|  |  |
| --- | --- |
| **Bureau de la normalisationdes télécommunications** | **logo_F_** |
|  |  |

 Genève, le 27 septembre 2012

|  |  |  |
| --- | --- | --- |
| Réf.:Tél.:Fax:E-mail: | **Circulaire TSB 311**COM 17/ MEU+41 22 730 5866+41 22 730 5853tsbsg17@itu.int | - Aux administrations des Etats Membres de l'Union |
|  |  | **Copie**:- Aux Membres du Secteur UIT-T;- Aux Associés de l'UIT-T;- Aux établissements universitaires participant aux travaux de l'UIT-T;- Aux Président et Vice-Présidents de la Commission d'études 17;- Au Directeur du Bureau de développement des télécommunications;- Au Directeur du Bureau desradiocommunications |

|  |  |
| --- | --- |
| Objet: | **Réunion de la Commission d'études 17 en vue d'approuver les projets de nouvelle Recommandation UIT-T X.1126, X.1154, X.1526 et X.1544 conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Johannesburg, 2008),****Genève, le26 avril 2013** |

Madame, Monsieur,

1 A la demande du Président de la Commission d'études 17, *Sécurité*, j'ai l'honneur de vous informer que ladite Commission d'études, qui se réunira du 17 au 26 avril 2013, a l'intention d'appliquer la procédure décrite dans laSection 9 de la Résolution 1 de l'AMNT (Johannesburg, 2008) pour l'approbation des projets de nouvelle Recommandation mentionnés ci-dessus.

2 Vous trouverez dans l'**Annexe 1** le titre, le résumé et la localisation des projets de nouvelle Recommandation UIT-T proposés pour approbation.

3 Tout Etat Membre, Membre de Secteur, Associé de l'UIT ou établissement universitaire participant aux travaux de l'UIT; constatant qu'un brevet, dont lui ou une autre organisation est titulaire, couvre peut-être, en totalité ou en partie, des éléments des projets de Recommandation qu'il est proposé d'approuver est invité à communiquer ces renseignements au TSB, conformément à la politique commune de l'UIT-T, l'UIT-R, l'ISO et la CEI en matière de brevets.

Les renseignements existants sur les brevets sont accessibles en ligne sur le site web de l'UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Compte tenu des dispositions de laSection 9 de la Résolution 1, je vous serais reconnaissant de bien vouloir me faire savoir au plus tard **le 5 avril 2013** à 24 heures UTC si votre Administration autorise la Commission d'études 17 à examiner, lors de sa réunion, lesdits projets de nouvelle Recommandation aux fins d'approbation.

Si des Etats Membres estiment que la procédure d'approbation ne doit pas se poursuivre, ils sont invités à faire connaître leurs raisons et à proposer les modifications susceptibles de permettre la reprise des procédures d'examen et d'approbation des projets de nouvelle Recommandation.

5 Si au moins 70% des réponses des Etats Membres sont en faveur de l'examen, aux fins d'approbation, de ces projets de nouvelle Recommandation lors de la réunion de la Commission d'études, **une séance plénière se tiendra le 26 avril 2013** pour appliquer la procédure d'approbation.

En conséquence, j'invite votre Administration à se faire représenter à cette réunion. Les **administrations des Etats Membres de l'Union** sont invitées à communiquer le nom du Chef de leur délégation. Si votre Administration souhaite se faire représenter à cette réunion par une exploitation reconnue, un organisme scientifique ou industriel, ou une autre entité s'occupant de questions de télécommunications, le Directeur doit en être informé, conformément à l'article 19, numéro 239, de la Convention de l'UIT.

6 L'ordre du jour ainsi que tous les renseignements pertinents concernant la réunion de la Commission d'études 17 seront disponibles dans la Lettre collective qui sera publiée ultérieurement.

7 Après la réunion, le Directeur du TSB fera connaître, par voie de circulaire, la décision prise au sujet de ces Recommandations. Cette information sera également publiée dans le Bulletin d'exploitation de l'UIT.

Veuillez agréer, Madame, Monsieur, l'assurance de ma haute considération.

Malcolm Johnson
Directeur du Bureau de la
normalisation des télécommunications

**Annexe**:1

**ANNEXE 1
(de la Circulaire TSB 311)**

Résumé et localisation des textes

Projet de nouvelle Recommandation UIT-T X.1126 (X.msec-6), Aspects de sécurité des téléphones intelligents
COM 17 – R 67

Résumé

Avec le développement constant des fonctionnalités et l'expansion des applications, les téléphones intelligents sont exposés à de nombreuses menaces au plan de la sécurité, susceptibles d'avoir de graves conséquences sociales et économiques. La Recommandation UIT-T X.1126 vise à protéger la vie privée des utilisateurs et à améliorer la sécurité du système d'information des téléphones intelligents.

Cette Recommandation définit les menaces sur les téléphones intelligents qui entrent dans la catégorie des vulnérabilités et des attaques. Pour répondre aux objectifs de sécurité, la Recommandation spécifie un cadre de sécurité hiérarchisé et les exigences de sécurité auxquelles doivent répondre les téléphones intelligents. En ce qui concerne le cadre de sécurité, cette Recommandation fournit les solutions nécessaires par des améliorations au système et des outils de protection de la sécurité.

Projet de nouvelle Recommandation UIT-T X.1154 (X.sap-4), Cadre général de l'authentification combinée dans un environnement à plusieurs fournisseurs de services d'identité
COM 17 – R 68

Résumé

Depuis récemment, de nombreux services d'application, en particulier les services financiers, ont besoin de méthodes d'authentification combinées ou plus fiables comme l'authentification à plusieurs facteurs pour faire face à l'augmentation des vols d'identité. Par exemple, des méthodes reposant sur un mot de passe à usage unique et d'autres nouvelles méthodes d'authentification sont utilisées au lieu des authentifications fondées sur un mot de passe traditionnelles.

La combinaison des méthodes d'authentification donne aux fournisseurs de services d'identité (IdSP) les moyens de mieux garantir l'authentification. La Recommandation UIT-T X.1154 fournit le cadre général de l'authentification combinée dans les environnements à IdSP multiples pour un fournisseur de services. Dans cette Recommandation, trois types de méthodes d'authentification combinée sont envisagées: l'authentification multifacteur, l'authentification multi-méthodes et les authentifications multiples.

Le cadre de la Recommandation décrit les modèles, opérations de base et exigences de sécurité pour chaque composant de modèle et chaque message entre les composants de modèle de sorte à maintenir un niveau général de la garantie d'authentification dans les situations où interviennent de multiples IdSP.

En outre, le cadre décrit les modèles, opérations de base et exigences de sécurité pour la prise en charge du service d'authentification qui gère une combinaison de IdSP multiples.

Projet de nouvelle Recommandation UIT-T X.1526 (x.oval), Langage ouvert d'évaluation de la vulnérabilité (Open Vulnerability and Assessment Language) (OVAL)
COM 17 – R 64

Résumé

Cette Recommandation porte sur le langage ouvert d'évaluation de la vulnérabilité (Open Vulnerability and Assessment Language), OVAL, norme communautaire internationale de sécurité de l'information conçue dans le but de promouvoir un contenu de sécurité ouvert et accessible publiquement, et de normaliser le transfert de cette information à travers l'ensemble des outils et services de sécurité. OVAL inclut un langage utilisé pour coder les données du système et différents référentiels de contenu tenus dans toute la communauté. Le langage normalise les trois étapes principales du processus d'évaluation: la collecte des informations de configuration des systèmes à des fins de test; l'analyse du système pour détecter la présence dans la machine de vulnérabilités, problèmes de configuration ou correctifs de logiciel spécifiques; et la présentation des résultats de cette évaluation. Les référentiels sont des collections de contenus accessibles au public et ouverts qui utilisent le langage.

La communauté OVAL a mis au point trois schémas écrits en langage de balisage extensible (XML) pour servir de cadre et de vocabulaire au langage OVAL. Ces schémas correspondent aux trois étapes du processus d'évaluation: un schéma des caractéristiques du système OVAL pour représenter les informations du système, un schéma de définition OVAL pour exprimer l'état d'une machine spécifiée et un schéma de présentation des résultats OVAL pour rendre compte des résultats de l'évaluation.

Le contenu écrit en langage OVAL est situé dans l'un des nombreux référentiels trouvés dans la communauté. Ce référentiel est appelé le référentiel OVAL. Il est le lieu de rencontre central où la communauté OVAL discute, analyse, stocke et diffuse les définitions OVAL. Chaque définition dans le référentiel OVAL détermine si une vulnérabilité logicielle spécifique, un problème de configuration, un programme ou un patch est présent sur le système.

La communauté de la sécurité de l'information contribue au développement d'OVAL en participant à la création du langage OVAL sur le Forum des développeurs OVAL et en écrivant des définitions pour le référentiel OVAL à travers le Forum de la communauté OVAL. Un comité OVAL, composé de représentants d'un large éventail d'industries, d'établissements universitaires et d'organisations gouvernementales du monde entier, supervise et approuve le langage OVAL et surveille l'affichage des définitions hébergées sur le site web OVAL. Cela signifie qu'OVAL reflète les idées et l'expertise combinée du plus large ensemble de professionnels possible dans le domaine de la sécurité et de l'administration des systèmes dans le monde entier.

Projet de nouvelle Recommandation UIT-T X.1544 (X.capec), Enumération et classification des motifs d'attaque communs (CAPEC)
COM 17 – R 65

Résumé

La Recommandation sur l'énumération et la classification des motifs d'attaque communs (CAPEC) est une spécification basée sur XML/XSD pour l'identification, la description et l'énumération des modèles d'attaque. Les modèles d'attaque sont un mécanisme puissant pensé pour pouvoir se mettre dans la perspective de l'attaquant. Ils décrivent les méthodes communes d'exploitation des failles de logiciels. Ces descriptions dérivent du concept de modèles de conception (design patterns) appliqué dans un contexte de destruction et non de construction et sont générées à partir d'une analyse en profondeur d'exemples d'exploitation des failles en temps réel. L'objectif de CAPEC est de mettre à la disposition du public un catalogue des modèles d'attaque ainsi qu'un schéma global et une taxinomie de classification.

Le CAPEC permet de:

• normaliser la saisie et la description des modèles d'attaque;

• réunir les modèles d'attaques connus en une énumération intégrée qui puisse être mise à profit de manière efficace et systématique par la communauté;

• classer les modèles d'attaques de sorte que les utilisateurs puissent facilement identifier le sous-ensemble de l'énumération complète qui est approprié dans leur contexte;

• associer les modèles d'attaque et les faiblesses (CWE) contre lesquelles ils sont utiles par des références explicites.

Le plus grand nombre de sources et d'exemples possibles sont mis à profit par la communauté CAPEC et d'autres parties intéressées en vue d'élaborer les définitions spécifiques et succinctes du Dictionnaire CAPEC et diverses arborescences de vues et de classement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_