الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1214

(2018/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

تقنيات التقييم الأمني في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات

التوصية ITU-T X.1214

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1214

تقنيات التقييم الأمني في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات

ملخص

تشرح التوصية ITU-T X.1214 منهجية للتقييم الأمني وأفضل الممارسات من أجل المطوّرين والمصنّعين ومشغلي الشبكات والأفراد من الخبراء الأمنيين في مجال الاتصالات لعناصر شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات للتعامل مع أمن العناصر القائمة على البرمجيات لديهم. فالشبكات التقليدية القائمة على تبديل الدارات والشبكات القائمة على الرزم على السواء معرّضة لتهديدات وهجمات مختلفة، من مصادر خارجية وداخلية على السواء، تستهدف مختلف أجزاء شبكة الاتصالات/تكنولوجيا المعلومات والاتصالات. وتشمل هذه التوصية ما يلي:

- الكشف عن مواطن الضعف في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؛
- منهجية التقييم الأمني في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1214	2018-03-29	17	11.1002/1000/13404

مصطلحات أساسية

تحليل إثنيني، الاختبار الآلي للبرمجيات، اختبار الاختراق، التقييم الأمني، الاختبار الأمني، استعراض شفرة المصدر، مسح مواطن الضعف.

---

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

لشبكات الاتصالات/تكنولوجيا المعلومات والاتصالات دور حاسم في التنمية الاقتصادية لمعظم البلدان. وقد أدى ذلك إلى تنظيم الحكومة لصناعة الاتصالات، بما في ذلك اشتراطات لضمان أمن معدات وشبكات الاتصالات. وينبغي لمشغلي الاتصالات اعتماد برنامج أمني متين ومدار من أجل ضمان حماية العناصر القائمة على البرمجيات والخاصة بشبكاتهم من الهجمات الضارة الداخلية والخارجية، على السواء، مع ضمان الامتثال لمتطلبات البيئة التنظيمية المحلية. وبالنسبة لهذه العناصر القائمة على البرمجيات، يتطلب ذلك آلية شديدة الفعالية للتقييم الأمني تقوم على المعايير وأفضل الممارسات الأمنية المتفق عليها عالمياً.

والحفاظ على وضع متسق للأمن عبر شبكة منظمة ما في مواجهة عالم التهديدات ذات الطابع المتغير على الدوام مهمة تتسم بالتعقيد واستنزاف الوقت. وربما يتحتم على المنظمات تحمل نفقات باهظة للتعافي من أي انتهاك أمني. وتتعلق هذه التكاليف بجهود العلاج وبرامج حماية العملاء والاستبقاء، والأنشطة القانونية وتثبيط همم الشركاء في الأعمال وانخفاض إنتاجية الموظفين وتدني الإيرادات. ومن شأن وجود نهج فعال للتقييم الأمني أن يساعد في تفادي هذه العثرات المالية من خلال التحديد الاستباقي للمخاطر التي تهدد أصولها وقدراتها القائمة على البرمجيات ومواجهتها قبل وقوع الهجمات أو قبل وقوع الانتهاكات الأمنية. والتقييم المستقل من المنظور الأمني طلب متزايد من الأسواق التي على شاكلة الحكومات والقطاع المالي والاتصالات.

وتسلط هذه التوصية الضوء بشكل أساسي على تقنيات التقييم الأمني التي يتعين على مشغلي شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات وموردي الخدمات اعتمادها من أجل التحديد الاستباقي لمواطن الضعف بالنسبة للعناصر القائمة على البرمجيات وتقييمها.

التوصية ITU-T X.1214

تقنيات التقييم الأمني في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات

1 مجال التطبيق

تناقش هذه التوصية تقنيات التقييم الأمني التي يمكن استخدامها في العناصر القائمة على البرمجيات في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات. فالشبكات التقليدية القائمة على تبديل الدارات والشبكات القائمة على الرزم على السواء معرّضة لتهديدات وهجمات مختلفة، من مصادر خارجية وداخلية على السواء، تستهدف مختلف أجزاء العناصر القائمة على البرمجيات في شبكة الاتصالات/تكنولوجيا المعلومات والاتصالات. ويمكن للتقييم الأمني للمكونات القائمة على البرمجيات قبل استعمالها في هذه الشبكات أن يساعد المشغلين وموردي الخدمات على تحسين اعتمادية الشبكات بشكل كبير. بيد أن هناك متطلب بخصوص التقييس في هذا المجال، بحيث يتسنى توفير المعايير وأفضل الممارسات العالمية للتقييم الأمني للعناصر القائمة على البرمجيات، لفائدة المطورين والجهات المصنعة والمشغلين والأفراد من الخبراء الأمنيين.

ويمكن استعمال هذه التقنيات فرادى أو جماعات حسب المطلوب أو المناسب.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1520] التوصية ITU-T X.1520 (2014)، *مواطن الضعف والتعرض الشائعة.*

[ITU-T X.1524] التوصية ITU-T X.1524 (2012)، *تعديد مواطن الضعف الشائعة (CWE).*

[ITU-T X.1544] التوصية ITU-T X.1544 (2013)، *تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC).*

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة وثائق أخرى:

1.1.3 وسيلة التخزين (repository) [ITU-T X.1524]: مجموعة صريحة أو ضمنية من العناصر المتعلقة بمواطن الضعف الأمنية المتصلة بالبرمجيات لدعم قدرة ما، مثل قاعدة بيانات خاصة بمواطن الضعف الأمنية أو مجموعة مخططات في محلل للشفرات أو موقع على الويب.

2.1.3 نقطة التعرض (vulnerability) [ITU-T X.1520]: أي موطن ضعف في البرمجيات يمكن استغلاله لانتهاك حرمة نظام ما أو المعلومات التي يحتويها.

3.1.3 موطن الضعف (weakness) [ITU-T X.1524]: هو قصور أو عيب في شفرة البرنامج، أو تصميمها، أو معماريتها، أو نشرها، قد يصبح في مرحلة ما نقطة تعرض، أو قد يسهم في إدخال نقاط تعرض أخرى.

2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 التحليل الإثنيني (binary analysis): تقنية لتحديد مواطن الضعف في الملفات المنفذة بلغة الآلة.

2.2.3 الاختبار الآلي للبرمجيات (fuzzing): تقنية لاكتشاف نقاط التعرض غير المعروفة أو التي لم تكن معروفة من قبل في برمجية ما عن طريق تقديم مدخلات غير متوقعة إلى البرمجية ومراقبة سلوكياتها المتوقعة.

3.2.3 تغيير (mutation): بايتات أو كلمات أو سلاسل فردية مغيّرة ضمن إحدى رزم بيانات الدخل.

4.2.3 اختبار الاختراق (penetration testing): تقنية لتقييم أثر استغلال نقاط تعرض محددة.

5.2.3 التقييم الأمني (security assessment): دراسة صريحة لتحديد موضع نقاط التعرض والمخاطر الأمنية.

6.2.3 مسح قائم على التوقيع (signature based scanning): تقنية مسح تقارن بين محتويات هدف ما وقاعدة بياناته المتضمنة لتوقيعات معروفة لتحديد نقاط التعرض.

وفي حالة المواءمة مع أحد التوقيعات، يحدد الماسح نقطة التعرض كما يقترح الإجراء العلاجي.

7.2.3 استعراض شفرة المصدر (source code review): تقنية لتحديد مواطن الضعف في مقاطع شفرة البرمجية المكتوبة بلغات رفيعة المستوى.

8.2.3 الأداة (tool): تطبيق برمجي أو جهاز لفحص مستضيف أو شبكة أو جزء من برمجية أو تطبيق إثنيني أو أي حالة مصطنعة تنتج معلومات تتعلق بنقاط التعرض أو مواطن الضعف أو حالات التعرض، مثل ماسح نقاط التعرض أو أداة الاختبار الآلي للبرمجيات أو أداة استعراض شفرة المصدر أو المحلل الإثنيني أو أداة اختبار الاختراق.

9.2.3 مسح نقاط التعرض (vulnerability scanning): تقنية لتحديد نقاط التعرض المعروفة أو المنشورة داخل هدف ما.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

CAPEC تعديد أنماط الهجمات الشائعة وتصنيفها *(Common Attack Pattern Enumeration and Classification)*

CVE نقاط الضعف والتعرض الشائعة *(Common Vulnerabilities and Exposures)*

CWE تعديد مواطن الضعف الشائعة *(Common Weakness Enumeration)*

DUT الجهاز قيد الاختبار *(Device Under Test)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

OS نظام التشغيل *(Operating System)*

SQL لغة الاستعلام البنيوية *(Structured Query Language)*

5 الاصطلاحات

لا توجد.

6 المفهوم الأساسي – الاختبار الأمني

غالباً ما تضم شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات خليطاً غير متجانس من المعدات من موردين مختلفين. ويجب وجود برنامج اعتماد من طرف ثالث ذي مصداقية وموثوقية عالية لإجراء تقييم لتحديد مواطن الضعف والتعرض الأمنية الموجودة في عمليات تنفيذ برمجيات المعدات وبرمجياتها الثابتة وعتادها وتقييمها. ويدور التقييم الأمني لأي منتج بشكل أساسي حول اكتشاف نقاط التعرض الموجودة والتحقق منها. ويمكن تقسيم اكتشاف نقاط التعرض إلى فئتين رئيسيتين (انظر الفقرتين 1.6 و2.6).

1.6 اكتشاف نقاط تعرض معروفة أو منشورة

توجد نقاط التعرض الخاصة بالبرمجيات بصورة يومية في المنتجات البرمجية الشائع استعمالها. ويتم نشر نقاط التعرض، مثل نقاط ومواطن التعرض الشائعة (CVE)، من قبل قاعدة بيانات نقاط التعرض الوطنية والعديد من قواعد البيانات الأخرى. وتعد الإدارة الفعالة لنقاط التعرض المنشورة أحد الأنشطة الهامة في الجهود الأمنية بالشركات الحديثة. ولعلها مهمة شاقة تلك المتعلقة بالتتبع اليدوي لجميع نقاط التعرض الموجودة في الأنظمة وعلاجها بالشكل المناسب. وتوجد أدوات مؤتمتة تجري المسح القائم على التوقيع لاكتشاف نقاط التعرض وتحديدها إزاء نقاط ومواطن التعرض [انظر في البيبليوغرافيا b-CVE].

2.6 اكتشاف نقاط تعرض غير معروفة أو لم تكن معروفة من قبل

تشمل هذه الفئة اكتشاف نقاط الضعف التي لم تنشر بعد. وهناك نهج متنوعة لتنفيذ ذلك لكل نهج منها مزاياه وعيوبه. ولا يوجد نهج واحد مكتمل كما لا يوجد أسلوب وحيد يمكنه اكتشاف جميع نقاط التعرض المحتملة لهدف بعينه. والأدوات والتقنيات المستخدمة في اكتشاف نقاط تعرض غير معروفة أو صفرية تشمل أدوات الاختبار الآلي للبرمجيات وأدوات استعراض شفرة المصدر وأدوات التحليل الإثنيني. وترد تفاصيل عن هذه الأدوات في الفقرات من 2.7 إلى 5.7.

7 تقنيات الاختبار الأمني

كما ورد أعلاه، هناك نهج متنوعة للكشف عن نقاط التعرض للعناصر القائمة على البرمجيات، لكل نهج منها مزاياه وعيوبه. ولا يوجد أسلوب وحيد يمكنه اكتشاف جميع نقاط التعرض المحتملة لهدف بعينه. لذا، فإن آلية التقييم الفعالة ستنظر بكل تأكيد في اعتماد النهج المتعددة، والتي تناقش في الفقرات من 1.7 إلى 5.7.

1.7 مسح نقاط التعرض

ماسح نقاط التعرض في الشبكات عبارة عن جهاز أو برمجية للاستخدام في مسح معمارية أي شبكة والإبلاغ عن أي نقاط تعرض يتم تحديدها في عناصر الشبكة القائمة على البرمجيات. وأثناء مسح نقاط التعرض، تقارن قاعدة بيانات لتوقيعات نقاط التعرض بالمعلومات المتحصل عليها عبر مسح الشبكة لوضع قائمة بنقاط التعرض المفترض وجودها في الشبكة. كما يتم في بعض الأوقات دمج أداة لاختبار الاختراق للإعلان عن إمكانية الاستغلال الفعلي لنقاط التعرض التي يتم تحديدها للتحقق الكامل من وجودها. وتحليل نقاط التعرض عبارة عن العملية التي تقيم مدى خطورة نقاط التعرض التي يتم تحديدها. وعادةً ما يوجد بالمنظمات عدد كبير من نقاط التعرض في بيئتها التشغيلية يفضي بعضها إلى مخاطر أمنية أعلى من البعض الآخر. فمثلاً، لبعض نقاط تعرض البرمجيات عواقب وخيمة إذا استغلت. وبالتالي، من المهم تقييم المشكلات الأكثر أهمية وعلاجها أولاً.

ويمكن إجراء مسح التعرض على الأنظمة الموصولة بالإنترنت وكذلك على الشبكات الداخلية غير الموصولة بالإنترنت لتقييم نقاط تعرض البرمجيات.

ويجب أن تكون الأدوات ووسائل التخزين والخدمات المستخدمة في مسح التعرض متوافقة مع نقاط الضعف والتعرض الشائعة (CVE) طبقاً للمتطلبات والوظائف الموصفة في التوصية [ITU-T X.1520].

2.7 الاختبار الآلي للبرمجيات (Fuzzing)

يعرف الاختبار الآلي للبرمجيات بأنه طريقة لاكتشاف نقاط التعرض غير المعروفة أو غير المعالجة في البرمجية من خلال تقديم مدخلات غير متوقعة ومراقبة السلوك المتوقع للبرمجية من حيث الاستثناءات. وعادةً ما تكون هذه العملية مؤتمتة أو شبه مؤتمتة تضم عمليات متكررة للتلاعب في البيانات وتقديمها إلى البرمجية المستهدفة للمعالجة. وقد تكون البرمجية المستهدفة كدسة بروتوكولات أو تطبيق أو ملفات، حسب نوع أداة الاختبار "Fuzzer" هل هي "Fuzzer" للبروتوكول أم "Fuzzer" للتطبيق أم "Fuzzer" للملف. ولا يحتاج الباحث أو القائم بالاختبار إلى معرفة العمل الداخلي للهدف ولهذا السبب يشار إلى هذه النهج أيضاً بنهج اختبار.

وهناك في الأساس نوعان من النهج الخاصة بالاختبار Fuzzing وهما الاختبار Fuzzing القائم على التوليد والاختبار Fuzzing القائم على التغيير على النحو الوارد في الفقرتين 1.2.7 و2.2.7 على التوالي.

1.2.7 الاختبار Fuzzing القائم على التوليد

في هذا النهج، تبدأ عملية وضع حالات الاختبار بدراسة مواصفة معينة لفهم جميع بنى البيانات المدعومة ومديات القيم المقبولة لكل منها. وتولد بعد ذلك المدخلات للأهداف بحيث تختبر الشروط الحدية أو تنتهك المواصفة تماماً. وقد يتطلب وضع حالات الاختبار قدر هائل من العمل التمهيدي بيد أنه يتميز بالقدرة على إعادة استخدامه من أجل عمليات تنفيذ متعددة للاختبار لنفس البروتوكول أو نسق الملف.

2.2.7 الاختبار Fuzzing القائم على التغيير

تجري أدوات الاختبار Fuzzing القائم على التغيير تغييراً لعينات البيانات القائمة في صورة عمليات الالتقاط للرزم ذات الصلة بالهدف لوضع حالات الاختبار. وتخضع كل بايتة أو كلمة أو سلسلة فردية في هذه العينات للتغيير ثم ترسل نحو الهدف. ويحتاج هذا النهج إلى قدر ضئيل جداً من عمليات البحث التمهيدية ويمكن تنفيذه في فترة زمنية قصيرة. بيد أن هذا النهج لا يتسم بالكفاءة الكبيرة حيث قد يحتاج إلى تجميع كميات هائلة من عينات البيانات للحصول على تغطية حيدة للبروتوكول المستهدف.

وتعمل أدوات الاختبار Fuzzing بشكل أفضل مع المشكلات التي يمكنها أن تتسبب في حدوث عطب للبرنامج، مثل التدفق المفرط في الدارئ والبرمجة العابرة للمواقع وهجمات رفض الخدمة وأعطاب النسق وحقن لغة الاستعلام البنيوية (SQL). والاختبار Fuzz أقل فعالية بالنسبة للتعامل مع التهديدات الأمنية التي لا تتسبب في حدوث أعطاب للبرنامج مثل برمجيات التجسس وبعض الفيروسات والديدان وحصان طروادة ومتتبع لوحة المفاتيح.

والأدوات وأماكن التخزين والخدمات المستخدمة في الاختبار Fuzzing يجب أن تكون متوافقة مع تعديد مواطن الضعف الشائعة (CWE) طبقاً للمتطلبات والوظائف الموصفة في التوصية [ITU-T X.1524].

3.7 استعراض شفرة المصدر

استعراض شفرة المصدر نهج شائع يستخدمه مطوري البرمجيات للتوصل إلى مواطن الضعف أو العيوب ويعرف أيضاً باختبار الصندوق الأبيض. ويمكن إنجازه إما يدوياً أو بمساعدة أدوات الأتمتة. ونظراً إلى أن برامج البرمجيات عادةً ما تتضمن الملايين من خطوط الشفرة، فإن الاستعراض اليدوي الخالص ليس عملياً بشكل عام. وتعد أدوات الأتمتة مصدراً قيماً يجعل المهمة أسهل ولكنه لا يمكنه إلا تحديد مقاطع الشفرة التي يحتمل تعرضها أو المشتبه بها. ويحتاج الأمر في بعض الأوقات إلى تحليل بشري لتحديد ما إذا كانت القضايا المكتشفة سارية بالفعل لأن هذه الأداة تنتج أيضاً نتائج إيجابية زائفة. ويتثمل القيد الأكبر في هذا النهج في مقاومة البائعين أو المصنعين لتبادل شفرة المصدر.

ويجب أن تكون الأدوات ووسائل التخزين والخدمات المستخدمة في استعراض شفرة المصدر متوافقة مع تعديد مواطن الضعف الشائعة (CWE) على النحو المحدد في المتطلبات والوظائف الموصفة في التوصية [ITU-T X.1524].

4.7 التحليل الإثنيني

يشار عادةً إلى التقييم الأمني باستخدام تعليمات لغة الآلة بدلاً من شفرة المصدر بالتحليل الإثنيني. وينشئ التحليل الإثنيني نموذجاً سلوكياً بتحليل التحكم في تطبيق ما وتدفق بياناته من خلال شفرة الآلة القابلة للتنفيذ – الأسلوب الذي يراه المهاجم. وخلافاً لأدوات شفرة المصدر، يكتشف هذ النهج بدقة القضايا المتمركزة في التطبيق الأصلي ويوسع تغطيته بحيث تطول نقاط التعرض في مكتبات الطرف الثالث والمكونات الجاهزة والشفرات المطروحة من قبل وحدة تجميع أو تأويلات محددة للمنصة.

وتطوير البرمجية عبارة عن عملية متعددة المراحل حيث إن الأنواع المتنامية من التهديدات – مثل التهديدات الصادرة عن الشفرات الخبيثة وبرمجيات الأبواب الخلفية – يستحيل كشفها بأدوات استعراض شفرة المصدر لأنها لا تكون مرئية في شفرة المصدر. ويمكن كشف هذه التهديدات باستعمال تحليل إثنيني سكوني على التطبيق في شكله النهائي.

ويجب أن تكون الأدوات وسائل التخزين والخدمات المستعملة في التحليل الإثنيني متوافقة مع تعديد مواطن الشعف الشائعة (WE) طبقاً للمتطلبات والوظائف الموصفة في التوصية [ITU-T X.1524].

5.7 اختبار الاختراق

اختبار الاختراق عبارة عن محاولة استباقية ومصرح بها لتقييم أمن أي بنية تحتية بالمحاولة الآمنة لاستغلال نقاط تعرض النظام، بما في ذلك نظام التشغيل (OS) والبروتوكول وعيوب التطبيق والتشكيلات غير السليمة وحتى السلوك الخطر للمستعمل النهائي. ويتمثل الغرض الأساسي من اختبار الاختراق في قياس إمكانية إصابة الأنظمة أو المستعملين النهائيين بالخلل وتقييم أي عواقب ذات صلة لهذه الحوادث على الموارد أو العمليات المتضمنة. وتجرى الاختبارات عادةً باستخدام تكنولوجيات يدوية أو مؤتمتة للانتهاك النظامي للخدمات والنقاط النهائية وتطبيقات الويب والشبكات اللاسلكية وأجهزة الشبكات والأجهزة المتنقلة وغيرها من نقاط التعرض المحتملة. وقد يكون هدف اختبار الاختراق صندوق أبيض (يوفر الخلفية ومعلومات عن النظام) أو صندوق أسود (يوفر المعلومات الأساسية فقط أو لا يوفر أي معلومات بالمرة).

ويمكن بإجراء هذا الاختبار التحديد الاستباقي لنقاط التعرض الأكثر حرجاً أو الأقل أهمية أو التي تعطي إيجابيات زائفة. ويمكن هذا الأمر أي منظمة من تحديد أولويات الأنشطة العلاجية بطريقة أكثر استنارة وتطبيق الإصلاحات الأمنية اللازمة.

ويجب أن تتوافق الأدوات ووسائل التخزين والخدمات المستخدمة في اختبار الاختراق مع تعديد وتصنيف أنماط الهجمات الشائعة (CAPEC) طبقاً للمتطلبات والوظائف الموصفة في التوصية [ITU-T X.1544].

التذييل I

مخطط انسيابي

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

سيمثل تنظيم تقنيات التقييم الأمني في مخطط انسيابي بداية جيدة لعملية التقييم الأمني. ولتحقيق ذلك، يمكن النظر في نموذج يبدأ فيه التقييم من الجزء التكويني الأصغر في الشبكة ويمتد إلى الأنظمة المتكاملة المستخدمة فيها. ويوفر الأمن بداية لشفرة المصدر لعناصر البرمجيات، ثم للتطبيقات والمكتبات في النظام وصولاً إلى الأنظمة الموجودة في الشبكة وللشبكة المنشورة بأكملها في النهاية.

من هنا، يمكن تنظيم عملية التقييم الأمني بكاملها في مرحلتين رئيسيتين.

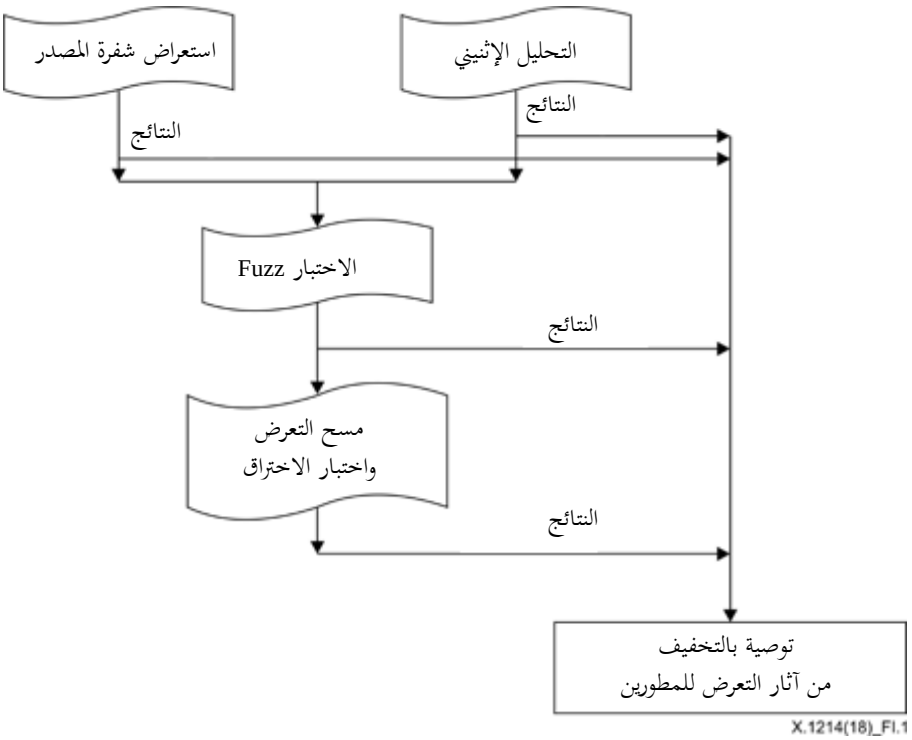
'1' الأولى هي مرحلة ما قبل النشر والتي يمكن فيها فحص الهدف بشكل كامل باستخدام جميع تقنيات التقييم الأمني التي نوقشت وينبغي استعمال نتائج هذ التقييم في التخفيف من آثار نقاط التعرض المكتشفة.

'2' ويمكن أن تكون الثانية مرحلة ما بعد النشر والتي يكون فيها الهدف قيد التشغيل بالفعل في الشبكة. وفي هذه المرحلة، قد لا يكون عملياً إخضاع الهدف لجميع تقنيات التقييم. وبالتالي، يمكن للمحللين الأمنيين اللجوء إلى المسح الدوري للتعرض للتأكد من أن نقاط التعرض التي يتم تحديدها بعد نشر المنتج تعالج بانتظام بتثبيت الوسائل العلاجية وغيرها.

وفي مرحلة ما قبل النشر، يمكن كخطوة أولى تحليل الشفرات مصدر عناصر البرمجيات علاج العيوب المكتشفة. وبعد ذلك، تعالج التطبيقات والمكتبات التي تستخدمها هذه التطبيقات بتحليل إثنيني. ويأتي الاختبار Fuzz بعد التحليل الإثنيني ثم المرحلة النهائية المتمثلة في مسح التعرض واختبار اختراق النظام. وينبغي تمرير النتائج والملاحظات الخاصة بالتقييم الشامل على المطورين المعنيين، لكي يتسنى لهم اتخاذ التدابير التصحيحية للتخفيف من آثار جميع نقاط التعرض المكتشفة.

وفي مرحلة ما بعد النشر، يمكن إخضاع الشبكة بأكملها لمسح دوري للتعرض. وتعالج أي نقاط تعرض بمجرد اكتشافها.

والشكل I.1 عبارة عن مخطط انسيابي يبين العملية.



الشكل 1.I – مخطط انسيابي لتقنيات التقييم الأمني

التذييل II

تقنيات إضافية أخرى لتعزيز أمن شبكة تكنولوجيا المعلومات والاتصالات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل بعض التقنيات لزيادة تعزيز أمن شبكة الاتصالات/تكنولوجيا المعلومات والاتصالات.

1.II تقييم قوة كلمة السر

يستعمل الاستيقان القائم على كلمة السر على نطاق واسع في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات لأغراض مختلفة، مثل التشكيل والإدارة والتشغيل والصيانة وتوفير الخدمة. وينبغي لمديري الأنظمة تقييم متانة كلمات السر هذه للتأكد من أنه لن يسهل قرصنتها. ولهذا الغرض، يمكن إجراء عملية فك كلمة السر. وهناك آليات عديدة لهذه العملية مثل هجمات القاموس وهجمات القوة الغاشمة وجداول قوس قزح.

2.II تقييم السرية الاجتماعية

يمكن في بعض الحالات استخدام التلاعب النفسي داخل المنظمات لكي تقوم بالإفصاح عن المعلومات السرية. وهو نوع من حيل الثقة الغرض منه جمع المعلومات أو الاحتيال أو النفاذ إلى الأنظمة. ويمكن إجراء الهندسة الاجتماعية لتقييم مصداقية هؤلاء الأفراد أو المجموعات داخل منظمة. ويمكن تحديد أهداف محددة عندما تدرك المنظمة وجود تهديد أو عندما ترى أن فقدان معلومات من شخص ما أو مجموعة محددة من الأشخاص يمكن أن يكون له أثر بالغ.

3.II التقييم الأمني الوظيفي

حتى وإن لم تشارك في التقييم الوظيفي أداة (أدوات) محددة، فإن هذا النهج يكمل تقنيات الكشف عن نقاط التعرض التي نوقشت في الفقرتين 1.II و2.II.

والمتطلبات الوظيفية الأمنية لأي جهاز أو عنصر شبكة مستخدم في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات هي كالتالي:

'1' الاستيقان المحلي لمستعمل فيما يتعلق بتشكيلة الجهاز وإدارته؛

'2' الاستيقان عن بُعد لمستعمل فيما يتعلق بتشكيلة الجهاز وإدارته؛

'3' تخزين مؤمن لكلمة السر في جهاز؛

'4' تحقق مؤمن من إدارة مفتاح التجفير؛

'5' آلية لحماية الجهاز من التعديل غير القانوني للبرمجيات؛

'6' حماية حركة إدارة الجهاز عن بُعد؛

'7' تصنيف مستعمل إدارة جهاز حسب الامتيازات/التصاريح؛

'8' التزامن الآمن في الميدان الزمني؛

'9' توليد حدث لمراجعة الجهاز قيد الاختبار (سجلات) باستعمال الجهاز قيد الاختبار (DUT)؛

'10' تصدير آمن لسجلات مراجعة الجهاز قيد الاختبار باستعمال الجهاز قيد الاختبار.

4.II المسح اللاسلكي

يمكن للمسح اللاسلكي أن يساعد المنظمات على اتخاذ تدابير تصحيحية للتخفيف من حدة المخاطر الأمنية الناتجة عن التكنولوجيات الممكنة لاسلكياً. وينبغي لأداة المسح اللاسلكي أن تكون قادرة عن مسح جميع الأجهزة اللاسلكية التي تعتمد المعيار 802.11 لمعهد مهندسي الكهرباء والإلكترونيات (IEEE)، للأجهزة اللاسلكية [b-IEEE Std. 8802-11]، المحلية منها أو الدولية. ويمكن للمسح اللاسلكي تحديد الأجهزة اللاسلكية غير المخولة ضمن نطاق أجهزة المسح واكتشاف الإشارات اللاسلكية خارج محيط المنظمة والكشف عن هجمات الباب الخلفية والانتهاكات الأمنية المحتملة.

5.II استخدام وحدة تجفير نمطية مؤمنة وعمليات تنفيذ الخوارزمية

تستعمل خوارزميات التجفير من أجل تجفير وفك تجفير بيانات الاستيقان أو بيانات المستعمل بغرض النقل الآمن للبيانات عبر شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات. وبرغم التصميم الجيد لهذه الخوارزميات، من الشائع وجود أخطاء في التنفيذ. وعند نشر خوارزميات غير آمنة تنطوي على عيوب في التنفيذ في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، فإن المهاجمين يمكنهم استخدام نفس الخوارزميات مما يؤدي إلى خسائر محتملة ضخمة في البيانات ووقوع أنشطة اقتحام احتيالية. ولذا، يمكن استخدام وحدات تجفير نمطية وخوارزميات مؤمنة بشكل جيد في شبكات الاتصالات/تكنولوجيات المعلومات والاتصالات.

6.II التجسس على الشبكات

التجسس على الشبكات عبارة عن تقنية تفاعلية تراقب اتصالات الشبكة وتفكك تشفير البروتوكولات وتفحص الرأسيات للتأشير على المعلومات المهمة. ويشار إليه أيضاً بمراقب الشبكة أو محلل الشبكة ويمكن استخدامه بشكل شرعي من جانب الشبكة أو مدير النظام لمراقبة حركة الشبكة والكشف عن الأعطال.

وباستخدام المعلومات التي يتحصل عليها المتجسس على الشبكة، يمكن لأي إدارة أو خبير أمني تحديد عدد كبير من الرزم واستعمال البيانات لتحديد الاختناقات والمساعدة على الحفاظ على نقل البيانات في الشبكة بأمان وكفاءة.

بيبليوغرافيا

[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – International Standard – Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation. https://cve.mitre.org/cve/

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2019