Sécurité Logicielle

LAURENT NANA

Plan

- Introduction
- Concepts généraux de la sécurité logicielle
- Messagerie électronique et protocoles de messagerie sécurisés
- Maliciels
- Vulnérabilités des applications et des réseaux/Internet

Introduction (1/2)

- La *sécurité logicielle* concerne les *mécanismes liés aux malveillances logicielles*
- Un système est *vulnérable* à une *action malveillante* si celle-ci *peut se réaliser avec succès* contre ledit système
- La *sécurité* peut être définie comme la propriété d'un système visant à assurer sa *disponibilité*, son *intégrité* et sa *confidentialité*
- La *disponibilité* d'une ressource : *période* de temps *pendant laquelle* le *service* qu'elle offre est *opérationnel*

Introduction (2/2)

- L'*intégrité* d'une ressource est relative au fait qu'elle reste intacte, *non détruite ou modifiée sans l'autorisation de son propriétaire*
- La *confidentialité* d'une donnée ou d'un système est liée à la notion de *maintien du secret*, c'est à dire l'*accès* à la donnée ou au système *uniquement par la (les) personne(s) autorisée(s).*
- L'*objectif de la sécurité d'un système* est de *réduire les risques de sécurité liés à l'utilisation de ce système*, voire de les éliminer.

Concepts généraux

- Principaux types de mécanismes de la sécurité logicielle
- Menaces des (ou actions malveillantes contre les) systèmes
- Conséquences des menaces
- Résorption des vulnérabilités

Principaux types de mécanismes de la sécurité logicielle

- Mécanismes de détection d'actions de malveillance logicielle
- Mécanismes de protection contre les malveillances logicielles
- Mécanismes de défense contre les malveillances logicielles
- Mécanismes de résilience des systèmes contre les malveillances logicielles.

Menaces ou actions malveillantes contre les systèmes

- Atteinte à la disponibilité des systèmes et des données
- Destruction, corruption ou falsification des données
- Vol ou espionnage des données
- Utilisation illicite d'un système
- Utilisation d'un système compromis pour attaquer d'autres cibles

Conséquences des menaces

- Coûts humains et financiers
- Risques de
  - Perte de données sensibles
  - Indisponibilité des infrastructures et des données
  - Dommages pour le patrimoine intellectuel et la notoriété
- Risque = préjudice x probabilité d'occurrence

Résorption des vulnérabilités (1/2)

- Définir les risques et les objets à protéger
- Identifier et authentifier les accès
- Empêcher les intrusions
- Concevoir la défense en profondeur
- Aspects organisationnels de la sécurité
- Veille auprès des CERT (Computer Emergency Response Time)
- Failles de sécurité

Résorption des vulnérabilités (2/2)

- Systèmes de management de la sécurité de l'information (SMSI)
- Norme ISO 27001
- Projet de certification de sécurité Open Source OSSTMM

Résorption des vulnérabilités
Définir les risques et les objets à protéger

- Fixer un périmètre de sécurité : qu'est-ce qui est à protéger ?
- Elaborer une politique de sécurité : qu'est-ce qui est autorisé/ interdit ?
- Classer les ressources (données/programmes) en catégories publiques/privées => gestion conséquente des droits d'accès

Résorption des vulnérabilités
Identifier et authentifier les accès

- Authentification des accès aux ressources privées
- Vérification des droits d'accès par rapport aux habilitations données
- Nécessité de chiffrement des données notamment d'authentification en cas de transmission via le réseau
- Chiffrer et authentifier vont de pair (protection contre des usurpations d'identité, …)

Résorption des vulnérabilités
Empêcher les intrusions

- Intrusions visant à corrompre ou à rendre inaccessibles les données.
- Utilisation d'un *pare-feu* (firewall) et du *filtrage* de communications réseau
- Mise en place de zones démilitarisées (DMZ).
- Utilisation de Systèmes de détection d'intrusions (IDS) et de Systèmes de Prévention d'Intrusions (IPS)

Résorption des vulnérabilités
Concevoir la défense en profondeur

- Il s'agit d'envisager que l'attaquant puisse franchir la ligne de défense sans qu'il devienne impossible de l'arrêter.
- Nécessaire à cause de la difficulté de délimiter de façon pérenne le périmètre de sécurité, notamment du fait des évolutions technologiques qui amènent à considérer que le succès de la prévention ne peut plus être garanti.
- Prévoir les moyens de limiter les conséquences d'une attaque réussie qui se produira forcément un jour.

Résorption des vulnérabilités
Aspects organisationnels de la sécurité

- Prendre en compte le comportement humain et social : les moyens techniques de sécurité doivent être adaptés pour l'humain. Le dispositif technique de sécurité ne suffit pas à lui tout seul
- Ne laisser aucun utilisateur du système avec un accès incontrôlé au réseau
- Vérifier les dispositifs de sécurité : s'assurer qu'ils sont opérationnels et que ceux en charge de leur mise en œuvre le seront également en cas de sinistre (utilisation de simulations, …).

Résorption des vulnérabilités
Veille auprès des CERT (1/2)

- CERT = Computer Emergency Response Time
- Les CERT vérifient et publient les alertes relatives à la sécurité des ordinateurs (vulnérabilités récemment découvertes, etc.)
- Les alertes émanent des éditeurs de logiciels ou d'utilisateurs
- La publication des alertes incite les producteurs de systèmes logiciels à la correction des vulnérabilités.

Résorption des vulnérabilités
Veille auprès des CERT (2/2)

- Plusieurs organismes de CERT
- 1er CERT créé en 1988 à l'université de Carnegie Mellon, USA
- CERTA créé pour les administrations et services publics en France (supervisé par l'ANSSI),
- CERT Renater pour les universités et organismes de recherches en France,
- CERT-IST pour le monde industriel en France, …

Résorption des vulnérabilités
Failles de sécurité

- L'attaquant essaye souvent de repérer et d'exploiter les failles
- Différents types de failles:
  - Failles de conception : algorithme inapproprié ou faux, formule de calcul fausse, …
  - Failles d'implémentation : erreurs de programmation conduisant par exemple à un débordement de zone mémoire, …
  - Faille « zéro-day » : faille de sécurité inconnue ou non corrigée
- Meilleure protection face aux failles de logiciels : capacité de riposte rapide, commençant très souvent par une désactivation du composant mis en défaut par l'attaque.

Résorption des vulnérabilités
Systèmes de management de la sécurité de l'information

- But : maintenir et améliorer, en matière de sécurité de l'information, la position de l'organisme qui le met en œuvre
- ISO 27001: norme destinée aux SMSI
- ISO/IEC 15408:
  - Norme pour l'évaluation des propriétés de sécurité des produits et des systèmes de traitement de l'information.
  - Est parallèle à l'ISO 27001.
- Normalisation utile lorsque l'environnement de l'entreprise fait de la certification ISO 27001 une obligation légale ou en cas de relation contractuelle avec une entreprise requérant cette certification ou pour donner une valeur morale supérieure à un produit.

Résorption des vulnérabilités Norme ISO 27001 (1/2)

- 4 phases: Plan, Do, Check, Act
- Phase Plan : définir le champ du SMSI, identifier et évaluer les risques, produire le document (State Of Applicability, SOA) qui énumère les mesures de sécurité à appliquer
- Phase Do : affecter les ressources nécessaires, rédiger la documentation, former le personnel, appliquer les mesures décidées, identifier les risques résiduels

Résorption des vulnérabilités Norme ISO 27001 (2/2)

- Phase Check : audits et revues périodiques du SMSI, qui produisent des constats et permettent d'imaginer des corrections et des améliorations
- Phase Act : prendre les mesures qui permettent de réaliser les corrections et les améliorations dont l'opportunité a été mise en lumière par la phase Check, préparer une nouvelle itération de la phase Plan.

Résorption des vulnérabilités
Projet de certification de sécurité OSSTMM

- Institute for SECurity and Open Methodologies (ISECOM) : organisme de sécurité fondé en 2001 qui se proclame « ouvert »
- Elaboration d'un référentiel de mesures de sécurité et d'audit (méthodologie de vérification de la sécurité des systèmes), Open Source Security Testing Methodology Manual (OSSTMM) disponible en ligne.
- Ne permet pas d'avoir la garantie institutionnelle souvent recherchée telle que celle obtenue avec ISO 27001, car les auditeurs sont auto certifiés.

Plan

- ✓Introduction
- ✓Concepts généraux de la sécurité logicielle
- Messagerie électronique et protocoles de messagerie sécurisés
- Maliciels
- Vulnérabilités des applications et des réseaux/Internet

Messagerie électronique et protocoles de messagerie sécurisés

- Introduction
- Risques et besoins de sécurité
- Impératifs de sécurité et mesures de sécurité
- Protocoles de messagerie sécurisés
- Recommandations pour sécuriser un système de messagerie
- Exemples de courriers malveillants et de mesures de détection/ prévention
- Protocole SMTP
- Courrier électronique indésirable : SPAM ou pourriel

Introduction

- Les messages transmis par courriel circulent en général en clair sur le réseau
- Outil de travail et application critique pour les organisations
- Nécessité de prendre des dispositions adéquates pour la transmission d'informations confidentielles
- Nécessité d'avoir une messagerie disponible, fiable, performante et sûre.

Risques et besoins de sécurité (1/2)

- Perte, interception, altération ou destruction de messages
- Divulgation d'informations confidentielles
- Infection des systèmes par le biais de messages contenant des codes malveillants (virus, vers, Chevaux de Troie)
- Inondation de messages (spam, …)
- Usurpation d'identité, harcèlement des utilisateurs
- Refus de service par défection d'une composante du système de messagerie

Risques et besoins de sécurité (2/2)

- Répudiation (non reconnaissance de la réception/transmission d'un message par un acteur du système)
- Risques liés aux réseaux (attaque au niveau du routage, des serveurs de noms, …).

Impératifs de sécurité

- Confidentialité et intégrité des messages
- Non-répudiation (preuve de l'émission, preuve de la réception, signature, certification de messages)
- Authentification de l'identité de tous les acteurs du système de messagerie (utilisateurs, ATM, …)

Mesures de sécurité

- Installation sur les serveurs et postes de travail des anti spams et des antivirus
- Mise en œuvre éventuelle d'un serveur de désincubation qui examine tous les messages et leurs pièces jointes ; permet notamment d'augmenter les chances de détection de virus en exécutant plusieurs antivirus simultanément.
- Nécessité de prendre en compte
  - les limites des antivirus (efficacité uniquement pour les virus pour lesquels ils ont été configurés)
  - le ralentissement que peut induire les antivirus et anti spams installés

Protocoles de messagerie sécurisés

- Certains logiciels de messagerie intègrent des capacités de chiffrement et signatures électroniques pour assurer la confidentialité, l'intégrité et l'authenticité des messages échangés et des correspondants
- Enrichissement du protocole SMTP (Simple Mail Transfer Protocol) pour intégrer des mécanismes de sécurité : protocoles ***S/MIME***, PEM, ***PGP***, …
- PEM (Privacy Enhancement for Internet Electronic Mail) : standard proposé pour chiffrer des messages électroniques, qui combine des algorithmes de chiffrage RSA et DES. Il est peu utilisé à cause de sa complexité

Protocole de messagerie sécurisé S/MIME

- S/MINE = Secure Multipurpose Internet Mail Extensions
- Extension sécurisée du protocole MIME intégrant des services d'authentification par signature et de confidentialité par chiffrement.
- Permet de chiffrer tout type de contenu
- Signature du message réalisée par chiffrement, via la clé privée de l'émetteur (RSA, DES), d'un résumé du message (message digest) créé par une fonction à sens unique MD5 ou SHA-1

Protocole de messagerie sécurisé PGP (1/2)

- PGP = Pretty Good Privacy
- Solution visant la confidentialité de la transmission des messages et l'authentification de l'émetteur
- Peut poser des problèmes de compatibilité avec MIME
- Versions libre et commerciale disponibles
- Sources disponibles => possibilité d'éviter les portes dérobées utilisables pour l'espionnage ou la prise de contrôle à distance

Protocole de messagerie sécurisé PGP (2/2)

- Exécution possible sur un grand nombre de plateformes
- N'est développé ni par une agence gouvernementale, ni par un organisme de normalisation : c'est un des aspects appréciés par certains internautes
- Utilise l'algorithme IDEA (International Data Encryption Algorithm) pour le chiffrement des messages, MD5 pour le hash du résumé, RSA pour le chiffrement du résumé et pour l'échange de la clé privée nécessaire à IDEA
- Propose 5 types de services pour le renforcement de la sécurité

Services PGP

- Authentification par signature digitale
- Confidentialité des messages par chiffrement (CAST, IDEA, Triple DES, Diffie-Hellman, RSA): clés de chiffrement utilisées une seule fois et pour un seul message.
- Compression ZIP après signature du message et avant son chiffrement
- Conversion de formats pour assurer la compatibilité entre systèmes de messagerie.
- Fragmentation de messages et réassemblage pour l'adaptation aux restrictions de taille des messages supportée par les systèmes.

Authentification par signature digitale avec PGP

- L'émetteur crée un message à partir duquel un résumé (hash) d'une longueur de 160 bits est généré en utilisant SHA-1
- Le résumé est chiffré avec la clé privée de l'émetteur et l'algorithme RSA et est transmis au récepteur
- Le récepteur décode le hash avec la clé publique de l'émetteur et génère un nouveau hash par la même fonction à sens unique SHA-1 et le compare avec celui reçu et déchiffré.
- En cas de correspondance, le message est authentifié.

Recommandations pour sécuriser un système de messagerie (1/2)

- Du côté du serveur :
  - Implanter des logiciels anti-virus et anti-spam
  - Filtrer les messages sur certains critères paramétrables (taille, fichiers attachés, etc.)
  - Eviter les comptes de maintenance par défaut
  - Assurer la protection physique du serveur

Recommandations pour sécuriser un système de messagerie (2/2)

- Du côté de l'utilisateur
  - Installer, gérer et imposer l'usage de logiciels antivirus
  - Définir les règles d'utilisation de la messagerie (ne pas ouvrir de fichiers exécutables, …)
  - Sensibiliser suffisamment les utilisateurs aux risques encourus
  - Faire engager les utilisateurs sur un usage approprié des ressources informatiques
  - Configurer correctement le poste de travail de l'utilisateur et sa messagerie
  - Implanter des versions de messagerie sécurisées
  - Utiliser des procédures de chiffrement pour des messages confidentiels et réaliser l'authentification des sources.

Exemples d’illustration de courriers malveillants et de mesures de détection/prévention

- Courrier électronique forgé
- Courrier électronique indésirable

Courrier électronique forgé (1/2)

- Une des attaques les plus faciles à réaliser
- Utilisable à des fins criminelles, pour harceler, diffamer, révéler des informations embarrassantes
- Hameçonnage ou phishing : courrier forgé visant l'obtention d'informations confidentielles en se faisant passer pour un expéditeur de confiance
  - Peut utiliser également des sites Web forgés, difficiles à distinguer des sites Web originaux, pour obtenir des informations de la victime

Courrier électronique forgé (2/2)

- Possibilité d'ouvrir une connexion Telnet sur le port 25 d'un serveur SMTP et d'envoyer un message avec une adresse forgée, car le serveur ne vérifie pas l'adresse de l'expéditeur.
- Possibilité d'inclure dans un courrier un lien vers un site ressemblant à celui d'un site de compte en ligne de banque

Traçage de courrier électronique forgé (1/2)

- Avant de délivrer un courrier, chaque serveur manipulant le courrier insère en haut de l'entête du courrier
  - Une ligne commençant par *Received :*
  - Une ligne contenant l'adresse IP de la machine qui lui a envoyé le courrier
- Il est donc possible de tracer un courrier jusqu'à la machine expéditrice

Traçage de courrier électronique forgé (2/2)

- Identification de l'expéditeur possible uniquement si la machine expéditrice conserve les dates et heures de connexion des utilisateurs.
- Identification de l'auteur difficile dans le cas de machines publiques, à moins qu'il ait laissé d'autres traces de son passage (paiement par CB, caméra de surveillance, …)

Protocole SMTP

- SMTP : Simple Mail Transfer Protocol.
- Protocole simple utilisé par Sendmail pour le transport de messages entre machines sur internet.
- Basé sur TCP/IP.
- Transaction sendmail : 5 commandes
  - HELO : salutations entre le client et le serveur.
  - MAIL FROM : spécification de l'expéditeur
  - RCPT TO : spécification du récepteur
  - DATA : donnée du message
  - QUIT : fin de la transaction.

Exemple de session Telnet sur serveur SMTP

$ Telnet example.org 25
S: 220 example.org ESMTP Sendmail 8.13.1/8.13.1; Wed, 30 Aug 2006 07:36:42 -0400
C: HELO mailout1.phrednet.com
S: 250 example.org Hello ip068.subnet71.gci-net.com [216.183.71.68], pleased to meet you
C: MAIL FROM:<xxxx@example.com>
S: 250 2.1.0 <xxxx@example.com>... Sender ok
C: RCPT TO:<yyyy@example.com>
S: 250 2.1.5 <yyyy@example.com>... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
From: Dave To: Test Recipient Subject: SPAM SPAM This is a test script.
S: 250 2.0.0 k7TKIBYb024731 Message accepted for delivery
C: QUIT
S: 221 2.0.0 example.org closing connection
Connection closed by foreign host.
$

Exemple d’entête de réception

Received: from serv2.DOMAINE.local ([213.223.244.1])
by mail.icewarp.com (Merak 7.2.1) with ESMTP id CRA73883
for <lgoc@icewarp.com>; Mon, 09 Feb 2004 09:28:40 +0100
Received: from metallo ([219.95.18.216]) by serv2.DOMAINE.local with Microsoft SMTPSVC(5.0.2195.532);
Mon, 9 Feb 2004 09:30:12 +0100
From: "Sazedur Cerezo"<lgoclgoc@YAHOO.COM>
To: lgoc@icewarp.com
Subject: lgoc: H*G*H-Lo0k Younger Whl1e L0slnq We19ht
Mime-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
Return-Path: lgoclgoc@YAHOO.COM
Message-ID: <SERVCOM2QFgkASNplKc000165d3@servcom2.DOMAINE.local>
X-OriginalArrivalTime: 09 Feb 2004 08:30:15.0039 (UTC) FILETIME=[F10A78F0:01C3EEE6]
Date: 9 Feb 2004 09:30:15 +0100

Courrier électronique indésirable : SPAM ou pourriel

- Définitions
- Techniques de diffusion du SPAM
- Protection des serveurs
- Spambots
- Messagerie gratuite en ligne

Courrier électronique indésirable : définition (1/2)

- Définition : « le spamming ou spam est l'envoi massif et parfois répété, des courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière dans les espaces publics de l'internet, forums de discussion, liste de diffusion, annuaires, sites web, etc. » (Commission Nationale de l'informatique et des Libertés – CNIL)

Courrier électronique indésirable : définition (2/2)

- Définition : « Le spam est l'envoi de courriers électroniques à destination d'adresses e-mail collectées de manière déloyale. Cela signifie que les données n'ont pas été collectées de manière transparente, soit parce que l'internaute n'était pas informé de l'identité du collecteur, soit parce qu'on ne lui a pas précisé les finalités du traitement ou qu'on les a détournées. Enfin, il y a spam lorsqu'un courrier ne permet pas une désinscription sélective ou totale. » (Syndicat National de la Communication Directe - SNCD)

Le spam est plus une nuisance qu'un vrai risque de sécurité ; c'est la façon dont il est distribué qui crée un risque

Techniques de diffusion du spam

- Utilisation de relais ouverts
- Spambots
- Messagerie gratuite en ligne

Diffusion de spam par relais ouverts

- L’attaquant n’utilise en général pas son propre système informatique mais celui d’une victime, car son compte serait très probablement bloqué par son fournisseur d’accès internet (FAI) avant qu’il n’ait diffusé l’ensemble de ses messages.
- Utilise très souvent des serveurs de courriers avec une liste de plusieurs milliers d’adresses de destination.

Diffusion de spam par relais ouverts (2/2)

- Plusieurs risques pour la structure dont le serveur est utilisé abusivement :
  - Risque d'interruption d'envoi et d'acheminement de courriers du fait de la surcharge du serveur
  - Risque de paralysie du serveur à cause d'une saturation de son disque par des logs de délivrance du courrier
  - Risque d'inondation de la boîte aux lettres de l'administrateur par des courriers générés lorsqu'une adresse électronique est inexistante
  - Risque de coupure de l'accès internet par le FAI en cas de plainte des destinataires du spam
  - Risque que les destinataires du spam mettent le serveur en liste noire le serveur abusé.

Protection des serveurs contre les mauvais relais

- Configurer le serveur pour qu'il n'accepte que des courriers dont soit l'expéditeur, soit le destinataire appartient au même domaine que le serveur :
  - Evite que le serveur soit utilisé comme relai pour du courrier n'ayant aucun rapport avec le domaine.
- Configurer le serveur pour que seuls les systèmes appartenant au même domaine que lui puissent envoyer du courrier avec un expéditeur faisant partie du domaine :
  - Evite qu'une personne extérieure se fasse passer pour un utilisateur du domaine

Spambots (1/2)

- Utilisation de robots pour la diffusion de spam
  - Ici le terme robot désigne la machine compromise qui obéit aux ordres du maître
- Moyens de compromission du robot :
  - Virus, par exemple suite à un clic de l'utilisateur sur un fichier attaché infecté
  - Connexion à l'internet d'une machine présentant des failles de sécurité
  - Etc.

Spambots (2/2)

- Robot élémentaire : relai SMTP ouvert à tous
- Robot plus élaboré
  - Connection du robot à un serveur de discussion (par exemple un IRC – Internet Relay Chat) et attente des commandes du maître
  - Connection du maître à l'IRC et envoi de ses instructions à tous les robots écoutant sur le canal
  - Possibilité pour un pirate d'avoir un réseau de plusieurs milliers ou millions de robots et de maîtres

Diffusion de spam par le biais de la messagerie gratuite en ligne

- Utilisation abusive de messageries gratuites en ligne telles que Hotmail, yahoo, Gmail ou d'autres moins connues
- Ces sites limitent le nombre de messages qui peuvent être envoyés à partir d'un même compte.
- Les diffuseurs de spam essaient de créer des scripts ouvrant automatiquement des milliers de nouveaux comptes et utilisent ces comptes pour envoyer le maximum de courriers
- Utilisation de « Captchas » (devinettes graphiques nécessitant un raisonnement qui ne peut être fourni par un programme automatique) pour se protéger contre les robots

Lutte contre les spams

- Filtrage
- Listes noires et listes blanches
- Signature de spam
- Listes grises

Filtrage (1/2)

- Solution la plus courante pour l'élimination des spams
- Possibilité de filtrage au niveau du serveur ou de la machine du destinataire
- Possibilité de filtrage portant sur le contenu du courrier ou sur son enveloppe :
  - Utilisation de mots clefs (Viagra, …)
  - Paramètre de l'entête du courrier (temps de transit total, …)
  - Critères liés au formatage des messages (titre du message en lettres capitales, …)

Filtrage (2/2)

- SpamAssassin :
  - Logiciel de lutte contre les spams utilisant des règles de filtrage
  - Applique plusieurs centaines de règles auxquelles sont affectées des poids
  - Calcul d'un score après analyse
  - Message considéré comme spam en cas de dépassement d'un seuil fixé.

Il n'y a pas de filtre parfait : il y a des possibilités de faux positifs et de faux négatifs

Listes noires, listes blanches et signatures de spam(1/2)

- Listes noires et listes blanches
  - S’appliquent en général au niveau du serveur
  - Une liste noire contient les adresses IP de machines qui envoient du spam
  - Une liste blanche contient les adresses IP, noms de domaines, des expéditeurs de confiance (connus pour ne pas envoyer de spam)

Listes noires, listes blanches et signatures de spam(2/2)

- Signature de spam
  - Approche basée sur la caractéristique d'envoi en masse et de circulation du spam sur des périodes longues avec éventuellement quelques variations.
  - Basée sur la mutualisation des efforts de chacun
  - Les bases de signatures de spams recensent les spam en circulation et indexent une signature de ces derniers

Listes grises (1/2)

- Porte d'entrée vers le purgatoire pour les messages arrivant sur un serveur de courrier
- Fonctionnement :
  - L'expéditeur est bloqué à son premier envoi de message sur le serveur considéré.
  - Le serveur conserve l'adresse IP du serveur SMTP effectuant l'envoi ainsi que l'adresse électronique de l'expéditeur et du destinataire
  - Le courrier est jeté
  - D'après le protocole SMTP (RFC 2821) le serveur qui a envoyé le message doit réémettre le message car n'a pas reçu l'accusé de réception.

Listes grises (2/2)

- Fonctionnement (suite):
  - D'après le protocole SMTP (RFC 2821) le serveur qui a envoyé le message doit réémettre le message car n'a pas reçu l'accusé de réception.
  - Si le message est reçu pour la seconde fois et que le triplet (adresse IP du serveur expéditeur, adresse de l'émetteur, adresse du destinataire) correspond à la valeur stockée, le message est délivré au destinataire, ainsi que tous les messages ultérieurs ayant le même triplet
- L'hypothèse de fonctionnement est que les machines qui envoient des spams ne perdent pas du temps à faire la réémission de messages qui n'ont pas abouti.

Plan

- ✓Introduction
- ✓Concepts généraux de la sécurité logicielle
- ✓Messagerie électronique et protocoles de messagerie sécurisés
- Maliciels
- Vulnérabilités des applications et des réseaux/Internet

Maliciels

- Introduction
- Virus
- Vers
- Protection contre les maliciels

Introduction

- Maliciel (malware) :
  - Programme ayant pour but de s'introduire dans un système informatique, de l'endommager ou d'en tirer profit
  - Englobe différents types de logiciels indésirables : virus, vers, chevaux de Troie, portes dérobées (backdoors), espiogiciels (spywares), publiciels (adwares)
- Il est important de les éliminer pour éviter les dommages directs ou indirects qu'ils peuvent engendrer

Virus

- Un virus a besoin d'un hôte pour s'exécuter : un fichier de données brutes tel qu'un fichier texte ne peut donc pas être un virus car il ne peut pas exécuter de commandes.
- Familles de virus suivant le type d'hôte :
  - Fichiers exécutables
  - Secteur d'amorçage et MBR (Master Boot Record)
  - Macros
  - Fichiers malformés
  - Virus furtifs
  - Virus polymorphes

Virus opérant via les fichiers exécutables

- La forme la plus classique de virus infecte des fichiers exécutables tels que les .exe ou .com sous Microsoft Windows
- Le virus s'exécute au cours de l'exécution du programme et se poursuit même après la fin de ce dernier. Il peut donc infecter d'autres fichiers tant que l'ordinateur est allumé.

Virus opérant via le secteur d'amorçage et le MBR (1/2)

- Le secteur d'amorçage contient le premier programme qui permet de lire et démarrer le système d'exploitation.
- Le virus qui infecte le secteur d'amorçage est exécuté avant le démarrage du système d'exploitation et peut se loger dans la mémoire avant lui.
- Les clefs ou CD-ROM peuvent comporter un secteur d'amorçage, et dans un tel cas, peuvent être infectés de façon similaire s'ils sont insérés dans l'ordinateur avant le démarrage.
- Le MBR est le premier secteur d'un disque partitionné. Il pointe sur le secteur d'amorçage de la partition active.

Virus opérant via le secteur d'amorçage et le MBR (2/2)

- L'infection du MBR permet d'exécuter un programme autre que celui présent dans le secteur d'amorçage
- Pour être débarrassé du virus, il faut détecter et effacer toutes les parties du virus

Virus opérant via des macros ou via des fichiers malformés

- Virus opérant via des macros
  - Les macros utilisées dans les logiciels de traitements de textes, de bases de données ou les tableurs peuvent être utilisées pour créer des virus qui vont infecter d'autres fichiers ou envoyer le même fichier par courriel à d'autres utilisateurs
- Virus opérant via des fichiers malformés
  - Création de fichier (JPEG, WMF, BMP, Word, Excel, Powerpoint, …) délibérément malformés provoquant l'exécution de virus par le programme chargé d'afficher le fichier
  - Technique la plus fréquente : débordement de tampons

Virus furtifs et virus polymorphes

- Virus furtifs
  - Modifient les routines utilisées pour accéder aux fichiers ou à la mémoire, de telle sorte qu'elles ne montrent que des contenus parfaitement propres
  - Les antivirus fonctionnant généralement par analyse du contenu des fichiers et de la mémoire vive des ordinateurs ne se rendent donc pas compte des modifications dues au virus
- Virus polymorphes
  - Virus capables de se modifier à chaque infection, ce qui rend leur identification difficile

Les vers

- Programmes indépendants se déplaçant d'ordinateur en ordinateur, à travers le réseau (reproduction par auto copie).
- Pas de modification de données et ni d'autres programmes, mais possibilité de :
  - S'accaparer des ressources système au cours de leur reproduction,
  - Transporter des virus, des bactéries ou des bombes logicielles.
- « Grand Vers de l'Internet » des années 1988 :
  - Origine du renforcement de la vigilance en matière de sécurité informatique.
  - Exploitation des portes dérobées dans Sendmail pour sa reproduction.
  - Détecté grâce à une faiblesse dans son code qui l'a poussé à se comporter comme une bactérie sur certains systèmes.
- Exemples de vers: Loveletter, SirCam, BugBear

Loveletter

- Message électronique avec le sujet « I love you » et un fichier joint en VBS (Visual Basic Script)
- Le fichier attaché s'exécute lorsque l'utilisateur l'ouvre par un double clic
- Lors de son exécution, envoie une copie du message électronique à toutes les adresses qu'il trouve dans le carnet d'adresses de Microsoft Outlook
- Se propage aussi par les chats IRC (Internet Relay Chat) en modifiant le fichier d'initialisation d'un client IRC populaire
- Remplace aussi des fichiers images et de musique qu'il trouve sur le disque dur
- Modifie la page de démarrage de Microsoft Internet Explorer afin de télécharger un logiciel censé trouver tous les mots de passe enregistrés dans l'ordinateur.

SirCam (1/2)

- Premier virus à large distribution créant un risque de perte de confidentialité en plus des risques de perte d'intégrité et de disponibilité
- Choisit un fichier au hasard sur le disque dur de la victime, l'infecte et l'envoie comme fichier attaché dans un courrier électronique
- Le destinataire s'infecte en cliquant sur la pièce jointe

SirCam (2/2)

- Choisit les destinataires dans le carnet d'adresses de la victime et en examinant le contenu des pages Web visitées par la victime, présentes dans le cache local du navigateur Internet, d'où une propagation plus rapide

BugBear (1/2)

- Exploite une faille de Microsoft Internet Explorer (IE) pour créer des attachements exécutés automatiquement lors de l'affichage du message, sans qu'il ne soit nécessaire de cliquer dessus
- Installe une porte dérobée sur la cible qui permet à un pirate de se connecter sur la machine infectée et d'y exécuter des commandes arbitraires
- Récupère tous les mots de passe d'accès à des sites Web qui sont mémorisés par IE et les envoie dans un courriel à une vingtaine de boîtes aux lettres sur Internet

BugBear (2/2)

- Installe également un espion de clavier et enregistre les frappes faites par l'utilisateur de la machine infectée.
- Arrête tous les antivirus et les pare-feu qu'il trouve sur la machine s'il en a les droits : l'anti-virus ne pourra plus se mettre à jour et ne pourra donc plus le détecter ultérieurement
- Scrute tous les fichiers qui peuvent contenir des adresses électroniques et envoie une copie de lui-même à 170 adresses.

Protection contre les maliciels

- Logiciels antivirus
- Architecture pour une défense en profondeur

Logiciels antivirus

- Moyen de défense classique
- Reconnaissent les maliciels et les éliminent
- 3 modes de fonctionnement de base :
  - Constitution d'une base de virus connus et recherche de la signature de ces virus dans des fichiers ou du trafic réseau
  - Analyse statique d'un code de programme pour détecter des opérations douteuses
  - Simulation de l'exécution d'un programme pour en analyser le comportement
- Possibilité de combinaison de modes

Logiciel antivirus avec fonctionnement par signature

- Création d'une signature pour chaque virus connu et recherche de ces signatures dans le fichier à analyser
- Possibilité de nettoyage du fichier infecté lorsque possible, ou mise en quarantaine (décision laissée à l'utilisateur).
- Augmentation du risque de faux positifs lié à l'augmentation constante du nombre de virus et du nombre de fichiers présents sur un ordinateur, avec comme risque la suppression ou la mise en quarantaine d'un fichier inoffensif et nécessaire.

Logiciel antivirus avec fonctionnement par analyse spectrale

- Elaboration d'une liste des instructions et des appels système contenus dans un programme et comparaison de ce spectre aux spectres caractéristiques de virus connus.
- Génère beaucoup de faux positifs, mais peut aussi découvrir de nouveaux virus

Logiciels antivirus avec fonctionnement par analyse comportementale

- Le code est exécuté en mode simulation et ce qu'il fait est contrôlé
- Le mode simulation permet d'éviter la propagation du virus
- Difficulté : si certaines fonctions du virus sont activées sous certaines conditions, on peut ne pas observer les conséquences de leur activation si la simulation ne satisfait pas lesdites conditions.

Logiciels antivirus – Architecture pour une défense en profondeur (1/2)

- La protection contre les virus est un cas typique de défense en profondeur
- Protection efficace uniquement en cas d'installation de logiciels antivirus à tous les niveaux du réseau : postes de travail et ordinateurs portables, serveurs de fichiers, serveurs de messagerie, proxy HTTP et FTP et SMTP
- Les antivirus doivent être configurés pour se mettre à jour automatiquement et régulièrement

Logiciels antivirus – Architecture pour une défense en profondeur (2/2)

- Nécessité d'une console centrale qui vérifie la bonne mise à jour des antivirus : permet de pallier à l'oubli de réactivation de l'antivirus après un arrêt volontaire par un utilisateur, …
- Idéalement veiller à ce que l'utilisateur n'ait pas de droit d'administration sur sa machine et exécuter l'antivirus sur les serveurs qui fonctionnent 24h/24 et permettent d'arrêter les virus avant qu'ils n'arrivent chez les utilisateurs
- L'installation de filtres génériques sur les proxies n'est pas difficile et permet d'atteindre une protection très efficace.

Plan

- ✓ Introduction
- ✓ Concepts généraux de la sécurité logicielle
- ✓ Messagerie électronique et protocoles de messagerie sécurisés
- ✓ Maliciels
- Vulnérabilités des applications et des réseaux/Internet

Vulnérabilité des applications et des réseaux

- Denis de service
- IP Spoofing
- Sniffing
- Vol de session
- Exploits

Dénis de service – DoS (1/2)

- Une attaque par déni de service d'un système consiste à paralyser des ressources de ce dernier de telle sorte qu'il ne puisse plus fonctionner correctement:
  - Envoi de trafic tellement important à la cible de façon à ce qu'elle ne soit plus en mesure de répondre aux requêtes normales
  - Monopolisation du nombre de connexions simultanées
  - Monopolisation de la mémoire vive
  - Blocage du système suite à une erreur inattendue

Dénis de service – DoS (2/2)

- Cas les plus intéressants pour les pirates : attaques anonymes
- Exemples d'attaques de type DoS
  - SYN Flooding
  - Attaques par réflexion (Smurf)
  - Denis de services distribués (DDoS)

Attaque de DoS SYN Flooding

- Une des attaques de DoS les plus anciennes
- Consomme toutes les ressources TCP d'un ordinateur
- Attaque la phase d'établissement de connexion TCP (paquets SYN) en remplissant la file utilisée au niveau de la cible pour stocker les demandes de connexion (acquittements) à traiter.
  - Conséquence : empêche la cible d'accepter de nouvelles connexions.
  - Possibilité d'attaque anonyme en utilisant une adresses IP source arbitraire dans le paquet SYN

Protection contre les attaques SYN flooding

- Les pare-feu et les systèmes d'exploitation récents ont les moyens de protection contre ces attaques
- Effacement de connexions partiellement établies si elles ne sont pas acquittées dans un délai raisonnable

Protection contre les attaques SYN flooding

- Utilisation de SYN cookies :
  - Les seules informations gardées par le serveur lors de la réception d'un SYN sont stockées dans l'ISN proposé au serveur par le client
  - L'ISN est envoyé avec le SYN-ACK et aucune ressource n'est consommée sur le serveur
  - Le serveur retrouve l'information dans le numéro de séquence présent dans le paquet d'acquittement du client

DoS- Attaques par réflexion (Smurf)

- Un exemple d'attaque par réflexion consiste à noyer la victime dans un flux de réponses ICMP (protocole utilisé notamment par « ping » pour vérifier l'atteignabilité de machines sur le réseau).
- Fonctionnement de ICMP:
  - Envoi d'un paquet ICMP « echo request »
  - A la réception, le destinataire répond par l'envoi d'un paquet ICMP « echo reply » à l'adresse source indiquée dans le paquet de requête.

DoS- Attaques par réflexion (Smurf)

- Principe de l'attaque:
  - Le pirate inscrit l'adresse cible comme adresse IP source dans l'entête IP du paquet ICMP de requête.
  - Le destinataire envoie sa réponse à l'adresse cible indiquée par le pirate plutôt qu'au pirate.
  - L'effet peut être amplifié par le pirate en envoyant son message à une adresse de diffusion (octet machine du sous-réseau mis à 255)
- D'autres attaques par réflexion existent
  - Applications acceptant des paquets UDP et générant des messages d'erreurs plus longs que la requête du pirate: possibilité de modification de l'adresse source dans le paquet UDP.

DoS- Attaques par réflexion (Smurf)

- Solutions usuelles pour lutter contre ces attaques : configuration du routeur pour ne pas relayer des informations provenant de l'extérieur de leur réseau
  - Description de l'approche disponible dans la RFC 1812 : « a router MAY have an option to disable receiving network-prefix-directed broadcasts on an interface and MUST have an option to disable forwarding network-prefix-directed broadcasts. These options MUST default to permit receiving and forwarding network-prefix-directed broadcasts ».

DoS- Denis de service distribués

- Cas typique: le pirate utilise abusivement un ensemble de machines pour déclencher une attaque simultanée de la victime à partir des machines compromises.
- Le pirate s'appuiera typiquement sur la présence d'une vulnérabilité dans un logiciel s'exécutant sur un grand nombre de machines pour installer sur ces machines un client s'exécutant de manière cachée.

DoS- Denis de service distribués

- Les machines infectées ne communiquent pas directement avec le pirate, mais avec un serveur intermédiaire (serveur de « chat » par exemple) sur lequel le pirate va également se connecter.
- Possibilité d'utiliser les machines infectées pour des attaques de type réflexion, ou pour d'autres attaques.

IP Spoofing

- IP Spoofing : référence à la falsification d'adresses sources IP
- Idée du pirate:
  - Exploiter les adresses positionnées comme adresses de confiance par le routeur/pare-feu ou à travers un mécanisme du type « .rhosts ».
  - Le routeur/pare-feu laissera passer les paquets supposés venir de la machine de confiance, même s'ils ont été falsifiés; de même, dans le cas d'utilisation du .rhosts, la machine cible exécutera sans besoin de mot de passe les commandes supposées venir de la machine de confiance mentionnée dans le .rhosts

IP Spoofing

- Falsification difficile dans le cas de TCP:
  - Dans la phase d'initialisation, le destinataire doit transmettre à l'émetteur l'accusé de réception avec le numéro du paquet suivant attendu (ISN) et le pirate a besoin de l'ISN pour sa manœuvre.
  - 2 cas possibles tout de même: pirate et machine forgée dans le même sous réseau, spoofing aveugle

TCP spoofing

- Cas où le pirate et la machine dont l'IP est usurpée sont dans le même sous-réseau:
  - L'attaquant peut observer le trafic circulant sur le réseau et récupérer l'ISN du message transmis à la machine dont il veut se faire passer.
- Spoofing aveugle (cas où le pirate n'est ni sur le sous-réseau de la machine dont l'IP est usurpée, ni sur celui de la machine victime de l'attaque):
  - Le pirate doit deviner l'ISN, par exemple par
    - Echantillonnage de l'algorithme de l'ISN par ouverture de quelques connexions légitimes
    - Envoi de valeurs aléatoires jusqu'à obtention d'une bonne valeur.

UDP Spoofing

- Attaque plus facile, car pas besoin d'échange de paquets pour établir la connexion
  - Possibilité d'émettre une requête DNS vers un serveur en se faisant passer pour une autre machine
  - Possibilité de se faire passer pour le serveur DNS auprès de la machine qui a fait la requête: nécessite de deviner un identifiant de 16 bits qui se trouve dans la requête et la réponse DNS.
- Solution adoptée par la plupart des clients DNS pour réduire les risques: utilisation de ports source aléatoires qui fait passer à 32 le nombre de bits à deviner

Sniffing

- Capture d'une image du trafic circulant sur une portion du réseau
- Vise à exploiter la circulation en clair de mots de passe sur le réseau dans plusieurs méthodes d'authentification (Telnet, rsh, ftp, http avec authentification basique, pop, imap)

Sniffing

- Très utilisé par les pirates pour étendre leurs attaques
  - Après avoir pris possession d'une machine, le sniffing permet de trouver les mots de passe permettant d'accéder à d'autres machines
  - Efficace dans les réseaux locaux utilisant un média partagé (par exemple WLAN): le sniffer peut voir le trafic de toutes les machines du réseau => plus de chance de trouver un mot de passe
  - Efficacité de l'attaque réduite en cas de connexion des machines via des commutateurs, car le commutateur ne propage les paquets que vers les machines potentiellement destinataires
  - Possibilité d'utiliser une attaque *ARP Spoofing* dans ce dernier cas.

ARP Spoofing

- ARP : protocole permettant d'établir le lien entre les adresses Ethernet et les adresses IP des machines connectées à un réseau
- Ce lien doit être établi avant l'envoi de trames au destinataire:
  - L'émetteur de la trame envoie une requête ARP à toutes les machines connectées au même sous-réseau
  - La machine qui reconnaît son adresse IP dans la requête répond en envoyant son adresse Ethernet
  - Pour un envoi à une machine hors de son sous-réseau, l'émetteur fait une demande ARP pour connaître l'adresse Ethernet de la passerelle par défaut.

ARP Spoofing

- L'ARP Spoofing consiste à diffuser de fausses réponses ARP qui donnent l'adresse Ehernet du pirate pour toutes les adresses IP du sous-réseau.
- La plupart des implémentations d'ARP enregistrent dans le cache toutes les réponses qu'elles voient passer =>
  - Le pirate peut donc faire dévier tout le trafic de son sous-réseau vers son adresse Ethernet
  - Il pourra en toute discrétion sniffer tout le trafic avant de l'acheminer vers les destinataires effectifs

Vol de session

- Vol de session (session hijacking) = moyen de pénétrer dans un système sans avoir besoin de connaître un nom d'utilisateur et un mot de passe
- Fonctionnement:
  - Le pirate attend qu'un utilisateur légitime se connecte à distance au système
  - Il prend ensuite le contrôle de la connexion et l'utilise à ses fins

Vol de session

- Vol d'une connexion TCP
  - Le pirate espionne un client TCP qui se connecte à distance (par exemple avec Telnet)
  - Il attend que le client soit authentifié
  - Il envoie des commandes à sa place en forgeant des paquets TCP
  - Le serveur ne fera pas la différence entre les paquets normaux du client et ceux forgés; toutefois, cela peut générer une avalanche d'acquittements => attaque plus efficace si le pirate peut bloquer le trafic du client, par exemple par un déni de service.

Vol de session HTTP

- La notion de session n'existe pas réellement dans le protocole HTTP: chaque requête est traitée de manière indépendante
- La notion de session est généralement créée en envoyant chaque requête client avec 1 identifiant permettant d'associer la requête à la session courante.
  - L'identifiant peut être 1 cookie stocké chez le client en début de session
  - Une URL personnalisée incluant 1 identificateur du client peut également être utilisée.

Vol de session HTTP

- Mode opératoire:
  - Le pirate espionne les requêtes échangées entre le client et le serveur web
  - Il attend l'authentification du client puis envoie une requête à sa place

Exploits

- L’exploit est le terme utilisé en informatique pour désigner l’exploitation des défauts d’un logiciel à des fins de piratage
- Les défauts les plus intéressants pour les pirates sont ceux des serveurs en raison, d’une part, de leur accès via le réseau qui permet de faire des attaques à distance et, d’autre part, des privilèges d’administration dont ils disposent très souvent

Exploits

- Les exploits peuvent être classés en fonction des types de vulnérabilités:
  - Vulnérabilités conceptuelles
  - Failles techniques
  - Failles des applications en ligne

Vulnérabilités conceptuelles

- Il s’agit de vulnérabilités liées à une mauvaise conception.
- Elles sont autant variées que les applications disponibles sur les systèmes informatiques en réseau
- Exemple: parcours de répertoires dans un serveur Web
  - But du serveur Web: donner accès aux pages stockées dans une arborescence de fichiers dont le répertoire racine est bien fixé.
  - De nombreux appareils actuels possèdent un serveur Web embarqué pour faciliter leur gestion à distance.

Vulnérabilités conceptuelles

- Exemple: parcours de répertoires dans un serveur Web (suite)
  - Compaq fournit un logiciel de maintenance à distance (Compaq Server Management Agent) qui dans l'une de ses versions antérieures permettait d'insérer ../.. dans l'arborescence et n'empêchait pas de sortir du répertoire racine du serveur Web.
  - Une faille semblable existait sur le serveur IIS de Microsoft et permettait en plus d'exécuter des programmes arbitraires sur le serveur http://a.b.com/**scripts**/..**%c0%af**../winnt/system32/cmd.exe?/c+dir

Failles techniques

- Il s'agit de failles liées à une mauvaise conception
- La faille la plus souvent exploitée est le « buffer overflow » (débordement de tampon)
- Principe du débordement de tampon
  - Exploitation du débordement de la zone de buffer allouée pour les données d'entrées du programme
  - Un tel débordement est possible si la taille des données entrées est supérieure à celle attendue et que le programme n'a pas prévu la vérification et le traitement nécessaires.

Failles techniques

- Principe du débordement de tampon (suite)
  - Les données fournies en trop pourront écraser une zone mémoire contenant les valeurs d'autres variables, des instructions du programme ou des adresses de saut pour la suite du programme
  - La bonne connaissance de l'architecture de la machine à exploiter permet de créer un bloc de données contenant un programme malicieux qui va écraser la mémoire de manière à faire exécuter ce dernier.

Illustration du débordement - Exécution des appels de procédures

- Dépôt des paramètres de la procédure sur la pile
- Dépôt de l'adresse de retour sur la pile
- Dépôt de la valeur actuelle du pointeur de trame sur la pile (sfp – saved frame pointer)
- Réservation d'une zone mémoire pouvant contenir toutes les variables locales de la procédure
- Stockage du début de cette zone dans le pointeur de trame (fp – frame pointer)

Exemple

```
Void f (int x, int y)    {
  char buffer [20];
  strcpy (buffer, '' hello world '');
}



Void main ()   {
  f (1, 2);
}
```

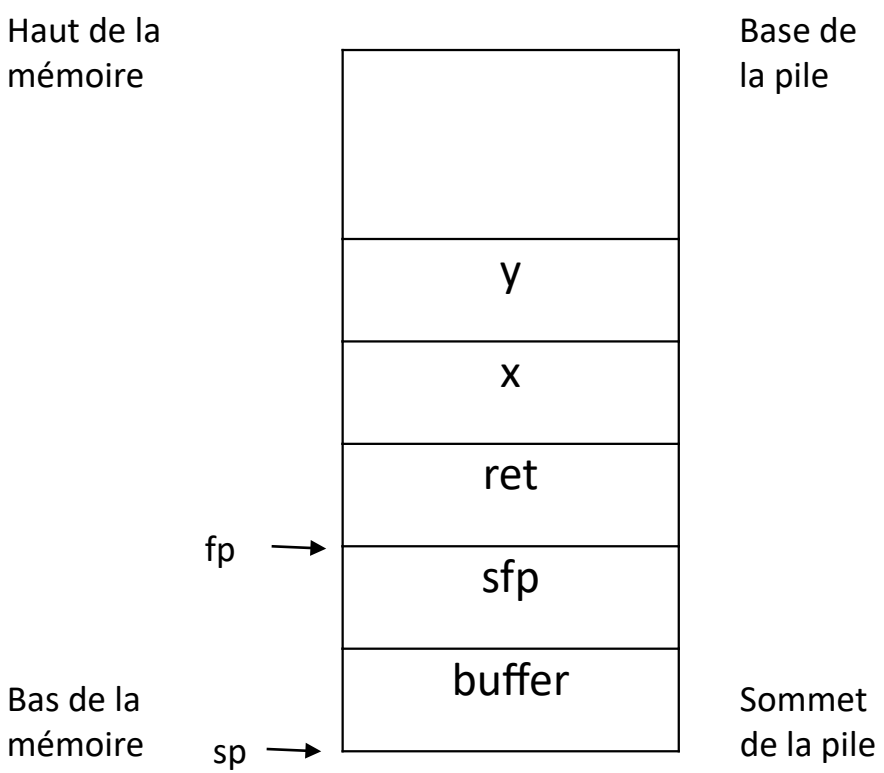

Illustration du débordement - description du mécanisme

- Le débordement du buffer écrasera d'abord sfp, puis l'adresse de retour, puis d'autres éléments de la pile
- A la fin de l'exécution de la procédure, le programme ne retourne pas à l'adresse qui avait été déposée dans la pile, mais à l'adresse qui l'a remplacée suite à l'écrasement

Illustration du débordement - description du mécanisme (suite)

- Pour faire exécuter un programme arbitraire grâce à un débordement de mémoire:
  - Le pirate s'organise pour construire un contenu du buffer qui permettra de remplir la zone réservée ainsi que sfp et l'adresse de retour
  - L'astuce consiste à trouver la valeur de retour qui conduira à l'exécution du programme malicieux
- Les débordements de tampons peuvent également être exploités dans le tas (zone de mémoire où se trouvent les variables allouées dynamiquement)

Stratégies de protection des compilateurs contre le débordement de tampon

- Vérification de l'intégrité de la pile juste avant la fin de l'exécution d'une procédure
- Réorganisation aléatoire des programmes et des bibliothèques dans la mémoire afin que les pirates ne sachent pas la localisation des instructions dans la mémoire
- Utilisation de zones de mémoire non exécutables pour la pile et le tas: évite l'exécution d'instructions injectées dans des variables sur la pile ou le tas.

Failles des applications en ligne

- Plusieurs types d'erreurs de programmation de sites web permettent aux pirates de prendre le contrôle de ces derniers
- L'open Source Web Application Security Project (OWASP) a pour objectif de recenser ces erreurs et d'aider les développeurs à les éviter: publication régulière des « top ten » des erreurs les plus répandues, …
- 2 erreurs parmi les plus classiques: « Cross Site Scripting » et « injections SQL »

Cross Site Scripting (1/3)

- Consiste en l'injection de code malicieux (HTML ou Javascript) dans une page Web
- Nécessite que le site Web autorise ses visiteurs à fournir des informations, par exemple via des formulaires, et que le site réaffiche ces informations ensuite dans ses pages, si possible sans les modifier
- Un exemple typique est 1 livre d'or: en cas d'inscription d'un code javascript dans le livre d'or, ce code sera exécuté dans le navigateur des personnes qui consulteront le site

Cross Site Scripting (2/3)

- Le pirate optera très souvent pour une référence à un script localisé ailleurs plutôt qu'à la saisie directe du code du script
- Insertion d'un code tel que

  <script src="//pirat.es/evil-script.js ''>

  => Origine de l'appellation « Cross Site Scripting ».
- Les scripts injectés par le pirate pourront prendre le contrôle complet du navigateur de la victime.

Cross Site Scripting (3/3)

- Ces scripts pourront notamment:
  - Faire apparaître des informations erronées
  - Faire apparaître un formulaire d'authentification frauduleux qui permet au pirate de récupérer le nom et le mot de passe de la victime
  - Récupérer le cookie de session et l'envoyer au pirate pour qu'il puisse faire un vol de session
  - Enregistrer tout ce que la victime écrit dans les champs des formulaires
  - Cliquer et effectuer des actions à la place de la victime, par exemple pour passer une commande

Injection SQL (1/5)

- Consiste à injecter des commandes qui seront interprétées par la base de données d'une application en ligne
- Si l'application n'empêche pas l'utilisateur d'injecter du code SQL dans les informations qu'il fournit, ce dernier peut manipuler la base à sa guise.

Injection SQL (2/5)

- Exemple:

```
$requete = requete (‘’select Pseudo from t_user where Pseudo=‘ ’’.$User.’’ ‘ and Passe =‘ ‘’.$Password.’’ ‘
‘’);
If (my_sql_num_rows ($requete) == 0)
{
   // mauvais mot de passe
   header (‘’Location:login_admin_mediabox404.php?Fct=Bad_Pseudo’’);
}
Else
{
  // mot de passe ok
```

Injection SQL (3/5)

- Si la chaine vide est saisie comme mot de passe et pour l'utilisateur l'on saisit ' OR 1=1 /*

  on obtient ce qui suit:

```
$requete = select Pseudo from t_user where Pseudo=' ' OR 1=1 /* ' and Passe =' ';
If (my_sql_num_rows ($requete) == 0)
{
   // mauvais mot de passe
}
Else
{
  // mot de passe ok
```

Injection SQL (4/5)

- Dans ce cas, le mot de passe est accepté quelles que soient les données de la base.
- Si l'utilisateur connaît le nom de l'administrateur, il peut se connecter à son compte en saisissant comme user nom_admin '/*

Injection SQL (5/5)

- Les attaques d'injection SQL peuvent avoir des conséquences désastreuses en donnant accès à toutes les informations utilisées par l'application
- Meilleure défense: vérifier que les informations fournies par les utilisateurs sont conformes au format attendu
- Si les caractères spéciaux comme les guillemets sont autorisés, ils doivent être traités de manière à ne pas avoir d'effet sur les pages HTML et sur les requêtes SQL.

Quelques points à retenir (1/7)

- La sécurité peut être définie comme la propriété d'un système visant à assurer sa disponibilité, son intégrité et sa confidentialité.
- Les principaux risques de sécurité d'un système sont : l'atteinte à sa disponibilité et à ses données ; la destruction, la corruption, la falsification, le vol et l'espionnage de ses données ; son utilisation illicite.
- L'objectif de la sécurité d'un système est de réduire les risques de sécurité liés à son utilisation, voire de les éliminer.

Quelques points à retenir (2/7)

- La mise en place de la sécurité repose sur 4 principaux types de mécanismes : des mécanismes de détection de malveillances, de protection, de défense et de résilience contre les malveillances.
- Elle nécessite de : définir les risques et les objets à protéger, d'identifier et authentifier les accès au système, d'empêcher les intrusions, de concevoir la défense en profondeur, de prendre en compte la dimension organisationnelle (comportement humain, vérification du dispositif de sécurité, veille technologique, norme, …)

Quelques points à retenir (3/7)

- La messagerie électronique est une des applications logicielles requérant une attention particulière en matière de sécurité
- Elle est sujette à différents risques de sécurité : perte, interception, altération ou destruction de messages ; divulgation d'informations confidentielles, infection des systèmes par le biais de messages contenant des codes malveillants (virus, …) ; inondation de messages (spam, …), usurpation d'identité, harcèlement des utilisateurs, refus de service, répudiation, risques liés aux réseaux (routage, …)

Quelques points à retenir (4/7)

- Des actions sont nécessaires pour limiter les risques de sécurité relatifs à la messagerie électronique
- Du côté serveur, il s'agit notamment d'implanter des logiciels anti-virus et anti-spam, de filtrer les messages sur certains critères paramétrables (taille, fichiers attachés, etc.), d'éviter les comptes de maintenance par défaut, d'assurer la protection physique du serveur

Quelques points à retenir (5/7)

- Du côté utilisateur, il s'agit d'installer, gérer et imposer l'usage de logiciels antivirus ; de définir les règles d'utilisation de la messagerie, de sensibiliser suffisamment les utilisateurs aux risques encourus, de faire engager les utilisateurs sur un usage approprié des ressources informatiques, de configurer correctement le poste de travail de l'utilisateur et sa messagerie, d'implanter des versions de messagerie sécurisées, d'utiliser des procédures de chiffrement pour des messages confidentiels et réaliser l'authentification des sources

Quelques points à retenir (6/7)

- Les maliciels ou malware sont des programmes ayant pour but de s'introduire dans un système informatique, de l'endommager ou d'en tirer profit. Parmi ces derniers, l'on a les virus, vers, chevaux de Troie, portes dérobées, espiogiciels, et publiciels
- L'utilisation appropriée de logiciels antivirus et la mise en œuvre de mesures de défense en profondeur permettent d'éviter ou de limiter les risques liés à ces maliciels

Quelques points à retenir (7/7)

- Les applications et les réseaux sont vulnérables à différentes attaques : dénis de service, IP Spoofing, sniffing, vol de session, exploits.
- Il est important de prendre des dispositions adéquates pour éviter ou au moins limiter les effets de telles attaques.

Quelques références

- Sécurité Informatique. Gildas Avoine, Pascal Junod, Philippe Oechslin. Vuibert, 2ème édition, 2009