الجمهورية العربية السورية
جامعة قرطبة الخاصة
كلية الهندسة / تكنولوجيا هندسة الاتصالات والمعلومات

ملخص محاضرة خاصة بمقرر مادة
"أمن ووثوقية معلومات"
للفصل الثاني للعام الدراسي 2020/2019

الولوج الآمن Secure Access إلى شبكة الانترنت

• كيف يتم الولوج Access إلى شبكة الانترنت:

عادة يتم الولوج إلى شبكة الانترنت من خلال عدة بروتوكولات أهمها وأشهرها هو بروتوكول نقل النص التشعبي Heiber Text Transfer Protocol (HTTP).

تعريف الولوج: يتم أنشاء وصلة اتصال Connection Link بين المستخدم End-User عبر المتصفح Browser وبين الموقع المطلوب Web-Site عبر المخدم Server.

I. آلية الولوج عبر بروتوكول نقل النص التشعبي Hyber Text Transfer Protocol (HTTP):

1. عند ولوج المستخدم إلى عنوان ما باستخدام، يتم أنشاء وصلة اتصال Connection Link بين المستخدم End-User وبين الموقع المطلوب عبر المخدم Server. يتم عبرها نقل جميع المعلومات **الصريح** "PlainText.
2. عند عدم تحديد منفذ محدد يتم نقل جميع المعلومات والبيانات عبر المنفذ رقم **80** Port
3. يتم النقل بدون الحاجة إلى فحص صلاحية الموقع وبالتالي **لا يحتاج شهادة تحقق** للموقع المطلوب التواصل معه Certificate Authority (CA).
4. يتم العمل في **طبقة التطبيقات** Application Layer
5. يتم تنفيذ عملية نقل البيانات بشكل **سريع**

• مخاطر الولوج بالنص الصريح Plain Text Access:

إن جميع المعلومات الشخصية (الاسم، العنوان، رقم الحساب البنكي،...) للمستخدم وكذلك البيانات المراد إرسالها بـ "النص الصريح" PlainText غير آمنة Insecure Connection وبالتالي ستكون عرضة لمخاطر المراقبة والتجسس والسرقة من خلال ما يسمى الشخص الثالث الذي يمكن أن يكون موجود بين طرفي الإرسال:

Man in the Middle (**MitM**) والذي يمكن أن يكون أحد أو جميع الأشياء التالية:

1- مزود خدمة الانترنت (نفسه) Internet Service Provider (ISP)
2- الحكومات Goverment
3- المتطفلين Hackers
4- شبكات التجسس Spying Network

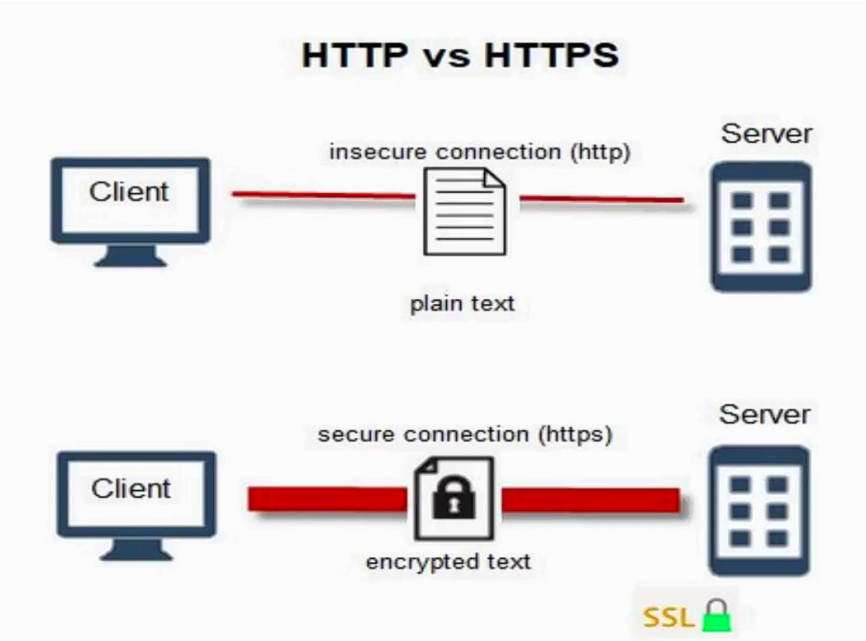
من هنا دعت الحاجة إلى تطوير بروتوكول آمن لنقل المعطيات هو بروتوكول نقل النص التشعبي Heiber Text Transfer Protocol Secure (HTTPS) أو ما يعرف اختصارا Secure HTTP.

III. آلية الولوج عبر بروتوكول نقل النص التشعبي الآمن Hyber Text Transfer Protocol Secure (HTTPS):

1. عند ولوج المستخدم إلى عنوان ما باستخدام، يتم أنشاء وصلة اتصال آمن Secure Connection Link بين المستخدم End-User وبين الموقع المطلوب عبر المخدم Server. يتم عبرها نقل جميع المعلومات الشخصية (الاسم، العنوان، رقم الحساب البنكي،...) للمستخدم وكذلك البيانات المراد إرسالها بـ "**النص المشفر**" Encrypted Text.
2. عند عدم تحديد منفذ محدد يتم نقل جميع المعلومات والبيانات عبر المنفذ رقم **443** Port
3. يتم النقل بعد فحص صلاحية الموقع وبالتالي **يحتاج شهادة تحقق من الصلاحية** للموقع المطلوب التواصل معه Certificate Authority (CA).
4. بعد التحقق يتم **تشفير جميع المعلومات والبيانات** باستخدام أحد البروتوكولين التاليين:
   - بروتوكول طبقة المنافذ الآمنة Secure Sockets Layer (**SSL**) (وهو النسخة الأقدم لبروتوكول التشفير المستخدم في تشفير بروتوكول نقل النص التشعبي HTTP)
   - بروتوكول طبقة المنافذ الآمنة Transport Layer Seurity (**TLS**) (وهو النسخة الأحدث لبروتوكول التشفير المستخدم في تشفير بروتوكول نقل النص التشعبي HTTP)
5. يُعيد الانتهاء من عمليات التشفير تظهر **أيقونة "القفل" Padlock Icon** والتي تعني أن جميع المعلومات والبيانات التي ستنتقل لاحقا، ستكون بالنص المشفر Encrypted Text.
6. يتم العمل في **طبقة النقل** Transport Layer
7. يتم تنفيذ عملية نقل البيانات بشكل **أبطأ** من البروتوكول HTTP بزمن يتراوح بين(500 -250 mSec) وذلك لأن عمليات التشفير المنفذة على المعلومات والبيانات تحتاج لوقت إضافي تبعا لنوع وخصائص بروتوكول التشفير المستخدم.

- **جدول مقارنة الولوج باستخدام بروتوكولي HTTP vs HTTPS:**

Protocol	HTTP	HTTTS
Text	Encrypted Text	Plain Text
Default Port	80	443
Certificate Authority (CA)	no	yes
Connection	Insecure Connection	Secure Connection
Operating Layer	Application Layer	Transport Layer
Pad Icon	no	yes



• ملاحظات:

• يعتبر محرك البحث google أن جميع المواقع Web-Sites و المخدمات Servers التي لا تمتلك شهادة التحقق CA ولا تعمل وفق البروتوكول HTTPS غير آمنة.

• إن ظهور أيقونة القفل PadLock لا تعني –بالضرورة أن الموقع آمن- بل تعني أن جميع المعلومات والبيانات المنقولة ستكون بالنص المشفر Encrypted Text.

• يعتبر البروتوكول HTTPS مثال عن **التشفير المختلط** Mixed Encryption حيث يتم فيه تنفيذ نوعين من أنواع التشفير:

1- التشفير غير المتماثل Asymmetric Encryption:

2- التشفير المتماثل Symmetric Encryption:

مثال:

عند طلب الولوج إلى مخدم Yahoo Server بكتابة الطلب في نافذة بحث المتصفح https://www.yahoo.com

- يقوم **مخدم** Yahoo Server بإنشاء **مفتاحين خاص وعام** يتم من خلالهما التحقق وتسليم الشهادة Certificate Authority (CA) كتوقيع الكتروني Digital Signature للمخدم (**تشفير غير متماثل**)

- بعد إتمام عملية التحقق يقوم المتصفح بإنشاء **مفتاحين متماثلين** يتم من خلالهما تشفير وفك تشفير معطيات الرسالة المراد إرسالها (**تشفير متماثل**)

• تسمي بعض المراجع شهادة التحقق من الصلاحية SSL Certificate بـ شهادة **حيازة أو امتلاك وتطبيق بروتوكول التشفير** (**SSL**) Secure Sockets Layer.

***

أسئلة محتملة:

- ما هي آلية الولوج عبر بروتوكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure (HTTPS) " ذكر ملخص الـ 6 نقاط

- قارن بين بروتوكولي HTTP و HTTPS.

- قارن بين بروتوكولي HTTP و HTTPS من حيث السرعة؟ أيهما تفضل في حال الحاجة إلى إرسال معطيات ضخمة (ملفات فيديو) غير حساسة

- قارن بين بروتوكولي HTTP و HTTPS من حيث السرعة

- عدد مخاطر الولوج بالنص الصريح Plain Text Access؟ وما هو البروتوكول المناسب لنقل معطيات شديدة الحساسية

- عرف كلا من التعابير و المصطلحات التالية بما لا يزيد عن سطرين:

1- MitM
2- SSL
3- TSL
4- Mixed Encryption
5- Certificate Authority (CA)
6- Plain Text
7- Digital Signature
8- Padlock Icon
9- Port Number 80
10- Port Number 443

حلب 2020/3/16

مع كل التمنيات بالنجاح التوفيق

مدرس المقرر: **الدكتور حسن مسلماني**