

ما الذي يحتاج كل مكتبي إلى معرفته عن (HTTPS)؟

جاكوب هوفمان أندروز



المخلص:

يناقش المقال (HTTPS) من منظور حماية خصوصية مستخدمي المكتبات وحرية البحث، موضحاً أن حذف سجلات الإعارة وحده لا يحمي استعلامات الفهارس والخدمات الشبكية. ويعرض توصيات لتشفير الموقع كاملاً وإعادة التوجيه وتفعيل الحماية المناسبة، وتأمين المتصفحات، ومطالبة موردي الكتب الإلكترونية بمعايير خصوصية مماثلة. كما يناقش حدود الإضافات الانتقالية ومشكلات بوابات الشبكات اللاسلكية التي قد تترك المستخدم أو تعود تجاهل التحذيرات. ويربط التشفير بتقليل جمع البيانات ومراجعة الاحتفاظ بها والتدقيق الدوري في خدمات الموردين. ويؤكد أن رسالة المكتبة ثابتة بينما تتغير التهديدات ووسائل صونها. وتبقى الأدوات والإصدارات ومشروعات الشهادات ضمن سياق المقال التاريخي، ولا يقدم العرض تحققاً من استمرارها أو دليل إعداد محدثاً لكل بيئة.

الكلمات المفتاحية: (HTTPS)، خصوصية المستخدمين، المكتبات، تشفير الاتصال، خدمات الموردين

مقدمة:

يدرك المكتبيون منذ زمن طويل أن حماية خصوصية المستخدمين أمر حاسم لإتاحة المعرفة. فالكاتب قد تقدم معلومات شديدة الرفض اجتماعياً، ولذلك تحاول مجتمعات محلية وحكومات أحياناً حظر أكثرها إثارة للاعتراض. ويرى المكتبيون بحق أن من واجبهم الحفاظ على الوصول إلى الكتب، وخصوصاً المحظورة. وفي الولايات المتحدة يعد هذا الدفاع عن التعبير جزءاً أصيلاً من حقوق التعديل الأول للدستور.

لكن الإتاحة لا تعني مجرد وجود المادة على الرف. فإذا عُد الكتاب «خطيراً»، فقد يتجنب المستفيد استعارته خوفاً من استخدام السلطات سجل إعارته ضده. ولهذا خاض المكتبيون نضالاً طويلاً وشاقاً لحماية خصوصيته.

ومن ذلك في السنوات الأخيرة مقاومة (Library Connection) لسلطة أوامر حظر الإفصاح غير الدستورية في خطابات الأمن القومي، واختيار مكتبات كثيرة عدم الاحتفاظ بسجلات الإعارة بعد إعادة المواد.

غير أن حماية السجلات وحدها لم تعد كافية. فكثيرًا ما يصل المستفيدون إلى الفهارس والخدمات الأخرى عبر الإنترنت. وتعلمنا خلال السنتين الماضيتين أن وكالة الأمن القومي تجمع كميات هائلة من حركة الإنترنت وتحتفظ بها على نحو غير دستوري. أي إن البحث عن كتاب في فهرس إلكتروني قد يكون سجل قبل أن يستعيّره المستفيد أصلًا. وليست الوكالة التهديد الوحيد؛ فمستفيدون آخرون يستطيعون بأدوات جاهزة اعتراض الاستعلامات وبيانات الدخول بمجرد وجودهم على شبكة المستهدف نفسها.

لحسن الحظ يوجد حل يصبح تطبيقه أسهل كل يوم. فبروتوكول (HTTPS)، النسخة الآمنة من (HTTP)، يشفر جميع الاتصالات بين متصفح الويب وال خادم. وكان الرأي السائد في التسعينيات يقصر ضرورته على حماية أرقام البطاقات الائتمانية وكلمات المرور.

لكن هذا الرأي تغير لسببين: اتضح تكرر التجسس على المعلومات لأسباب غير مالية؛ وخفضت الخوارزميات المحسنة وسرعات المعالجة كلفة (HTTPS) كثيرًا. فقد أفادت (Google) مثلاً بأن تطبيقه زاد كلفة المعالج 1% فقط.

أما الكلفة القديمة الأخرى، الحصول على شهادة، فتحوّلت خلال العقد الماضي من باهظة إلى مجانية بالكامل. وقد يكون الحصول على شهادة مجانية وإعدادها معقدًا، لكن (EFF) و (Mozilla) ومؤسسات أخرى تعمل على إزالة المتاعب بمشروع (Let's Encrypt) الجديد، الذي سيقدم شهادات مجانية سهلة الإعداد.

واحتفالًا بأسبوع «اختر الخصوصية» لجمعية المكتبات الأمريكية، تقدم (EFF) خمس توصيات للمكتبات.

(HTTPS) للموقع كله:

تستخدم بعض المكتبات (HTTPS) في جزء صغير جدًا من الموقع: نموذج الدخول إلى السجلات وطلب الكتب. وهذا غير كافٍ، فقد بينت أبحاث الأمن استحالة تأمين جزء من الموقع وحده. وينبغي أن تضمن المكتبة استخدامه في كل جزء من الصفحة الرئيسة إلى الفهرس، وفي كل الأوقات.

أي ينبغي أن يظهر في شريط العنوان بعد تحميل الموقع اتصال يستخدم (HTTPS). وينبغي في الخلفية إعادة توجيه الزوار توجيهًا دائمًا من (HTTP) غير الآمن إلى (HTTPS).

كما ينبغي ضبط ترويسة (HTTP Strict-Transport-Security)، أو (HSTS)، لضمان حصول الزوار العائدين دائمًا على النسخة الآمنة، حتى عند التدخل في الشبكة.

متصفحات أكثر أمانًا لحواسيبكم:

ما زالت مكتبات كثيرة عالقة مع إصدارات قديمة من (Internet Explorer) تفتقر إلى بعض خصائص أمن المتصفحات الحديثة، ومنها (HSTS). ومع أنه أضيف دعمها مؤخرًا جدًا، فإننا ما زلنا نوصي بـ (Firefox) أو (Chrome). فإلى جانب خصائص الأمن المدمجة، يدعمان طيفًا واسعًا من إضافات الأمن والخصوصية، مثل (HTTPS Everywhere) و (Privacy Badger).

HTTPS Everywhere) للمتصفحات:

تقدم (EFF) إضافة للمتصفح تساعد الناس على استخدام النسخة الآمنة من المواقع متى أمكن. وتستخدم مواقع كثيرة (HTTPS) في جزء صغير من مواقعها دون باقيها. وبمساهمات المجتمع من أنحاء العالم، نعد قائمة بهذه المواقع، ثم تحول الإضافة الاتصال بهذه الصفحات من (HTTP) إلى (HTTPS) عند زيارتها.

نوصي بها لحواسيب المكتبة كيلا يعترض المتطفلون استعلامات المستخدمين إلى المواقع الخارجية. ولها استخدام مهم آخر: يمكن إضافة موقع مكتبتكم إلى قائمتنا. وهذا مفيد إن كان الموقع يدعم (HTTPS) جزئياً ولم يعتمد استخدامه وحده بعد. لكن من المهم على المدى الأبعد تحويل الموقع كله إليه لخدمة المستخدمين الذين لا يملكون الإضافة.

مطالبة مزودي الكتب الإلكترونية باستخدام (HTTPS):

للأسف، تجعل قيود إدارة الحقوق الرقمية (DRM) معظم المكتبات لا تستطيع تقديم الكتب الإلكترونية إلا عبر عدد ضئيل جداً من المزودين. وتقاوم (EFF) آثار هذه القيود السلبية، لكننا نوصي في الأثناء بالضغط على المزودين لتحسين التزامات الخصوصية. فقد بين اكتشاف إرسال (Adobe Digital Editions) معلومات نظام الملفات دون تشفير إلى خوادم (Adobe) في السنة الماضية أن المزودين يقصرون كثيراً في الخصوصية.

ينبغي أن تطالب المكتبات كل مزود تتعامل معه باستخدام (HTTPS) في كل تطبيق وفي كل الأوقات. كما ينبغي ألا تقل الحماية التي توفرها سياسات الاحتفاظ بسجلات بيانات الكتب الإلكترونية عما توفره سياسة المكتبة نفسها، وألا تجمع بيانات تتجاوز الحد الضروري لتقديم الخدمة. وينبغي إخضاع التشفير والاحتفاظ بالسجلات كليهما لتدقيق سنوي للتحقق من استمرار عملهما كما ينبغي.

الشبكات اللاسلكية المفتوحة:

الشبكات اللاسلكية المفتوحة شائعة بالفعل في المكتبات، وهذا ممتاز. فهي أفضل السبل وأسهلها لإتاحة الإنترنت للمجتمع. لكن بعض الشبكات تستخدم «بوابات احتجاز» لعرض صفحة بدء تتطلب نقرة إقرار بشروط الاستخدام المقبول. وتسبب هذه البوابات مشكلات متعددة، وخصوصاً لمواقع (HTTPS).

ولأنها تضطر إلى اعتراض حركة الويب، فإنها تطلق تحذيرات «اتصال غير موثوق» عن شهادات مزيفة. وفي أفضل الأحوال تترك المستخدمين وثقل عليهم، وفي أسوأها تدرب رواد المكتبة على تجاهل تحذيرات المتصفح.

ومن أشهر استخداماتها عرض شروط الخدمة، لكنه ليس السبيل الوحيد لتقديم سياسة الوصول. ففي حركة (Open Wireless) نقدم نموذج سياسة يستطيع المشاركون تبنيه بتسمية شبكاتهم (openwireless.org). ويسهل ذلك الانضمام إلى الشبكة دون تحذيرات مربكة في المتصفح.

خاتمة:

للمكتبات دور حاسم في الحفاظ على الوصول إلى المعلومات. وهذا الدور لا يتغير، لكن تحديات الحفاظ عليه تتغير باستمرار. فالخدمات الجديدة والتجسس الواسع على الإنترنت يفرضان على المكتبيين فهم تهديدات خصوصية المستخدمين الجديدة، واتخاذ خطوات لصونها، سواء حجزوا الكتب من منازلهم أو تصفحوا الإنترنت على حواسيب المكتبة.

سيحتاج الأمر إلى عمل كثير، لكن (EFF) واثقة من قدرة مجتمع المكتبات على إنجازه.

المراجع:

- protect their patrons' privacy: <https://chooseprivacyweek.org/>
- ban the most objectionable ones: <http://www.ala.org/bbooks/>
- unconstitutional gag authority of National Security Letters: <http://www.ala.org/offices/oif/ifissues/usactlibrarians>
- off-the-shelf tools: https://www.wireshark.org/docs/wsug_html/
- 1% increase in CPU costs: <https://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>
- certificate,: <https://www.instantssl.com/ssl-certificate-products/https.html>
- completely: <http://www.startssl.com/?app=1>
- free: <https://buy.wosign.com/free/>
- Let's Encrypt: <https://letsencrypt.org/>
- Choose Privacy Week: <https://chooseprivacyweek.org/>
- Security research: <http://www.thoughtcrime.org/software/sslstrip/>
- HTTP Strict-Transport-Security header: <https://https.cio.gov/hsts/>
- very recently added to Internet Explorer: <http://blogs.msdn.com/b/ie/archive/2015/02/16/http-strict-transport-security-comes-to-internet-explorer.aspx>
- HTTPS Everywhere: <https://www.eff.org/https-everywhere/>
- Privacy Badger: <https://www.eff.org/privacybadger>
- HTTPS Everywhere: <https://www.eff.org/https-everywhere/>
- add your own library's site: <https://www.eff.org/https-everywhere/rulesets>
- DRM lockup: <https://www.eff.org/issues/drm>
- sent unencrypted filesystem information: <https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security>
- Adobe's servers: <https://www.eff.org/deeplinks/2014/10/what-we-can-learn-adobe-e-reader-mess>
- Open wireless: <https://openwireless.org/>
- captive portals: https://en.wikipedia.org/wiki/Captive_portal
- problems: <https://www.eff.org/deeplinks/2013/07/not-quite-open-wireless-what-does-it-mean-be-really-open>
- display a Terms of Service page: <https://openwireless.org/myths-legal>
- example policy: <https://openwireless.org/important-information.html>