Règlement du défi

SEC&SI

Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute

Le présent document constitue le règlement du défi « Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute.

Présentation générale

Le développement de la sécurité des systèmes d'information passe aussi par l'utilisation par le grand public de moyens sécurisés. Pour favoriser celle-ci, il est proposé à plusieurs équipes en compétition l'objectif de mettre à la disposition des citoyens un système d'exploitation sécurisé permettant d'accéder depuis un ordinateur aux services de banque en ligne, d'e-administration et à un service d'envoi de messages au minimum signés. Chaque équipe en compétition devra donc proposer une solution :

- **ergonomique** : l'utilisateur doit pouvoir continuer à utiliser son ordinateur sans changement, même si c'est cet ordinateur qui est utilisé pour l'usage des fonctions sécurisées ;
- **fonctionnelle** : la solution proposée devra être compatible des services en ligne couramment utilisés et l'utilisateur devra pouvoir stocker des éléments justificatifs éventuels ;
- **résistante aux agressions** : les vulnérabilités sur l'ordinateur et sur les applications utilisés ne doivent pas avoir un impact immédiat sur l'ensemble des applications sécurisées ;
- **adaptable** : la prise en compte des évolutions fonctionnelles et de sécurité nécessitera de pouvoir mettre à jour la solution, et ce de façon sécurisée.

Le défi s'organisera sur deux ans. Les équipes en compétition commenceront par proposer, à l'issue d'une phase de conception de six mois, une première version de leur solution. La période qui suivra sera l'occasion pour chaque équipe d'évaluer les solutions concurrentes au plan des différents critères ci-dessus. La mise en évidence de vulnérabilités sur les solutions concurrentes pourra faire l'objet de publications.

Présentation détaillée

Liste des équipes en compétition

Trois projets sont en compétition:

- le projet OSOSOSOS (Prononcer Foros), dont le coordinateur est Louis Granboulan (EADS IW);
- le projet Safe OS, dont le coordinateur est Thomas Hérault (Université Paris XI);

- le project SPACLik, dont le coordinateur est Christian Toinard (LIFO, ENSI Bourges).

Fonctionnalités attendues

L'idée du défi est de s'adresser à la population des internautes qui est donc habituée à des fonctionnalités graphiques intuitives. Les solutions proposées devront donc disposer d'une interface graphique.

Les fonctionnalités qui devront être disponibles sont au minimum les suivantes :

1. L'internaute dispose généralement d'un service de messagerie SMTP proposé par son fournisseur d'accès. La solution devra permettre d'utiliser ce service pour fournir un complément sécuritaire par la signature électronique des messages. Cette signature nécessitera de mettre en place dans la solution une ou plusieurs clés privées dont la sécurité devra bien entendu être assurée.
2. La télé-déclaration des impôts sur Internet est un processus désormais largement employé qui utilise une clé privée, des applications java et une possibilité d'accès sécurisé par https. La solution proposée devra permettre d'exploiter le service correspondant et de protéger les secrets nécessaires.
3. L'internaute est également de plus en plus enclin à accéder à des services en ligne sécurisés proposés par les banques, le commerce, les associations, les fournisseurs, les assurances, etc. Le standard de fait en matière de sécurité, observé pour ces services, est l'usage de SSL ou TLS, couplé à des services d'information non sécurisés basés sur http. La solution devra permettre d'utiliser ces services.
4. L'utilisation de ces différents services nécessite le plus souvent de pouvoir conserver des informations (récépissé de paiement, de déclaration, messages envoyés et reçus, etc.). La solution devra permettre une telle conservation en assurant la sécurité des données.
5. Tout système d'information, spécialement lorsqu'il est sécurisé, doit être en mesure de s'adapter à des évolutions matérielles, fonctionnelles ou à l'émergence de nouvelles menaces ou vulnérabilités. Ces évolutions doivent elles-mêmes être sécurisées pour garantir l'intégrité du système. Les solutions proposées devront intégrer ce besoin. Les mises à jour devront pouvoir être effectuées localement ou à distance depuis un serveur de mise à jour.

Planning détaillé

Un séminaire interne est organisé avant chaque phase d'évaluation pour que les équipes puissent présenter l'état d'avancement de leur projet. En raison du caractère novateur du défi SEC&SI, un séminaire supplémentaire sera organisé en fin de première phase d'évaluation. Les dates exactes des séminaires et le lieu de la rencontre seront précisés environ trois mois à l'avance.

- **1er octobre 2008** : Lancement du défi.
- **fin mars – début avril 2009** : Séminaire interne au défi de présentation

respective des propositions (date et lieu à préciser). Début de la période d'évaluation.

- **juin 2009** : Présentation des propositions au SSTIC ou en marge du SSTIC (à confirmer).
- **octobre 2009** : Clôture de la phase d'évaluation. Séminaire interne au défi de retour sur la phase d'évaluation. Ouverture de la deuxième phase de conception.
- **janvier 2010** : Séminaire interne au défi de présentation respective des propositions (date et lieu à préciser). Début de la deuxième phase d'évaluation.
- **avril 2010** : Fin de la deuxième phase d'évaluation. Ouverture de la troisième phase de conception.
- **juin 2010** : Présentation des propositions au SSTIC (à confirmer). Séminaire interne au défit de présentation des évolutions.
- **juillet 2010** : Début de la phase d'évaluation finale.
- **octobre 2010** : Annonce des résultats et débriefing.

Les trois équipes en compétitions sont classées par un jury sur la base de leur score. Afin d'assurer que le défi se déroule dans les meilleures conditions, les équipes s'engagent à coopérer avec le jury au maximum de leurs capacités. Les décisions du jury font autorité et sont irrévocables.

La constitution du jury est la suivante :

Yves Correc, DGA/CELAR;

Stéphane Coulondre, INSA Lyon;

Florent Chabaud, DCSSI;

Isabelle De Lamberterie, CNRS;

Yves Denneulin, Imag;

Éric Diehl, Thomson;

Loïc Duflot, DCSSI, Président;

Jean Goubault-Larrecq, ENS Cachan;

Sylvain Leroy, MINEFE;

Alain Merle, CEA.

Il n'est pas prévu que la composition du jury évolue au cours du défi. Cependant, si un changement dans cette composition était nécessaire, ce changement devrait être validé par le jury, l'ANR et les trois coordinateurs.

Le classement et les scores de chaque équipe sont remis à zéro après chaque période d'évaluation ce qui permettra aux équipes de tirer enseignement des attaques publiées sans pâtir, si les vulnérabilités correspondantes sont corrigées, de vulnérabilités des versions précédentes. Un classement différent sera donc obtenu lors de chaque phase d'évaluation. Est déclarée gagnante l'équipe dont la somme des trois classements est minimale. En cas d'ex-æquo, l'équipe gagnante est celle qui possède le score total (agrégé sur les trois phases) le plus élevé.

Exemple:

Phase 1: 1. Équipe B 2. Équipe C 3 Équipe A.	
Phase 2: 1. Équipe A 2. Équipe B 3 Équipe C.	
Phase 3: 1. Équipe A 2. Équipe C 3 Équipe B.	
Totaux des classements:	Équipe A: 3+1+1=5;
	Équipe B: 1+2+3=6;
	Équipe C: 2+3+2=7.
Vainqueur:	Équipe A.

Règles du défi

Proposition de solution

La plate-forme matérielle visée ne doit pas être contrainte. Il s'agit donc d'une architecture matérielle de type PC i386 disposant d'une MMU sur laquelle on peut imaginer que l'internaute fait tourner de façon habituelle un système d'exploitation quelconque (Dos, Windows 95, XP, Vista, Linux, BSD, etc.). L'idée est que la majorité des internautes doivent pouvoir utiliser les solutions proposées, donc on ne devra pas faire d'hypothèse réductrice sur les fonctionnalités de sécurité matérielles disponibles (par exemple extensions matérielles pour la virtualisation, IOMMU, TPM, etc.). La présence de telles fonctions pourra par contre être utilisée pour renforcer la sécurité de la solution dans ce cas ; le mécanisme de notation des solutions tiendra compte de telles initiatives (voir ci-dessous).

Les équipes devront proposer une solution basée sur un système d'exploitation Linux utilisant un noyau 2.6. Cette règle est destinée à faciliter la comparaison des solutions et à rendre plus facile l'évaluation croisée des solutions par les équipes. Elle vise aussi à pouvoir proposer des solutions s'adaptant à la diversité des plates-formes matérielles existantes.

Les équipes sont libres de modifier le noyau, d'appliquer des patches, de choisir leur distribution de base dans le respect des licences applicables.

La solution ne devra s'appuyer que sur du logiciel libre et, si nécessaire, sur des outils non libres mais gratuits, utilisables et diffusables librement dans le cadre correspondant à ce défi, c'est-à-dire un usage non commercial à des fins de recherche.

Règles de publication

Les équipes devront proposer en téléchargement leur solution et son code source pour que chaque équipe puisse procéder à son analyse. Cette mise à disposition devra être étendue sur l'internet au bout de 9 mois, pour que des analyses extérieures soient possibles. La solution devra être associée à une licence libre. La conception de la solution devra être documentée et présentée lors des séminaires organisés à cet effet.

Une équipe ayant mis en évidence une vulnérabilité d'une solution concurrente doit impérativement et dans le même temps :

- prévenir le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques de la DCSSI (CERTA) de cette

vulnérabilité ;

- Alerter l'équipe concurrente afin qu'elle soit en mesure de corriger la vulnérabilité ;
- prévenir le ou les responsables des développements éventuellement impactés. Il est important de tenir le CERTA au courant des démarches qui auront été entreprises pour lui donner la possibilité de suivre ces démarches et le cas échéant d'en initier d'autres ;
- signaler au jury la découverte d'une vulnérabilité (sans détails). Le CERTA transmettra au jury les éléments nécessaires à la cotation de l'attaque (voir plus bas).

La publication d'une vulnérabilité ne peut intervenir qu'une fois que le CERTA a donné son autorisation pour cette publication. La publication pourra ensuite bien entendu se faire à l'initiative de l'équipe ayant mis en évidence la vulnérabilité, sauf si cette dernière ne souhaite pas publier sur le sujet.

Règles de comparaison des solutions

Règles sur les attaques

Seront seules prises en compte pour le classement les attaques logiques sur le PC utilisateur équipé des solutions proposées. Les attaques physiques sur le PC de l'utilisateur, de même que l'espionnage de ses actions par un dispositif extérieur (« keylogger » par exemple) ne seront pas prises en compte. Sont **interdites** les attaques sur les services qui ne sont pas élaborés au titre de l'appel à projet mais qui font partie du périmètre utilisé par l'internaute (banque en ligne, commerce en ligne, télé-déclaration des impôts, etc.). Une proposition qui utiliserait un service en ligne particulier pour assurer des fonctions de sécurité (par exemple un serveur de mise à jour), ne pourra pas être attaquée au niveau de ce service ; il sera par contre possible de formuler des attaques théoriques de ce service sur la base des éléments de conception présentés. Ces attaques ne seront comptabilisées que dans la mesure où elles ont un impact sur la cible.

Il ne sera fait aucune hypothèse restrictive sur les capacités d'un attaquant réel. Celui-ci peut disposer d'un serveur malveillant sur l'internet, de capacités d'usurpation d'adresse IP, d'un réseau botnet, etc.

Principes du classement

Au départ, toutes les équipes se voient attribuer un score forfaitaire S_V de 100 points.

Le jury établit de façon régulière (tous les mois et demi) un classement des équipes pendant les phases d'évaluation. Ce comité juge souverainement et sans recours des litiges éventuels dans la constatation de la réalité d'une attaque ou de la vraisemblance de ses hypothèses. Il attribue en outre en fin de chaque phase d'évaluation une note d'ergonomie de la solution pour une proportion minoritaire des points en jeu.

Les différentes équipes participantes peuvent présenter au CERTA des attaques contre une autre solution. La démonstration de la validité d'une attaque fait gagner un certain nombre de points à une équipe, qui sont

équilibrés par les points perdus par l'autre équipe. En effet, à chaque attaque est associée une note (voir ci-dessous) A qui correspond au pourcentage des points de la solution vulnérable qui sera gagné par l'équipe ayant mis la vulnérabilité en évidence.

Le CERTA est garant de la confidentialité des attaques présentées jusqu'à ce que les conditions requises pour leur publication soient remplies. Le classement publié pourra ainsi faire mention de vulnérabilités ouvertes sans révéler la nature de ces vulnérabilités.

Si des attaques sont mises en évidence par des équipes ne participant pas au projet, les solutions vulnérables perdront des points que les solutions non vulnérables gagneront.

Une vulnérabilité qui affecterait de façon équivalente toutes les solutions ne sera pas comptabilisée : elle sera considérée comme une vulnérabilité résiduelle inévitable, sauf à ce que l'une des équipes démontre le contraire, auquel cas elle bénéficiera des points correspondant.

Le jury peut s'il le souhaite conduire une évaluation des solutions proposées. Cependant, pour des raisons évidentes de déontologie et de façon à ne pas artificiellement privilégier une solution par rapport à une autre, le jury ne peut pas modifier le score d'une solution pour une vulnérabilité qu'il aurait lui même mis en évidence. Le jury ne peut communiquer à quiconque le code source des solutions tant que ce dernier n'a pas été publié.

Biens à protéger

Pour permettre une comparaison la plus objective possible des solutions, seules les attaques sur les biens listés dans le tableau ci-dessous seront comptabilisées. En d'autres termes, une attaque sera considérée comme réussie si une atteinte à la confidentialité (C), à l'intégrité ou à l'authenticité (I) ou à la disponibilité (D) de l'un de ces biens est observée ou déduite des hypothèses réalistes annoncées de l'attaque.

Le tableau ci-dessous précise également un coefficient d'importance de l'attaque, c'est-à-dire une estimation de l'impact de celle-ci. Si une attaque concerne plusieurs biens, les mesures d'impact s'additionnent. Ces coefficients correspondent au pourcentage mis en jeu du score de la solution attaquée.

Bien concerné	Exemple de scénario possible	Mesure de l'impact			Commentaire
		I	C	D	
PC utilisateur	Utiliser une vulnérabilité de la solution proposée pour accéder à des données de l'utilisateur ou altérer son système natif ou l'empêcher d'utiliser la solution proposée.	4	2	1	La solution doit évidemment être fonctionnelle (D), mais elle doit de façon encore plus importante ne pas induire de vulnérabilité sur la configuration de l'utilisateur. La lecture d'informations pourrait ainsi compromettre des données personnelles de l'utilisateur et une atteinte à l'intégrité du système natif serait encore davantage dommageable.
Biens utilisateur sur	Récupérer ou altérer des données sensibles que	4	2	1	Ceci vise la fonctionnalité demandée de conservation sécurisée des

PC	l'utilisateur a obtenues ou élaborées lors de l'usage de ses services en ligne (récépissé de télé-déclaration, message envoyé, etc.)				données. Là encore, l'altération des données à l'insu de l'utilisateur est la menace ayant le plus d'impact.
Clés utilisateur sur PC	Récupérer ou altérer les éléments secrets cryptographiques dont l'utilisateur dispose pour accéder à ses services ou signer ses messages.	1	4	1	Ici l'altération de l'intégrité de la clé revient à la rendre indisponible puisqu'elle n'est plus utilisable pour l'accès au service. Par contre, si une clé privée est compromise, l'attaquant va pouvoir usurper l'identité de l'utilisateur et accéder en ligne et en différé à l'intégralité des données protégées par cette clé.
Biens utilisateur sur service	Profiter de la connexion de l'utilisateur pour usurper son identité, accéder aux données qu'il manipule ou modifier le logiciel pour qu'il mémorise ces données ou profiter d'erreurs d'effacement pour retrouver des informations de sessions antérieures, etc.	4	2	1	L'intégrité des données présentes sur le site est évidemment la propriété la plus recherchée. Une usurpation d'identité est considérée comme équivalente à l'altération des données d'authentification. Une destruction sur le site de données préalablement enregistrées par l'utilisateur serait d'ailleurs également considérée comme une atteinte en intégrité. Une attaque empêchant l'utilisateur d'accéder à ces informations mais sans que ces dernières soient altérées sur le site serait considérée comme une atteinte en disponibilité.
Mises à jour sécurisées	Introduire des mises à jour erronées dans le système.	2	0	1	La disponibilité des mises à jour est importante mais peut être empêchée au niveau réseau. L'introduction de mises à jour erronées n'a un impact important que si cela permet de monter une attaque sur les autres biens qui sera alors comptabilisée, d'où un coefficient d'impact relativement faible.

Gravité de l'attaque

L'impact d'une attaque sera en outre multiplié par un facteur d'aggravation :

Type d'attaque	Coeff.	Commentaire
ciblée	1	L'attaque doit viser un internaute particulier. Elle nécessite, par exemple, que son matériel soit vulnérable à une attaque particulière. Dans ce cas il n'y a pas d'aggravation.
générique	2	L'attaque peut être appliquée à tout internaute qui utiliserait cette solution. Par exemple, une vulnérabilité logicielle de la solution est exploitable par un virus. Dans ce cas l'impact est doublé.
systématique	4	L'attaque a un impact immédiat sur tous les internautes utilisant la solution. Par exemple, le système de mise à jour est percé ou une clé de sécurisation du système est compromise.
théorique	¼	Une attaque peut être démontrée moyennant des hypothèses de capacités d'attaque réalistes mais difficiles à mettre en œuvre

		(disponibilité d'un botnet, de capacité mémoire importante, prise de contrôle par l'attaquant d'un service distant, etc.) ou de vulnérabilité réalistes sur certains composants du système : - le navigateur web ; - le client de messagerie ; - une librairie partagée ; - etc. Dans ce cas, un coefficient réducteur est appliqué. Le fait que ce coefficient ne soit pas nul encourage à publier toute vulnérabilité structurelle et à corriger ces faiblesses avant qu'elles ne deviennent exploitables.

Si une solution propose une version destinée aux architectures 64 bits, toute attaque sur cette version sera considérée comme ciblée. Inversement, une attaque générique sur la version i386 se verra attribuée le coefficient d'aggravation 2, même si elle n'est pas applicable aux architectures 64 bits. Ceci vise à ne pas trop pénaliser une proposition qui chercherait à étendre le spectre des configurations matérielles utilisables, tout en privilégiant la sécurité de la configuration majoritairement rencontrée.

Mode de calcul

Pour une attaque donnée, l'impact de l'attaque (la note) A est calculé en sommant les différentes atteintes aux biens réalisées.

La note *A* de l'attaque est ensuite divisée par 100 puis multipliée par le score S_V de la solution attaquée, pour donner le nombre de points qui seront retranchés à la solution vulnérable et ajoutés à l'équipe ayant démontré l'attaque. Le total est arrondi au point supérieur.

Exemple: une attaque possédant une note d'impact A=12, sur une solution possédant un score de Sv=80 points permettra à l'équipe ayant mis en évidence l'attaque de marquer 12*80/100= 9,6 points (arrondi à 10 points). L'équipe impactée perd 10 points (son score devient donc 70). Une attaque notée 20 sur une solution possédant Sv=50 points permettrait également de marquer 10 points.

Une attaque sur une « bonne » solution rapporte donc davantage de points. Inversement, une solution qui aurait déjà été démontrée largement vulnérable pourrait avoir un nombre de points proche de zéro et le score global de l'attaque serait alors proche de 0 également. Enfin, une attaque rapporte au plus S_V points, c'est-à-dire que la note *A* de l'attaque est au plus de 100%.

Correction des vulnérabilités ouvertes

Afin d'encourager à la correction des vulnérabilités avérées, les attaques non théoriques n'ayant pas fait l'objet d'une correction sont comptabilisées toutes les deux semaines. Toutefois, pour éviter de trop favoriser l'équipe à l'origine de l'attaque, à compter de la deuxième semaine, les points gagnés sont répartis à parts égales entre les propositions non vulnérables (Si le nombre de point gagné est impair (2n+1 points), l'équipe ayant mis en évidence la vulnérabilité marque n+1 points).

La correction d'une vulnérabilité permet de récupérer ¾ des points perdus la quinzaine précédant la correction. Ainsi, une attaque avérée qui serait

immédiatement corrigée se retrouverait comptabilisée comme une attaque théorique. Inversement, la correction tardive d’une vulnérabilité ne rapportera qu’une part faible voire négligeable des points perdus.

Calcul du classement

Le calcul des points échangés lors des attaques ou par correction de vulnérabilités intervient dans l’ordre des annonces auprès du jury. Le classement est publié chaque mois.

Note d’ergonomie

À la fin de chaque période d’évaluation, le jury procède au classement des différentes solutions par rapport aux caractéristiques ergonomiques et fonctionnelles des propositions. Le classement donne lieu à un échange de 2 points par rang au tour préliminaire, de 5 points par rang au deuxième tour et de 10 points au tour final. Les équipes classées ex-æquo se partagent les points en jeu.

Exemple : Si au troisième tour, deux équipes sont classées premières ex-æquo au plan de l'ergonome, elles gagnent chacun cinq points et la dernière équipe perd 10 points.

La possibilité d'utilisation de fonctionnalités ou de plugins supplémentaires (flash, real audio, etc.) n'est pas requise, mais il sera tenu compte des apports correspondants en termes d’ergonomie. De même, la prise en compte des architectures 64 bits sera également comptabilisée.

Annexe: exemple de déroulé d'une phase d'évaluation

Début de la phase d'évaluation

0/ Au début de la phase d'évaluation, les 3 équipes possèdent 100 points

Solution A: S_A=100

Solution B: S_B=100

Solution C: S_C=100

1/ L'équipe A met en évidence une faiblesse théorique des solutions B et C. Si un attaquant connait une faille du navigateur retenu par ces deux solutions, alors il lui est possible d'accéder aux clefs d'authentification de l'utilisateur pour l'ensemble des services distants.

Seules les clés cryptographiques locales sont impactées par l'attaque. Le jury décide que l'impact de cette attaque est de 1 en intégrité, 4 en confidentialité et 1 en disponibilité. La note d'impact de cette attaque est donc de 6. L'attaque étant théorique, le facteur de criticité est de ¼. La note de l'attaque est donc de 1.5.

Les solutions B et C perdront donc 1.5% de leur score (arrondi au point supérieur, soit deux points) au profit de la solution A. Le score de chaque solution devient alors:

Solution A: S_A=104

Solution B: S_B=98

Solution C: S_C=98

2/ L'équipe A trouve effectivement une vulnérabilité dans le navigateur utilisé par la solution B (mais pas dans celui utilisé par la solution C), et peut produire une preuve de concept pour le scenario d'attaque présenté ci avant.

La note d'impact de cette attaque est toujours de 6. Cette fois, l'impact est générique (toutes les postes utilisant la solution sont impactés), mais n'est pas systématique car les clefs cryptographiques récupérées par l'attaquant sont propres à chaque utilisateur. Le facteur de criticité est donc de 2. La note de l'attaque est elle de 12.

La solution B perdra donc 12% de son score (arrondi supérieurement soit 12 points) au profit de la solution A. Le score de l'équipe C ne bouge pas. Le score devient alors:

Solution A: S_A=116

Solution B: S_B=86

Solution C: S_C=98

3/ Une semaine s'écoule, l'équipe B n'a pas corrigé la vulnérabilité. Elle pert encore 12 points. Les points perdus sont cette fois partagés entre les solutions

A et C (6 points pour A et 6 pour C). Le score devient alors:

Solution A: S_A=122

Solution B: S_B=74

Solution C: S_C=104

4/ L'équipe B parvient à corriger la vulnérabilité. Elle récupère alors ¾ des points perdus la semaine précédente soit 9% de son score au moment de la mise en évidence de la vulnérabilité (arrondi supérieurement soit 8 points). Les points ayant été distribués aux équipes A et C, le score de chacune de ces équipes diminue de 4 points.

Solution A: S_A=118

Solution B: S_B=82

Solution C: S_C=100

Fin de la phase première phase d'évaluation

5/ Le jury constate que la solution A est la moins ergonomique, alors que la solution C est elle très facile d'utilisation. 2 points sont perdus par l'équipe A au profit de l'équipe C.

Le classement à l'issue de la première phase d'évaluation des donc:

1er Solution A: S_A=116

2nd Solution C: S_C=102

3ème Solution B: S_B=82.