

#Spams Définition: envoi de masse et falsification du courrier électronique. Objectifs directs:

- Publicité, Fraude, intrusion de malware, phishing Dégâts indirects:
- surcharge de serveur
- admin de la messagerie est inondé de message d'erreur pour des adresses invalides
- le fournisseur internet peut couper la ligne, le serveur se fait placer sur liste noire ##Prévention du spam
- ne pas l'afficher, ne pas la transmettre, Filtre sur les serveurs sur la base des listes noires
- configurer les serveurs correctement #Messagerie électronique
- SMTP : sert à envoyer des messages, POP et IMAP servent à rapatrier des messages pour leur lecture
- POP: récupère le courrier en local, IMAP: permet de consulter les mails sur un serveur, laisse les messages sur le serveur. ##attaque par e-mails forgés falsification du courrier électronique en exploitant une faille conceptuelle de SMTP qui ne vérifie pas les sources. Informations fiables dans un e-mail:
- Fiables : champ Received, champ Return-Path, champ Delivered-to
- normalement fiable: peut-être forgé

#Attaques logicielles une fois qu'un programme est distribué, il peut-être soumis à toutes sortes d'attaques

- analyse: extraction d'algorithme, architecture
- modifie ou réutilise le logiciel
- distribue un programme modifié la protection logicielle inclut:
- développement sécurisé
- éviter de pouvoir insérer du code malveillant
- éviter de contourner les protections
- éviter les vols de code ##Manipulation mémoire
- écriture ou lecture en mémoire à un endroit non autorisé, buffer overflows
- un entier mal interprété, une chaîne est mal formée et interprétée de manière inattendue

Le buffer overflow est un bug qui permet d'écrire à l'extérieur de l'espace alloué au tampon en écrasant les données écrites à l'emplacement. Un shellcode est une suite d'instructions destinée à être injectée puis exécutée. ##Organisation mémoire La mémoire est organisée en segments.

- Stack stockage dynamique, Heap allocation de mémoire, .bss données globales initialisées
- .data données globales non-initialisées
- .text code exéc L'ESP (stack pointer) pointe l'adresse basse mémoire qui le top de la pile. L'EBP est l'endroit où est stockée la base de la pile L'EIP pointeur d'instruction.

 org\_mem

Lors d'un saut dans une fonction, un saut est effectué. Dès lors on doit sauver l'environnement.

l'appelant :


- pousse les paramètres (de droite à gauche).
- appelle la fonction
  - sauve l'adresse de retour dans EIP
  - saute à l'adresse de la fonction
- appelé
  - sauve et initialise EBP

- exécute son code
- recharge l'adresse de retour
- appelant :
  - restaure le stack pointer ##Différentes attaques
- stack smash: les variables sont écrasées
- stack off-by-one: dépassement d'un seul caractère
- heap overflow: les variables sur le heap sont manipulées
- integer overflow: entiers dépassant la taille
- format string bug: mauvaise interprétation d'un string ##Protection rendre la stack et le heap non exécutable, utilisation de canaris, randomisation des adresse mémoire librairies sécurisées

##Introduction à la cryptographie La cryptographie apporte confidentialité, authenticité et intégrité. De même que la non-répudiation, l'anti-clonage. La cryptographie étudie les codes secrets qui permet d'envoyer de l'information de manière confidentielle.

- Un Cipher est un algorithme permettant de rendre l'information confidentielle en général à clé secrète. .
- Un Pk est algorithme de chiffrement et déchiffrement à clé publique. La théorie du codage est la science qui permet d'envoyer de l'information de manière fiable et efficace.
- Le code est un système de symboles représentant de l'information. La stéganographie est l'art de dissimuler une information en la cachant, mais en ne transformant pas son contenu. La cryptographie symétrique utilise une clé secrète pour chiffrer et déchiffrer l'information. Elle utilise la même clé est requise pour le chiffrement et le déchiffrement. Pas de notion d'authentification de l'origine.
- Exemple: DES(Block ciphers), AES(Block ciphers), RC4 La cryptographie à clé publique génère une paire de clé. Une clé publique pour chiffrer le message et une clé privée pour déchiffrer le message. Chaque utilisateur possède une paire. Pas de secret partagé entre les deux utilisateurs.
- Exemple: RSA(Stream ciphers)

Le scytale pratique le chiffrement par transposition. Le chiffre de César remplace chaque lettre K lettre après elle. Le chiffrement de Vigenère propose l'idée de chiffrer via plusieurs caractères. Mais ces solutions sont rapidement cassée par la force brute ou l'études des fréquences des lettres. ##Les principes de Kerckhoffs

- la confidentialité du message doit reposer sur la confidentialité de la clé uniquement
- On ne fait pas reposer la sécurité sur la confidentialité de l'algorithme Vernam cipher utilise une clé aléatoire uniformément distribuée, pour ne pas pouvoir déduire des informations du texte, et de même taille que le message. On effectue un ou exclusif entre les deux pour chiffrer et déchiffrer. Il offre un chiffrement parfait mais il est inutilisable. La confidentialité parfaite signifie qu'on ne peut pas apprendre quelque chose sur le cipher text si on connaît le plain text est vice versa. blockvsStream

#DES Le Data Encryption standard est basé sur Lucifer et influencé par la NSA. C'est un block cipher qui chiffre par block de 64 bits. Il utilise des clés de 56 bits voir 64 bits. L'algorithme fonctionne dans un premier temps par une permutation des blocs. Puis vient le chiffrement par ronde. Seize tours sont effectué avec chaque fois une clé différente. lors de chaque tour le block est divisé en deux et permuter selon un schéma feistel. pour finir une permutation inverse à celle effectuée dans le premier temps est faite. DES possède des faiblesse connues. Et la recherche de clé est possible. Des Variantes TDES sont possibles mais trop lente.

#Mode de chiffrement L'Electronic code book chiffre chaque block indépendamment. Le Cipher block chaining utilise la partie chiffrée du block précédent pour chiffré l'actuel block. #Diffie-Hellman La distribution de clé est toujours un problème. Pour résoudre ce problème, On utilise des fonctions difficilement réversible.

diffiePNG

#RSA La paire de clé privée/publique dépendent mathématiquement l'une de l'autre. Tout le monde peut accéder à la clé publique mais personne peut accéder à la clé privée. RSA est sûr car la factorisation est un problème difficile. #Fonction de hachage Un message qui a passé par une fonction de hachage est appelé digest. Elles sont résistantes aux collisions, car il est infaisable de trouver deux messages avec le même haché. Elles sont résistantes aux préimages. Utilisations:

- Engagement / preuve pour caractériser un message de manière unique.
- extension de domaine en longueur fixe
- génération de nombre pseudo aléatoire à partir d'une graine
- exemple MD et SHA ##Modèle de Merkle-Damgard Les fonctions de compression sont un mélange de transpositions, de décalages, de substitutions, xor. Lors du découpage en bloc, il y a toujours un padding.

#Authentification de données MAC et signature MAC est un code de taille fixe qui est envoyé avec un message pour prouver son intégrité et une origine. Exemple: pour authentifier les messages Diffie-Hellman. ISO/IEC 9797 est une meilleure variante. Une signature évite toute répudiation de la source. Elle permet de s'assurer de la provenance, de le prouver, de prouver la livraison et de garantir l'intégrité des données. RSA et DSA permettent de signer.

#Authentification Facteurs d'authentification: l'authentification forte utilise au moins deux types de facteurs.

- ce que l'on sait, ce que l'on possède, ce que l'on est Types d'authentification:
- Par jeton passif fixe dans le temps: mot de passe, badge magnétique
- Par jeton actif changeant dans le temps: liste à biffer, SecureID.
- Par question réponse: fonctionnement asynchrone
- Par la biométrie
- Par un autre canal

#infrastructure à clé publique Un certificat est un lien entre une entité et une clé publique. Ce lien est certifié par une autorité tierce. Il est de type fichier texte de taille d'environ 1KB. Il n'y a plus besoin de connaître son interlocuteur ni de lui faire confiance.

- CA : « Certificate Authority »
- émettre, renouveler et maintenir les certificats
- RA : « Registration Authority »
- gérer les demandes
- VA : « Validation Authority »
- service de contrôle des certificats
- CPS : « Certification Practice Statement »
- CP : « Certificate Policy »