

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



```
eax, ebx, ecx, edx);
static void cpuid_smp_cpuid(void *cmd_block)
{
    struct cpuid_regs *cmd = (struct cpuid_regs *)cmd_block;
    cpuid_count(cmd->eax, cmd->ecx,
                &cmd->eax, &cmd->ebx, &cmd->ecx, &cmd->edx);
}
static loff_t cpuid_seek(struct file *file, loff_t offset, int orig)
{
    loff_t ret;
    struct inode *inode = file->f_mapping->host;
    mutex_lock(&inode->i_mutex);
    switch (orig) {
    case 0:
        file->f_pos = offset;
        ret = file->f_pos;
        break;
    case 1:
        file->f_pos += offset;
        ret = file->f_pos;
        break;
    default:
        ret = -EINVAL;
    }
    mutex_unlock(&inode->i_mutex);
    return ret;
}
static ssize_t cpuid_read(struct file *file, char __user *buf,
                          size_t count, loff_t *ppos)
{
    struct inode *inode = file->f_mapping->host;
    mutex_lock(&inode->i_mutex);
    if (count > 0)
        ret = cpuid_read_data(buf, count, ppos);
    else
        ret = 0;
    mutex_unlock(&inode->i_mutex);
    return ret;
}

```

Les attaques et leurs conséquences

```
</div>
<div class="y-cta-cta">
    <div id="y-page">
        <div id="y-header" class="clearfix">
            <div id="default-p_13838465" class="mod view_default"> <div id="default-p_13838465">
                <div id="default-p_14119506 d24" class="mod view_default"> <div id="default-p_14119506 d24">
                    </div>
                    <div class="help small">
                        <div id="account-tips" class="strong large"><a href="http://www.ubuntu.com/faq/faq-account-tips">
                            </div>
                    </div>
                </div>
            </div>
            <span class="y-chrome-top"><span class="left y-fg-pg-controls"><input type="checkbox" /></span></span>
        </div id="y-content" class="clearfix">
            <div id="y-masthead">
                <div id="default-p_13838465" class="mod view_default"> <div id="default-p_13838465">
                    <div id="default-p_14119506 d24" class="mod view_default"> <div id="default-p_14119506 d24">

```





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 formatting, 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



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
- Préviation des risques liés aux tiers (sous-traitants, bibliothèques ...)
- Préviation 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 (patches, SP ...)
- S.I. miroirs (tests, récupération ...)



La sécurité applicative



```
eax, ebx, ecx, edx);
static void cpuid_smp_cpuid(void *cmd_block)
{
    struct cpuid_regs *cmd = (struct cpuid_regs *)cmd_block;
    cpuid_count(cmd->eax, cmd->ecx,
                &cmd->eax, &cmd->ebx, &cmd->ecx, &cmd->edx);
}
static loff_t cpuid_seek(struct file *file, loff_t offset, int orig)
{
    loff_t ret;
    struct inode *inode = file->f_mapping->host;
    mutex_lock(&inode->i_mutex);
    switch (orig) {
    case 0:
        file->f_pos = offset;
        ret = file->f_pos;
        break;
    case 1:
        file->f_pos += offset;
        ret = file->f_pos;
        break;
    default:
        ret = -EINVAL;
    }
    mutex_unlock(&inode->i_mutex);
    return ret;
}
static ssize_t cpuid_read(struct file *file, char __user *buf,
                          size_t count, loff_t *ppos)
{
    char __user *start = buf;
    struct cpuid_regs *cmd = (struct cpuid_regs *)0;
    int cpu = 0;
    int pos = 0;
    while (count > 0) {
        cpuid_count(cmd->eax, cmd->ecx,
                    &cmd->eax, &cmd->ebx, &cmd->ecx, &cmd->edx);
    }
}
```

La prévention globale

```
</body>
<body class="yui-skin-sam">
    <div id="y-page">
        <div id="y-header" class="clearfix">
            <div id="default-p_13838465" class="mod view_default"> <div id="default-p_13838465">
                <div id="default-p_14119506 d24" class="mod view_default"> <div id="default-p_14119506">
                    </div>
                    <div class="help small">
                        <div id="account-tips" class="strong large"><a href="http://www.yui.com/yui/faq">
                            </div> </div>
                </div>
            </div>
            <span class="y-chrome-top"><span class="left y-fg-pg-controls"><input type="checkbox" />
                </div id="y-content" class="clearfix">
                <div id="y-masthead">
                    <div id="default-p_13838465" class="mod view_default"> <div id="default-p_13838465">
                        <div id="default-p_14119506 d24" class="mod view_default"> <div id="default-p_14119506">
                            </div>
                            <div class="help small">
                                <div id="account-tips" class="strong large"><a href="http://www.yui.com/yui/faq">
                                    </div> </div>
                    </div>
                </div>
            </div>
        </div>
    </body>
```



La prévention globale



- Procédures de notation et de suivi 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**



**CLUSIR Rhone-Alpes
Antenne de Grenoble**

**IUT Grenoble 2 – Dpt Informatique
8 Juin 2009 (17h30- 19h30)**

Formations en sécurité informatique

Éléments de réflexion sur les besoins et solutions de formation

Sébastien BOURDON

sebastien.bourdon@iut2.upmf-grenoble.fr

Maître de conférence en informatique (IUT 2 Grenoble)

Consultant en Sécurité des systèmes d'information (SBN Consultants)

Formation en sécurité des SI : plusieurs prérequis à la réflexion !

Sécurité des systèmes d'information => Plusieurs expertises :

- => Organisationnelle / fonctionnelle de l'entreprise (système d'information)
- => Organisationnelle et technique de l'informatique (Applications, Réseaux, Systèmes)
- => Organisationnelle / fonctionnelle / technique de la sécurité (informatique, infrastructure, accès physique)
- => Gestion des Ressources humaines (sensibilisation / formation / protection des utilisateurs)
- => Légales (responsabilités de l'entreprise, des salariés, méthodes d'investigations)

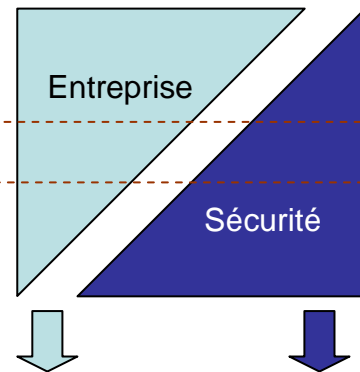
Reflexion sur la formation

=> Besoin d'expertise

=> Mode d'acquisition de l'expertise

- => Expérience
- => Encadrement
- => **Formation**
- => Recrutement
- => Assistance technique

Connaissance de l'entreprise / la sécurité



Acquisition d'expertise

- => **Existant + Cible**
- => **Moyens d'y parvenir**
- => **Resources / ROI**

Besoins très différents de formation

=> Place de la sécurité dans l'entreprise

=> Taille de l'entreprise

TPE / PE

: 1 responsable interne qui couvre tout

ME

: 1 RSSI (gouvernance + organisation + gestion du risque)
+ Expertise technique (externalisée / transférée à l'IT)

GE

: Stratégique (méthodologie, politique, plans de formation, ressources dédiés)
+ Pilotage / Conduite de projet (niveau managérial interne, méthodologie)
+ Expertise technique dédiée (conseil) / transférée à l'IT (externalisée)

Prestataire

: Diffuse (chez généralistes) / Pointue (experts en veille, sensibilisation, solution...)

Utilisatrice

Prestataire de service

Formation : Quel besoin pour qui ? Analyse de la valeur !

Ex1 : Développement logiciel sécurisé

Coeur de métier

Génie logiciel

2nde expertise : Approche sécurisée

Définition / respect de méthodologies de développement logiciel

Maîtrise des méthodes et outils de tests

Mise en place d'un environnement de suivi / maintenance corrective

Connaissance des risques & vulnérabilités liés au développement applicatif

Besoin d'expertise

(1) Très bien développer (limiter les failles techniques)

Architecture + Expertise fonctionnelle (limiter les failles de conception)

(2) Méthode qualité logicielle
Gestion de projet
Approche qualité

(3) Expérience de test
Catalogue d'outils & pratiques
Expérience sur outils de tests

(4) Mise en production / exploitation
Mise en production / exploitation
Plateforme de distribution de correctifs

(5) Culture de sécurité + Audit
Analyse de risque fonctionnel
Analyse de vulnérabilité technique

Réponse au besoin d'expertise SSI

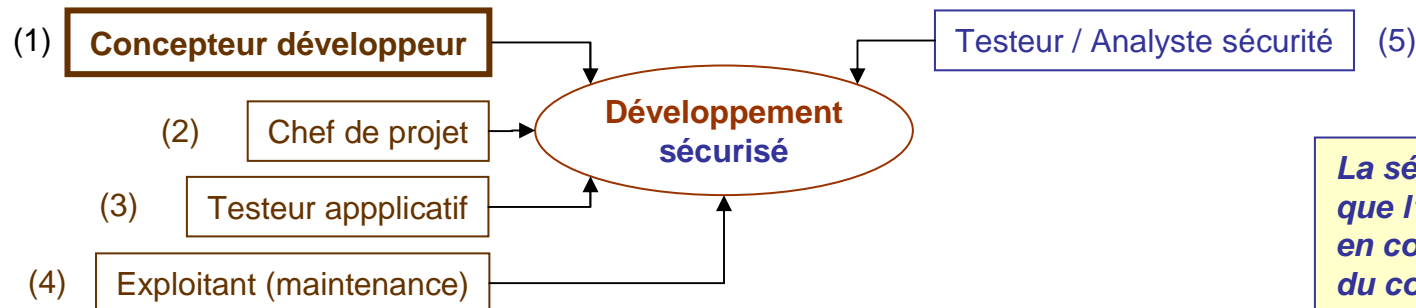
Mode d'acquisition :

- 1) Par l'**expérience**
- 2) Par **acquisition de connaissance**
 - Encadrement
 - Veille / autoformation
 - **Formation externe**
- 3) Par **acquisition de ressource**
 - Recrutement externe
 - Assistance technique

(!) La SSI est le domaine informatique qui sollicite le plus les capacités de veille

Selon la ressource existante

- (1) => Formation + Encadrement
(autres) => Recrutement + Encadrement



La sécurité est une 2^{ble} compétence que l'on peut acquérir par la formation en complément d'une très bonne expertise du coeur de métier (développeur)

Ex 2 : Administration & Supervision de la sécurité du SI

Coeur de métier

Administrateur systèmes
Windows, Unix, VM

Administrateur réseaux
WAN, (W)LAN, Filtrage TCP/IP

Administrateur applicatif
Appli. spé., ERP, middleware...

Approche sécurisée

Contrôle des standards
applicatifs et systèmes

Contrôle d'Intégrité
/ Sécurisation des flux

Contrôle d'accès utilisateur

Supervision des événements

Gestion des incidents / désastre

Besoin d'expertise sécurité

(1) Durcissement, monitoring,
Sauvegarde, haute disponibilité

(2) Expertise des solutions propriétaires
(Cisco, Checkpoint, Linux...)

(3) Segmentation, intégration de systèmes
(solutions propriétaires)

(3) Gestion du parc et des configurations
Stratégies de sécurité locale / groupe
Plateforme de gestion des mises à jours

(4) Outils AV, ASpam (locaux / réseaux)
Admin Firewall, VPN, SSL, PKI, ...
Admin Proxy, IDS, Honeypot, NAC...

(5) Admin. de domaine de ressources / annuaires
Charte utilisateurs, monitoring / reverse proxying
Solution globale d'identity access management (SSO...)

(6) Interconnexion / Remontées d'alertes des systèmes
Monitoring / Consolidation / Alerte de sécurité
Gestion / Suivi d'événements / Forensic

(7) Organisation de suivi des incidents + support IT
Plan de sauvegarde / restauration
Plan de continuité d'activité / gestion de crises

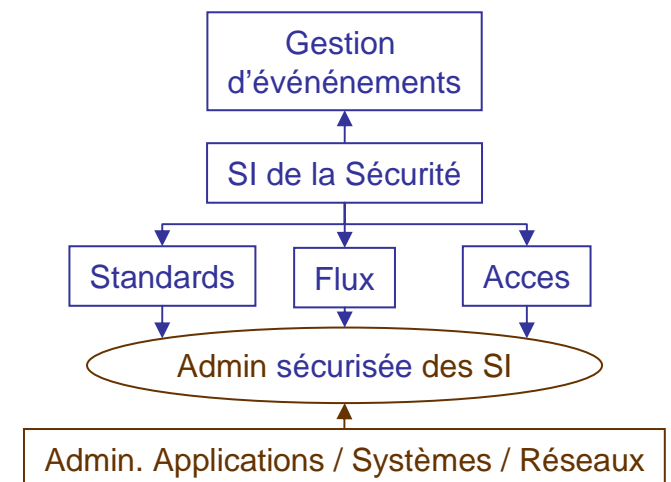
**La sécurité est une 2ble compétence
nécessite une très bonne compétence
dans le coeur de métier (administrateur)
... et de nombreuses formations**

Les exigences d'administration portent
sur le respect de :

- 1) l'intégrité des données
- 2) La disponibilité des services
- 3) La traçabilité des utilisateurs
- 4) La confidentialité des informations

Les formations permettant de maîtriser
les exigences de sécurité portent sur :

- 1) Les méthodes et process d'administration
- 2) Une vision globale du SI
- 3) La connaissance des failles et pratiques
- 4) L'expertise de solutions propriétaires



Sécurité = double compétence

Coeur de métier = Informatique

- ⇒ Développement informatique
- ⇒ Testeur
- ⇒ Administration réseaux & systèmes
- ⇒ Administrateur applicatif (ERP, SGBD, ...)
- ⇒ Administrateur du SI (domaine, utilisateurs, services...)
- ⇒ Concepteur / Intégrateur de systèmes (SI de la sécurité)
- ⇒ Gestionnaire de Parc / Support utilisateur
- ⇒ Chef de projet (déploiement de logiciels / infrastructures)
- ⇒ Auditeur informatique (analyse de risque, schéma directeur...)
- ⇒ Qualiticien (Iso, méthodes, domaines et best practices...)

Facteur d'excellence = Sécurité

- ⇒ Compréhension des failles de codage / vulnérabilités
- ⇒ Tests de vulnérabilité
- ⇒ Protocoles et fonctionnalités de sécurité
- ⇒ Segmentation, stratégies de sécurité,
- ⇒ Gestion centralisée / périmètre de sécurité / annuaire /...
- ⇒ Définition / Acquisition / Interprétation centralisé des alertes
- ⇒ Inventaire / classification des ressources / Gestion d'incident
- ⇒ Chef de projet (déploiement dédiés à la SSI)
- ⇒ Auditeur sécurité (tests de pénétration, vulnérabilité...)
- ⇒ Politiques de sécurité (Iso 27k, PDCA, analyse de risque, ltil...)

Définir le niveau d'expertise requis

Fondamentaux

- ⇒ Fondamentaux d'administration (réseaux & systèmes)
- ⇒ Fondamentaux de développement informatique (hacking, outils et SI)
- ⇒ Compréhension des Organisations, méthodes et process types
- ⇒ Enjeux et principes de la sécurité (vulnérabilités, menaces, risque...)
- ⇒ Formation aux méthodes de veille (autoformation / bulletin d'alerte)

Expertise pointue

- ⇒ Ingénierie d'organisation de la sécurité (audit / schéma directeur)
- ⇒ Formation propriétaires (expertise d'administration)
- ⇒ Certification (organisation & politiques, audit technique...)

Limiter le coût de la mise à niveau

Rationaliser l'informatique

- 1) Standards propriétaires
 - Complexité / compatibilité
 - Coût conseil / Formation des admin.
- 2) Obsolescence
 - Fin de support / formation / réappro
 - Gestion des RH
- 3) Approche globale
 - Interconnexion des systèmes
 - Mise en oeuvre de la politique globale

Rationaliser les formations

- ⇒ Standards (virtualisation, centralisation)
- ⇒ Ressources généralistes / stratégiques (internes)
- ⇒ Ressources atypiques (externes)

Exemple (*) de progression pédagogique de formation

(*) Licence pro Administration & Sécurité des Systèmes d'information

Développement logiciel

Génie logiciel

- Méthodologie de développement logiciel
- Méthodes et outils de tests
- Mise en pratique (Développement / framework)

Administration du Système d'information

Administration système
(Windows, Unix) + Durcissement
Virtualisation / Haute disponibilité

Administration réseau
WAN, (W)LAN, Filtrage TCP/IP

Administration applicative
nTiers, SGBD, C/S intranet

Administration d'un domaine
Stratégies de sécurité / groupe
Plateforme de mises à jours

Administration de la sécurité
Déploiement d'outils (AV, ASpam)
Firewall, Proxy, IDS, VPN, SSL, PKI

Système d'information de la sécurité
Interconnexion / Remontées des alertes
Monitoring / Consolidation / Alerte d'intervention
Gestion / Suivi d'événements / Forensic

Organisation de suivi des incidents
Plan de sauvegarde / restauration
Plan de continuité d'activité / gestion de crise

Environnement de la sécurité

- Sensibilisation par scénarisation**
Vulnérabilité / Menaces & Risques
Illustration technique des concepts
Environnement légal, Cybercriminalité et Intelligence économique
- Méthode de veille appliquée à la SSI et communication aux réseaux d'experts**
Mise en place d'une charte utilisateurs
Introduction aux méthodologies / normes

Compléments (RSSI, prestataire) :

- Ingénierie informatique sécurisée
- Développement logiciel sécurisé
- Théorie et technique de Cryptage
- Réalisation du SI de la sécurité
- Audit stratégique / organisationnel
- Organisation & Plan Qualité
- Conception de politique SSI
- Certification ISO (PDCA, risk, domaines...)

Solutions propriétaires

- Administration (réseau / systèmes / applications)
- Solutions intégrées de sécurité (IAM / SSO)

Audit de sécurité

- Outils/méthodes de tests de pénétration
- Prévention et réaction en cas d'attaque