La sécurité applicative

De quoi s'agit-il ?
Quel en est l'enjeu ?

Emilien Kia
CLUSIR - antenne de Grenoble / UPMF-IUT2
8 juin 2009

La sécurité applicative

- Introduction : qu'est-ce et pourquoi ?
- Les attaques et leurs conséquences
- Le traitement des vulnérabilités :
  - Pendant la spécification
  - Pendant la conception
  - Pendant le développement
  - Pendant la vie productive
- Prévention globale (ensemble du process)
- Conclusion

La sécurité applicative

Introduction :

Qu'est-ce que la sécurité applicative ?
Pourquoi la mettre en place ?

Qu'est-ce que la sécurité applicative ?

Définition courante :

- « Partie logicielle intégrée aux S.I. gérant la *sécurité de l'information* »
- « La sécurité de l'information est un processus visant à protéger des données contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisée. » (Wikipedia fr)

Qu'est-ce que la sécurité applicative ?

Définition étendue:

- Partie logicielle intégrée aux S.I. gérant :
  - La sécurité de l'information
  - L'intégrité du S.I.
  - La confidentialité du S.I.

Quel en est l'enjeu ?

- S.I. = cœur de l'activité
- S.I. = ensemble des données
- Conséquences en cas de :
  - Vol de données (vente à un concurrent)
  - Violation des données (suppression/modification)
  - Dégradation des services

La sécurité applicative

Les attaques et leurs conséquences

Les attaques et leurs conséquences

- Les failles
- Les attaques
- Leurs conséquences
  - Sur le système S.I.
  - Sur l'entreprise

Les attaques et leurs conséquences

Les failles :

- « portes anormalement entrouvertes »
- Origine volontaires ou non.
- Tous les étages applicatifs:
  - Système/configuration : LogInj, SeedLess, DefParam
  - Conception : ClientValidation, PasswordStorage
  - Développement : DoubleFree, OutOfRange
  - Outils/Langages : BufferOverflow

Les attaques et leurs conséquences

Les attaques :

- Les modes opératoires, les actions des pirates
- Dépend du but recherché :
  - Usurpation : manipulation de session
  - Introspection : injection (SQL, code …)
- Dépend des failles :
  - Overflow, string formating, brute force ...

Les attaques et leurs conséquences

Les conséquences :

- Rupture de la « triade DIC » :
  - Disponibilité (Denial Of Service)
  - Intégrité (Injection de données)
  - Confidentialité (Vol de données)
- Rupture de la traçabilité/imputabilité/preuve
  - Violation des journaux

La sécurité applicative

Le traitement des vulnérabilités

Le traitement des vulnérabilités

- Extension des critères qualité
- 4 phases de vie d'une application
  - Phase de spécification
  - Phase de conception
  - Phase de développement
  - Phase de production

Le traitement des vulnérabilités

Extension des critères qualité

- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité

Le traitement des vulnérabilités

Traitement en phase de spécifications

- Isolation des données/process sensibles
- Analyse et chiffrage des risques
  - EBIOS / MEHARI / OCTAVE
- Clauses en cas de défaut
- Procédures de sauvegardes/restauration/remise en route

Le traitement des vulnérabilités

Traitement en phase de conception

- Approche globale (top-down) par l'analyse des risques du S.I.
- Approche locale (bottom-up) par isolation de modules
- Prévision des risques liés aux tiers (sous-traitants, bibliothèques …)
- Prévision des risques liés à l'environnement d'exécution/de déploiement

Le traitement des vulnérabilités

Traitement en phase de développement

- Mutualisation des fonctionnalités
- Définition des invariants/prévariants
- Interception/remontée des exceptions
- Documentation exhaustive (paramètres, exceptions …)
- Génération de code
- Relecture et mesure de code

Le traitement des vulnérabilités

Traitement en phase de production

- Vérification de la configuration (droits …)
- Traces d'exploitation (load balancing, logs …)
- Suivi/SAV/MCO (patchs, SP …)
- S.I. mirroirs (tests, récupération ...)

La sécurité applicative

La prévention globale

La prévention globale

- Procédures de notation et de suivit qualité
- Audits réguliers de spécialistes « hors projet »
- Spécifications et exécutions de tests
- Procédures de livraison et mise en production

La prévention globale

Analogie de l'entreprise :

- **Services** (production, compta, achats, commerciaux, expéditions…)
- **Locaux** (pièces, étages, bâtiments, sites, pays...)
- **Personnels** (dirigeants, gestionnaires, techniques, commerciaux... employés, détachés, intérimaires, stagiaires...)
- **Prestataires**
- **Clients**

La sécurité applicative

Conclusion