Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1544

(04/2013)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange concernant les événements/les incidents/l'heuristique

Liste et classification des schémas d'attaque courants

Recommandation UIT-T X.1544

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	**X.1540–X.1549**
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1544

Liste et classification des schémas d'attaque courants

Résumé

La Recommandation UIT-T X.1544 est une spécification fondée sur le langage XML/XSD pour l'identification, la description et l'énumération des schémas d'attaque, lesquels sont un moyen puissant de cerner et de présenter le mode de fonctionnement de l'attaquant. Ces schémas sont des descriptions des méthodes courantes utilisées pour l'exploitation des logiciels. Ils découlent de schémas de conception appliqués à des fins destructrices plutôt que constructives et résultent de l'analyse approfondie d'exemples spécifiques d'exploitation concrète. L'objectif de la Recommandation "Liste et classification des schémas d'attaque courants" (CAPEC) est de mettre à la disposition du public un catalogue des schémas d'attaque ainsi qu'un schéma global et une taxonomie de classification.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1544	2013-04-26	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

La Recommandation "Liste et classification des schémas d'attaque courants (CAPEC, *common attack pattern enumeration and classification*)" est une spécification fondée sur le langage XML/XSD pour l'identification, la description et l'énumération des schémas d'attaque, lesquels sont un moyen puissant de cerner et de présenter le mode de fonctionnement de l'attaquant. Ces schémas sont des descriptions des méthodes courantes utilisées pour l'exploitation des logiciels. Ils découlent de schémas de conception appliqués à des fins destructrices plutôt que constructives et résultent de l'analyse approfondie d'exemples spécifiques d'exploitation concrète. L'objectif de la liste CAPEC est de mettre à la disposition du public un catalogue des schémas d'attaque ainsi qu'un schéma global et une taxonomie de classification.

La liste CAPEC permet:

- de normaliser l'identification et la description des schémas d'attaque;
- de regrouper les schémas d'attaque connus dans une liste intégrée pouvant être utilisée régulièrement et dans de bonnes conditions par la communauté;
- de classer les schémas d'attaque afin que les utilisateurs puissent facilement reconnaître le sous-ensemble de la liste complète, qui convient dans leur situation;
- de relier moyennant des références explicites les schémas d'attaque et les listes des failles courantes (CWE, *common weakness enumeration*) dont ils tirent parti.

La Recommandation UIT-T X.1544 a été élaborée sachant qu'il importait de maintenir, dans la mesure du possible, la compatibilité technique avec la version 1.0 des "*Prescriptions et Recommandations concernant la compatibilité CAPEC*" publiée par la MITRE Corporation, le 30 août 2012 (https://capec.mitre.org/compatible/requirements_v1.0.html).

Recommandation UIT-T X.1544

Liste et classification des schémas d'attaque courants

1 Domaine d'application

La présente Recommandation permet l'échange structuré de schémas d'attaque accessibles au public et fournit un schéma global et une taxonomie de classification.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité (CYBEX).*

3 Définitions

3.1 Termes définis ailleurs

Les termes suivants définis ailleurs sont utilisés dans la présente Recommandation:

3.1.1 autorité d'examen [b-UIT-T X.1520]: entité qui procède à un examen et est autorisée à accorder le statut de compatibilité avec la liste CAPEC (compatibilité CAPEC).

NOTE – MITRE est à ce jour la seule autorité d'examen.

3.1.2 vulnérabilité [UIT-T X.1500]: toute faille dans un logiciel susceptible d'être exploitée pour violer un système ou les informations qu'il contient [UIT-T X.1500].

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 pourcentage d'exactitude: pourcentage d'éléments de sécurité dans l'échantillon, qui renvoient aux identificateurs CAPEC corrects.

3.2.2 cas d'attaque: attaque précise contre une application ou un système donné, qui cible les vulnérabilités ou les failles de ce système.

3.2.3 schéma d'attaque: concept qui découle de l'observation des méthodes d'attaque courantes, lâchées dans la nature contre des applications ou des systèmes (par exemple, l'injection SQL, "l'attaque de l'homme du milieu" ou le détournement de session, etc.).

NOTE – Un même schéma d'attaque peut être associé à de nombreux cas d'attaques différents.

3.2.4 instrument: outil d'évaluation, outil d'évaluation dynamique de la sécurité des applications (DAST), outil d'évaluation de la pénétration, outil cadre pour les exploitations, outil de modélisation des menaces, base de données, site web, conseil ou service fournissant des informations sur les cas et les schémas d'attaque.

3.2.5 mise en correspondance/mappage: spécification des relations entre les éléments des schémas d'attaque dans un recueil et les éléments de la liste CAPEC qui sont liés à ces éléments.

3.2.6 propriétaire [basé sur b-UIT-T X.1520]: gardien (personne réelle ou société) en charge de l'instrument (tel que défini dans la présente Recommandation).

3.2.7 recueil: ensemble implicite ou explicite des éléments des schémas d'attaque, qui vient à l'appui d'un instrument, par exemple une base de données des schémas d'attaque, l'ensemble des cas d'attaque dans un outil DAST ou un site web.

3.2.8 examen: processus permettant de déterminer si un instrument est compatible avec la liste CAPEC.

3.2.9 version de l'examen: version datée de la liste CAPEC qui est utilisée pour déterminer la compatibilité CAPEC d'un instrument.

3.2.10 élément de sécurité: enregistrement dans une base de données, sonde d'évaluation, cas d'attaque, exploitation, charge utile, etc., qui est lié(e) à un schéma d'attaque donné.

3.2.11 mission: sonde, vérification, signature, etc., par un outil, qui exécute une action fournissant des informations sur la sécurité (c'est-à-dire l'élément de sécurité).

3.2.12 outil: application ou dispositif au logiciel qui évalue les propriétés de sécurité d'une application ou d'un système au moyen de la simulation, l'émulation ou la caractérisation d'attaques potentielles contre ce système, par exemple, un outil d'évaluation, un outil d'évaluation dynamique de la sécurité des applications (DAST), un outil d'évaluation de la pénétration, un outil cadre pour les exploits, un outil de modélisation des menaces.

3.2.13 utilisateur [basé sur b-UIT-T X.1520]: consommateur ou consommateur potentiel de l'instrument.

3.2.14 faille: lacune ou imperfection dans le code logiciel, la conception, l'architecture ou le déploiement d'un logiciel qui pourrait, à un moment donné, devenir une vulnérabilité, ou pourrait contribuer à l'introduction d'autres vulnérabilités.

4 Abréviations et acronymes

Les abréviations et acronymes suivants sont utilisés dans la présente Recommandation:

CAPEC liste et classification des schémas d'attaque courants (*common attack pattern enumeration and classification*)

CCR représentation de déclaration de couverture (*coverage claim representation*)

CIA confidentialité, intégrité ou disponibilité (*confidentially, integrity or availability*)

CWE liste des failles courantes (*common weakness enumeration*)

DAST outil d'évaluation dynamique de la sécurité des applications (*dynamic application security testing tool*)

GUI interface graphique utilisateur (*graphical user inerface*)

IDS système de détection d'intrusion (*intrusion detection system*)

POC point de contact

5 Conventions

Les mots clés "requis", "doit", "ne doit pas", "devrait", "ne devrait pas", "recommandé", "peut" et "facultatif" utilisés dans la présente Recommandation sont interprétés conformément au guide des auteurs de l'UIT-T (disponible à l'adresse http://www.itu.int/oth/T0A0F000004/fr).

6 Prescriptions de haut niveau

Les éléments ci-après définissent les concepts, les rôles et les responsabilités concernant la bonne utilisation des identificateurs CAPEC lors du partage des données entre les instruments d'évaluation de la sécurité (outils, recueils et services) pour permettre auxdits instruments d'être utilisés ensemble et pour faciliter la comparaison des outils et des services d'évaluation de la sécurité.

Conditions préalables

6.1 Le propriétaire de l'instrument doit être une entité juridique valable (organisme ou personne particulière) possédant un numéro de téléphone, une adresse électronique et une adresse postale valables.

6.2 L'instrument doit fournir des valeurs ou des informations supplémentaires qui vont au-delà de ce qui est fourni dans la liste CAPEC elle-même (à savoir le nom, la description, les risques, les références et les informations associées sur les failles).

6.3 Le propriétaire de l'instrument doit communiquer à l'autorité d'examen un point de contact technique qui est qualifié pour répondre aux questions en rapport avec la précision du mappage et les fonctionnalités de l'instrument en relation avec la CAPEC.

6.4 L'instrument doit être mis à la disposition du public ou d'un ensemble de consommateurs, dans une version prototype ou une version publique.

6.5 Pour être compatible avec la liste CAPEC, le propriétaire de l'instrument doit faire parvenir à l'autorité d'examen un "formulaire d'évaluation des prescriptions en matière de compatibilité avec la liste CAPEC dûment rempli".

6.6 Le propriétaire de l'instrument doit donner à l'autorité d'examen un libre accès au recueil de manière qu'elle puisse déterminer si le recueil satisfait à toutes les prescriptions associées en matière de précision du mappage.

6.7 Le propriétaire de l'instrument doit permettre à l'autorité d'examen d'utiliser le recueil pour identifier tout schéma d'attaque devant être ajouté à la liste CAPEC.

6.8 Le propriétaire de l'instrument doit accepter de se soumettre à toutes les prescriptions obligatoires en matière de compatibilité avec la liste CAPEC, y compris les prescriptions obligatoires pour le type spécifique d'instrument.

Fonctionnalité

6.9 Pour la compatibilité CAPEC, l'instrument doit permettre aux utilisateurs de localiser les éléments de sécurité à l'aide d'identificateurs CAPEC ("*fonction de recherche CAPEC*").

6.10 Pour la compatibilité CAPEC, lorsque l'instrument présente des éléments de sécurité à l'utilisateur, il doit lui permettre d'obtenir les identificateurs CAPEC associés ("*résultat CAPEC*").

6.11 Pour la compatibilité CAPEC, le mappage de l'instrument doit relier les éléments de sécurité avec précision aux identificateurs CAPEC appropriés ("*précision du mappage*").

6.12 Pour la compatibilité CAPEC, la documentation de l'instrument doit décrire de manière adéquate la liste CAPEC, la compatibilité CAPEC et la manière dont la fonctionnalité de l'instrument en relation avec la CAPEC est utilisée ("*documentation CAPEC*").

6.13 Pour la compatibilité CAPEC, la documentation de l'instrument accessible au public doit expressément faire état des identificateurs CAPEC considérés par le propriétaire de l'instrument comme étant couverts par l'instrument dans le cadre de sa fonctionnalité ("*couverture CAPEC*").

6.14 Pour la compatibilité CAPEC, le site web de l'instrument accessible au public DEVRAIT fournir la couverture CAPEC de l'instrument sous la forme d'un ou de plusieurs documents au format XML représentant une déclaration de couverture (CCR) CAPEC.

6.15 L'instrument doit indiquer la version datée de la liste CAPEC utilisée ("*version utilisée*").

6.16 L'instrument doit respecter toute prescription supplémentaire pour le type spécifique d'instrument, comme spécifié dans l'Annexe A.

6.17 L'instrument doit satisfaire à toutes les prescriptions applicables à ses supports de distribution, comme spécifié dans l'Annexe B.

6.18 Il n'est pas nécessaire que l'instrument:

- utilise les mêmes descriptions ou références que la liste CAPEC;
- intègre tous les identificateurs CAPEC dans son recueil.

Divers

6.19 Si l'instrument ne satisfait pas toutes les prescriptions applicables susmentionnées (6.1 à 6.18), son propriétaire ne doit pas annoncer qu'il est compatible avec la liste CAPEC.

7 Précision

La compatibilité CAPEC ne peut faciliter le partage et la corrélation de données que si le mappage de l'instrument est précis. C'est pourquoi les instruments compatibles avec la liste CAPEC doivent satisfaire aux prescriptions minimales d'exactitude décrites ci-après.

7.1 Le recueil doit être exact à 100%.

7.2 Au cours d'une période d'examen, le propriétaire de l'instrument doit corriger toutes les erreurs de mappage relevées par l'autorité d'examen.

7.3 Après la période d'examen, le propriétaire de l'instrument devrait corriger une erreur de mappage dans un délai raisonnable après que l'erreur a été initialement signalée, c'est-à-dire dans un délai correspondant à deux (2) versions du recueil de l'instrument ou dans les six (6) mois suivants (la plus courte des périodes étant retenue).

7.4 Le propriétaire de l'instrument devrait élaborer et signer une déclaration stipulant qu'à sa connaissance, il n'y a pas d'erreur dans le mappage.

7.5 Si l'instrument est fondé sur un autre instrument compatible avec la liste CAPEC (l'instrument "source") ou utilise un tel instrument et que son propriétaire se rend compte qu'il existe des erreurs de mappage dans l'instrument source, alors le propriétaire de l'instrument doit signaler ces erreurs au propriétaire de l'instrument source.

8 Documentation

Les prescriptions suivantes s'appliquent à la documentation fournie avec l'instrument.

8.1 La documentation doit inclure une description concise de la liste CAPEC et de la compatibilité CAPEC, pouvant reprendre mot pour mot des parties de documents disponibles sur le site web CAPEC.

8.2 La documentation doit décrire comment l'utilisateur peut trouver des éléments de sécurité particuliers dans le recueil de l'instrument à l'aide d'identificateurs CAPEC.

8.3 La documentation doit décrire comment l'utilisateur peut obtenir des identificateurs CAPEC à partir d'éléments particuliers dans le recueil de l'instrument.

8.4 Si la documentation comprend un index, celui-ci devrait inclure des références à la documentation sur la liste CAPEC sous le terme "CAPEC".

9 Version de la liste CAPEC utilisée

Les utilisateurs doivent savoir quelle est la version de la liste CAPEC qui est utilisée dans le recueil d'un instrument eu égard à son mappage avec la liste CAPEC. Le propriétaire de l'instrument peut indiquer le mappage en vigueur en donnant la version de la liste CAPEC ou la date à laquelle le mappage a été mis à jour.

9.1 L'instrument doit identifier la version de la liste CAPEC ou la date de la mise à jour utilisée pour la création ou la mise à jour du mappage grâce à au moins l'un des éléments suivants: journal des modifications, liste des nouvelles fonctionnalités, fichiers d'aide, ou un autre mécanisme. L'instrument est "à jour" par rapport à cette version ou à cette date.

9.2 Chaque nouvelle version de l'instrument devrait être à jour par rapport à la version de la liste CAPEC qui a été publiée au maximum quatre (4) mois avant que l'instrument ait été mis à la disposition de ses utilisateurs. Si un instrument ne satisfait pas cette prescription, il est "obsolète".

9.3 Le propriétaire de l'instrument devrait indiquer le délai dans lequel il mettra à jour le recueil de l'instrument après qu'une nouvelle version de la liste CAPEC ou une mise à jour a été mise à disposition sur le site web CAPEC.

10 Révocation de la compatibilité avec la liste CAPEC

10.1 Si une autorité d'examen a vérifié qu'un instrument est compatible avec une liste CAPEC, mais qu'elle a par la suite la preuve que les prescriptions ne sont plus satisfaites, elle peut révoquer son approbation.

10.1.1 L'autorité d'examen doit identifier les prescriptions spécifiques qui ne sont pas satisfaites.

10.2 L'autorité d'examen doit déterminer si les actions ou les déclarations du propriétaire de l'instrument sont "intentionnellement trompeuses".

10.2.1 L'autorité d'examen peut interpréter la phrase "intentionnellement trompeuse" comme elle le souhaite.

10.3 L'autorité d'examen ne devrait pas envisager la révocation d'une compatibilité CAPEC pour un instrument donné plus d'une fois tous les six (6) mois.

Mise en garde et évaluation

10.4 L'autorité d'examen doit adresser au propriétaire de l'instrument et au point de contact technique (POC) un avertissement de révocation au moins deux (2) mois avant la date prévue pour la révocation.

10.4.1 Si l'autorité d'examen constate que les actions ou les déclarations du propriétaire de l'instrument sont intentionnellement trompeuses, elle peut ne pas tenir compte de la période de préavis.

10.5 Si le propriétaire de l'instrument estime que les prescriptions sont respectées, il peut répondre à l'avertissement de révocation en fournissant des détails précis indiquant pourquoi l'instrument satisfait aux prescriptions en question.

10.6 Si propriétaire de l'instrument modifie l'instrument pendant la période de préavis de manière à la rendre conforme aux prescriptions en question, l'autorité d'examen devrait mettre un terme à l'action de révocation de l'instrument.

Révocation

10.7 L'autorité d'examen peut reporter la date de révocation.

10.8 L'autorité d'examen doit faire savoir que la compatibilité CAPEC a été révoquée pour l'instrument.

10.9 Si l'autorité d'examen découvre que les actions du propriétaire de l'instrument, en ce qui concerne les prescriptions de compatibilité CAPEC, sont intentionnellement trompeuses, la révocation devrait être d'au moins un an.

10.10 L'autorité d'examen peut faire connaître la raison de la révocation.

10.11 Le propriétaire de l'instrument peut publier sur le même site web une déclaration publique concernant la révocation.

10.12 Si l'approbation est révoquée, le propriétaire de l'instrument ne doit PAS demander de nouvel examen pendant la période de révocation.

11 Autorité d'examen

11.1 L'autorité d'examen doit examiner la compatibilité CAPEC de l'instrument, par rapport à une version donnée de la liste CAPEC, qui est la version de l'examen.

11.2 L'autorité d'examen doit identifier clairement la version de l'examen utilisée pour déterminer la compatibilité de l'instrument.

11.3 L'autorité d'examen doit identifier clairement la version du document contenant les prescriptions de compatibilité CAPEC qui a été utilisée pour déterminer la compatibilité de l'instrument.

11.4 L'autorité d'examen doit examiner tous les éléments du recueil de l'instrument quant à la précision du mappage CAPEC.

11.5 L'autorité d'examen devrait évaluer si le mappage d'un instrument est précis au moins une fois par an.

11.6 L'autorité d'examen doit fournir un exemplaire de la déclaration de compatibilité CAPEC sur demande de tout propriétaire valable de l'instrument désireux d'engager le processus de compatibilité CAPEC.

11.7 L'autorité d'examen doit fournir un exemplaire du formulaire d'évaluation des prescriptions de compatibilité CAPEC sur demande de tout utilisateur de l'instrument qui a soumis un formulaire de déclaration de compatibilité CAPEC.

Annexe A

Prescriptions selon les types d'instrument

(La présente annexe fait partie intégrante de la présente Recommandation.)

Puisqu'une gamme d'instruments très divers emploie une liste CAPEC, certains types d'instruments peuvent avoir des caractéristiques uniques, qui nécessitent une attention particulière en ce qui concerne la compatibilité avec la liste CAPEC.

A.1 L'instrument doit satisfaire à toutes les prescriptions supplémentaires qui sont liées au type particulier qui est le sien.

A.1.1 Si l'instrument est un outil d'évaluation, un outil d'évaluation dynamique de la sécurité (DAST), un outil d'évaluation de la pénétration, un outil cadre pour les exploitations, un outil de modélisation des menaces ou un produit qui intègre les résultats d'un ou de plusieurs de ces types d'éléments, il doit satisfaire aux prescriptions A.2.1 à A.2.8 applicables aux outils.

A.1.2 Si l'instrument est un service (tel qu'un service d'évaluation de la sécurité, un service d'évaluation de la pénétration ou un service d'enseignement ou de formation), il doit satisfaire aux prescriptions A.3.1 à A.3.5 applicables aux services de sécurité.

A.1.3 Si l'instrument est une base de données en ligne des attaques connues, une ressource Internet ou un site d'information, il doit satisfaire aux prescriptions A.4.1 à A.4.3 applicables aux instruments en ligne.

A.2 Prescriptions applicables aux outils

Les prescriptions applicables aux outils sont les suivantes:

A.2.1 L'outil doit permettre à l'utilisateur d'employer les identificateurs CAPEC pour repérer les missions associées à cet outil ("recherche CAPEC"), en fournissant au moins l'un des éléments suivants: une fonction "recherche", un mappage entre les noms des missions de cet outil et des identificateurs CAPEC, ou un autre mécanisme jugé suffisant par l'autorité d'examen.

A.2.2 Pour tout rapport où sont identifiés différents éléments de sécurité, l'outil doit permettre à l'utilisateur de déterminer les identificateurs CAPEC associés à ces éléments ("sortie CAPEC"), en procédant à au moins l'une des actions suivantes: inclure les identificateurs CAPEC directement dans le rapport, effectuer un mappage entre les noms des missions de l'outil et les identificateurs CAPEC, ou employer un autre mécanisme jugé suffisant par l'autorité d'examen.

A.2.3 La documentation mise à disposition du public doit explicitement mentionner les identificateurs CAPEC dont le propriétaire de l'instrument estime que l'outil assure la recherche dans le logiciel ("couverture revendiquée de compatibilité avec la liste CAPEC").

A.2.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CAPEC de l'instrument sous la forme d'un ou de plusieurs document(s) en format XML représentant la déclaration de couverture CAPEC (CCR).

A.2.5 Tout rapport ou mappage exigé doit satisfaire aux prescriptions en matière de support, comme spécifié à l'Annexe B.

A.2.6 L'outil ou le propriétaire de l'instrument devrait communiquer à l'utilisateur une liste de tous les identificateurs CAPEC qui sont associés aux missions de l'outil.

A.2.7 En fournissant un fichier contenant une liste des identificateurs CAPEC à l'utilisateur, l'outil devrait permettre à celui-ci de choisir un ensemble de missions.

A.2.8 L'interface de l'outil devrait permettre à l'utilisateur de naviguer, de choisir et de désélectionner un ensemble de missions au moyen des différents identificateurs CAPEC.

A.2.9 Si l'outil n'a aucune mission associée à un identificateur CAPEC, comme spécifié par l'utilisateur dans les prescriptions A.2.5 et A.2.6 relatives à l'outil, il devrait informer l'utilisateur qu'il ne peut exécuter la mission associée.

A.3 Prescriptions applicables aux services de sécurité

Les services de sécurité peuvent employer des outils compatibles avec la liste CAPEC dans leurs travaux, mais ils ne peuvent donner à leurs clients un accès direct à ces outils. Il peut donc être difficile pour leurs clients de recenser et de comparer les instruments des divers services. Les prescriptions applicables aux services de sécurité traitent de cette restriction potentielle.

A.3.1 Le service de sécurité doit être en mesure d'employer des identificateurs CAPEC pour indiquer à un utilisateur les éléments de sécurité qui sont éprouvés ou couverts par l'offre de service ("recherche CAPEC"), en procédant à l'une ou à plusieurs des actions suivantes: transmettre à l'utilisateur une liste des identificateurs CAPEC qui recense les éléments éprouvés ou couverts par ce service, communiquer à l'utilisateur un mappage entre les éléments de service et les identificateurs CAPEC, répondre à une liste d'identificateurs CAPEC présentée par l'utilisateur, en indiquant les identificateurs CAPEC qui sont éprouvés ou couverts par le service ou en employant un autre mécanisme.

A.3.2 Pour tout rapport où sont identifiés différents éléments de sécurité, le service doit permettre à l'utilisateur de déterminer les identificateurs CAPEC associés à ces éléments ("sortie CAPEC"), en procédant à au moins l'une des actions suivantes: autoriser l'utilisateur à inclure les identificateurs CAPEC directement dans le rapport, communiquer à l'utilisateur un mappage entre les éléments de sécurité et les identificateurs CAPEC, ou employer un autre mécanisme.

A.3.3 La documentation mise à la disposition du public doit explicitement mentionner les identificateurs CAPEC dont le propriétaire de l'instrument estime que le service de sécurité assure efficacement la couverture ("couverture revendiquée de compatibilité avec la liste CAPEC").

A.3.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CAPEC de l'instrument sous la forme d'un ou de plusieurs documents en format XML représentant la déclaration de couverture CAPEC (CCR).

A.3.5 Tout rapport ou mappage exigé qui est fourni par le service doit satisfaire aux prescriptions en matière de support, comme spécifié à l'Annexe B.

A.3.6 Si le service donne à l'utilisateur un accès direct à un produit qui identifie les éléments de sécurité, ce produit devrait être compatible avec la liste CAPEC.

A.4 Prescriptions applicables aux instruments en ligne

Les prescriptions applicables aux instruments en ligne sont les suivantes:

A.4.1 L'instrument en ligne doit permettre à un utilisateur de découvrir des éléments de sécurité dans le recueil des instruments en ligne ("recherche CAPEC") en fournissant l'un des éléments suivants: une fonction de recherche qui renvoie des identificateurs CAPEC pour les éléments associés, un mappage qui relie chaque élément avec son ou ses identificateurs CAPEC associés, ou un autre mécanisme.

A.4.1.1 L'instrument en ligne devrait fournir un modèle d'URL qui permette à un programme d'ordinateur d'établir aisément une liaison permettant d'accéder à la fonction de recherche, comme décrit au § A.4.1 sur les prescriptions relatives aux instruments en ligne.

Exemples de construction de lien:

http://www.example.com/cgi-bin/db-search.cgi?capecid=XXX

http://www.example.com/capec/xxx.html

A.4.1.2 Si le site est accessible au public sans exiger d'identification, le programme d'identification CGI devrait accepter la méthode "GET".

A.4.2 Pour tout rapport où sont identifiés différents éléments de sécurité, l'instrument en ligne doit permettre à l'utilisateur de déterminer les identificateurs CAPEC associés à ces éléments ("sortie CAPEC"), en procédant à au moins l'une des actions suivantes: autoriser l'utilisateur à inclure les identificateurs CAPEC directement dans le rapport, communiquer à l'utilisateur un mappage entre les éléments de sécurité et les identificateurs CAPEC, ou employer un autre mécanisme.

A.4.3 La documentation mise à disposition du public doit explicitement mentionner les identificateurs CAPEC dont le propriétaire de l'instrument estime que le recueil de l'instrument en ligne assure efficacement la couverture ("déclaration de couverture de compatibilité avec la liste CAPEC").

A.4.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CAPEC de l'instrument sous la forme d'un ou de plusieurs documents en format XML représentant la déclaration de couverture CAPEC (CCR).

A.4.5 Si l'instrument en ligne ne fournit pas les détails des différents éléments de sécurité, il doit effectuer un mappage qui relie chaque élément avec son ou ses identificateurs CAPEC associés.

Annexe B

Prescriptions en matière de support

(La présente annexe fait partie intégrante de la présente Recommandation.)

B.1 Le support de diffusion qui est employé par un instrument compatible avec une liste CAPEC doit avoir un format qui figure dans la présente annexe.

B.2 Le format du support doit satisfaire aux prescriptions propres à ce format.

B.3 Documents sous forme électronique (en format HTML, en format de traitement de texte, en format PDF, en format ASCII, etc.)

B.3.1 Le document doit avoir un format couramment disponible, disposant de lecteurs qui prennent en charge la fonction "recherche" ("recherche CAPEC"), tel que le format texte ASCII brut, le format HTML ou le format PDF.

B.3.2 Si le document ne fournit que des abréviations ou des titres pour les différents éléments, il doit énumérer les identificateurs CAPEC qui sont reliés à ces éléments ("sortie CAPEC").

B.3.3 Le document doit inclure un mappage entre les éléments et les identificateurs CAPEC, où sont énumérés les pages appropriées pour chaque élément.

B.4 Interface graphique utilisateur

B.4.1 L'interface graphique utilisateur (GUI) doit fournir à l'utilisateur une fonction de recherche qui permette à l'utilisateur d'introduire un identificateur CAPEC et d'extraire les éléments correspondants ("recherche CAPEC").

B.4.2 Lorsque l'interface GUI énumère les détails d'un élément, elle doit énumérer les identificateurs CAPEC qui correspondent à cet élément ("sortie CAPEC"). Sinon, elle doit mettre à la disposition de l'utilisateur un mappage sous un format qui satisfait à la prescription relative aux documents sous forme électronique au § B.3.1.

B.4.3 L'interface GUI devrait permettre à l'utilisateur d'exporter des données se rapportant à la liste CAPEC ou d'y accéder, sous un autre format, à condition que celui-ci satisfasse à la prescription relative aux documents sous forme électronique au § B.3.1.

Bibliographie

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2011), *Vulnérabilités et expositions courantes.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2013