ensure that nobody but Bob can read the msg by using cryptography to encrypt the message.

Privacy with Distribution List Exploders:-

*. If Alice is sending a msg to a distribution list which will be remotely Exploded, and Bob is only one of the receipenents.

> Local exploding requires diff mechanisms.

> Alice has to trust the maintainer of the mailing list, since a may insert extra names into the distribution list.

Authentication of the Source

* In an unsecured mail system, it is possible for Carol to send a msg to Bob where the FROM field says Alice.

*. This cause great harm if Bob takes the msg seriously.

Source Authentication based on public-key technology:-

*. Bob knows Alice's public-key, Alice digitally sign the msg, using her private key, which will assure Bob that Alice wrote the msg.

*. ~~the~~ Alice compute a hash of the msg & then to sign the msg digest, since computing a msg digest.

*. Since, computing a msg digest is faster than public key opns and the msg digest is usually a smaller quantity to sign than the msg.

Source Authentication based on secret keys:

(4)

MIC (or) MAC :- [Message Integrity Code]

* the MAC is the CBC residue of the msg compuled with the shared secret key.

* the MAC is the msg digest of the shared secret appended tot eh msg.

* the MAC is the encypted msg digest, where the 128-bit msg digest is encypted with the shared secret key, for instance in ECB (or) CBC mode

Source Authentication with Distribution list

> Source Authentication is easy with public keys and distribution lists.

> Source Authentication is complicated with secret keys.

> Using mail explodeus & secret-key technology.

Message Integrity

* Bob receives a msg from Alice, how does bob knows that carol did not intercept the msg & modify it ?

Message Integrity without source Authentication :-

* To provide msg integrity protection without source Authentication is possible ?

* the msg anonymous so there is no source verification.

Integrity protection :-

* To prevent someone from guessing that the first part of the msg was the proof that they were the kidnappers & substitute a diff second part of the msg, with diff duration for dropping off price money.

authentication by humans. No system provides this odd combination & due to such a small market that none is to be developed.

Non-Repudiation

Repudiation:-

* It is the act of denying that the particular person sent a msg.

Non-Repudiation:-

* If Alice sends a msg to Bob, Alice can't deny that the sent msg, Alice Bob prove to a third party that Alice send the msg.
* Non-repudiation based on public-key Technology.
* Plausible Deniability Based on Public-key Technology.
* Non-Repudiation with secret keys.

PRETTY GOOD PRIVACY [PGP]:-

(10)

* PGP is a secure mail protocol
* PGP performs encryption & integrity protection on files.

Process:- * one send a secure mail msg could first transform the file to be mailed using PGP & then mail the transformed file using traditional mailer.

Key distribution:-

* PGP uses public-key computation for personal keys.
* Public keys certifications and certificate chains verifications are done b/w PGP, PEM, S/MIME.
* PGP Assumes Apathy.
* With PGP, each user decides which keys to trust.

Efficient Encoding:-

* PEM
* PGP.