Syrian Arab republic

Ministry of Higher Education

Syrian private university

Information and system

Syrian Arab republic

Ministry of Higher Education

Syrian private university

Information and system

مشروع أعد لنيل شهادة هندسة المعلوماتية في أمن النظم والمعلومات

(تخرج 2)

SSL\TLS alert sup protocol security enchantment

Prepared by

Badr–Aldeen Abo loubada

Supervised by

Dr. Wassim junadi

Academic year

2025-2026

ملخص

نظرا للتتطور التكنلوجي السريع الذي شهده العالم خلال القرن ال 20، وتبعا للحاجة الماسة الى تأمين الاتصالات بين المسخدمين والمخدمات، ظهرت عدة محاولات هدفها تحسين الواقع الأمني للاتصلات، ومن هذة المحاولات تم تطوير برتوكول ال (secure socket layer) SSL، ويعرف ايضا ب (transport_layer_security)TLS.

بروتوكول TLS ونسخته السابقة SSL هو احد أكثر بروتوكولات الأمن السيبراني استخداما في مجال تصفح الانترنت، والذي يأمن السرية والتوثق من طرف واحد بين جهتي الاتصال (السيرفر والجهاز المتصل)، والذي يعتمد بشكل اساسي في اتصاله على بروتكول الاتصال الشبكي TCP(transmutation_control_protocol) في الطبقة الرابعة من طبقات ال OSI(open system interconnection).

ومن ضمن برتوكلاته المستخدمة هو البرتوكول الفرعي Alert protocol، والذي يقوم بارسال إشارة تنبيه لكلا الطرفين المتصلين بانهاء الجلسة من اجل الحفاظ على سلامة المعلومات من التعديل او التسريب، وغيرها من الأسباب التقنيه، وبناء على درجة التنبيه اما يتم انهاء الجلسة بشكل مباشر و غلق الاتصال من أحد الأطراف دون اعلام الطرف الاخر، او يتم بناء على اتفاق من قبل الطرفين مما يتيح انهاء الاتصال بشكل حميد.

ورغم صغر حجم ال Alert protocol الا انه احد اهم نقاط الحفاظ على اتصال أمن ضمن الجلسة المنشئة.

وسيتناول هذا البحث بعض اهم النقاط التي يمكن استغلالها ضمن Alert protocol، وسوف يتم العمل على فرض محاولات تحسين وإجراء مقارنات حول ما إذا كانت هذه التحسينات مجدية ويمكن تطبيقها على الواقع.

الفهرس

فهرس الأشكال

فهرس الجداول

قائمة المصطلحات

1. Line_tow
   1.1. Sup_line_two
   1.2. Sup_line_two
2. Line
   2.1. شس

قائمة الرموز

1. Line_tow
   1.1 Sup_line_two
   1.2 Sup_line_two
2. Line
   2.1

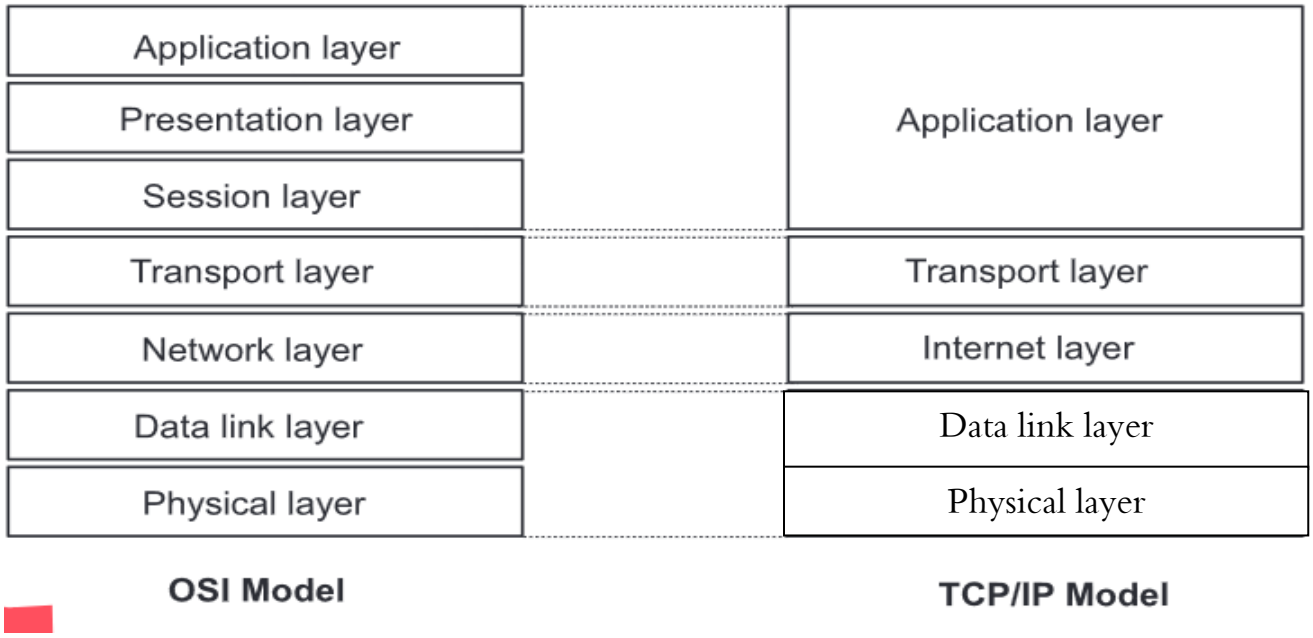
1 المقدمة

تهدف هذه المقدمة الى وضع حجر الاساس لموضوع هذا البحث، تبدء بذكر اهم مفاهيم أمن المعلومات والاتصالات بالفقرة 1,1، وثم تتعمق بشرح برتوكول الاتصال الأمن SSL\TLS بشكل عام، وتتابع بشرح البرتوكول الفرعي Alert sup protocol بشكل بسيط بالفقرة 1,2 وأهم جزئياته التي سيتم دراستها والعمل عليها 1,3 ، وسيتم توضيحهدف البحث 1,4، وعرض الدراسات المرجعية والمقارنة بينها 1,5، وتليها التطبيقات العملية 1,6 والتحديات 1,7.

1.1 أمن المعلومات والاتصالات

تبعا ل internet security glossary المحتوى في FC 4949 [1]، information security (INFOSEC) تشير الى "الإجرائات التي تطبق وتأكد على خدمات الأمن ضمن نظام المعلومات، مضمنا نظام الحاسوب (computer security) و نظم الاتصال (communication security)." وضمن هذا السياق، computer security (COMPUSEC) تشير الى خدمات الأمن التي يوفرها نظام الحاسوب (مثال خدمات تحكم الوصول)، بينما communication security (COMSEC) تشير خدنات الأمن التي يوفرها نظام الاتصال المسؤول تبادل المعلومات (مثال سرية المعلومات و التحقق و خدمات السلامة)، وبالتالي من الاجباري في اطار التنفيذ العملي COPMUSEC و COMSEC يجب أن يعملا على توفير قيمة مناسبة من INFOSEC، لانه وإذا فرضنا على سبيل المثال ان المعلومات مشفرة ومحميه خلال نقلها عبر الشبكة، ولكن في نفس الوقت المعلومات غير مشفرة في احدى الجهات التي يتم حفظ المعلومات ضمنها، وهذا يؤدي الى تغريض هذه المعلومات الى خطر الهجوم والحصول عليها من طرف ليس مخول له الحصول عليها، وهاذا يدل على أن ال COMSEC و ال COMPUSEC يجب أن يتوجدا معا لتأمين INFOSEC وخدمة حماية كاملة.

المعيار المستخدم ضمن البحث لبنية الأمان ال OSI (open systems intercommunication) المعرف من قبل ISO (international organization for standardization) [2]، دون الدخول الدقيق في المعيار نكتفي بذكر طبقات الاتصال المعرفة في المعيار OSI والذي يصف سبع طبقات والطبقات التي تقابله في معيار TCP/IP الذي يصف خمس طبقات، يظهر الشكل 1,1 الطبقات في كل معيار



Transport Layer Security 1.2

بعد ظهور WWW في النصف الاول 1990s وانتشار التسوق الالكتروني، ةاستخدام المعلومات الشخصية على صفحات الويب كمعلومات البطاقات البنكية وغيرها من المعلومات الخاصة، بدء تفكير الشركات الكبرى يذهب نحو طرق نقل المعلومات على الشابكة بأسلوب أمن يحمي المعلومات خلال النقل بين الطرفين، ومن ضمن الشركات كانت شركة Netscape Communication[1] والتي وضعن برتكول بين الطبقتين، وكانتطبقة وسيطة بين طبقة دنبا وطبقة عليا في مجال الأمن، وهي طبقة ال SSL/TLS وكانت وظيفتها تأمين الاتصال ونقل المعلومات بشكل أمن، ولموقها بين طبقات ال OSI اعتبرت طبقة التوصيل الأمن، والتي تعمل مع طبقة الاتصال وبروتكول ال TCP الذي يعتمد عليه في نقل المعلومات.

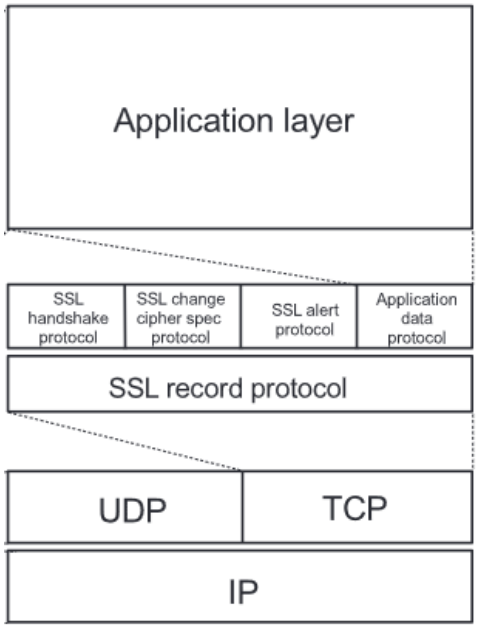
SSL/TLS هو بروتكول بين يعمل بين المستخدم والمخدم ويوفر خدمات الأمن التاليه [2].

- خدمة توثق (توثق كيان وتوتق أصل معلومات)
- خدمة اتصال مشفر
- خدمة الاتصال السليم (دون استرجاع)

رغم أن بروتكول SSL يستخدم التشفير باستخدام المفتاح العام الا انه لا يدعم خدمة عدم الإنكار وذلك لأنه يسختدم (massage authentication code) MAC عوضا عن التوقيع الرقمي [2].

[1] Netscape Communications (formerly known as Netscape Communications Corporation and commonly known as Netscape) was an American software company that was best known for its web browser, Netscape Navigator. The company was acquired by AOL Inc. (previously known as America Online) in 1999. Today, AOL is a subsidiary of Verizon Communications, Inc.

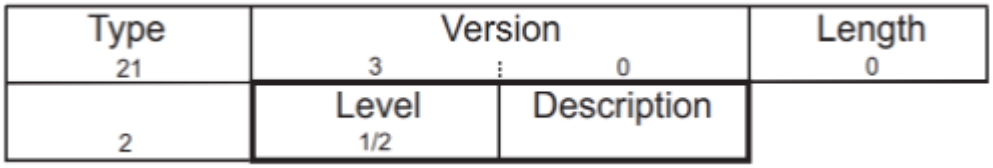
يوضح الشكل 1.2 توضع طبقة ال SSL والبتوكولات الفرعية التي تعمل ضمنه والتي تشتمل على



شكل 1.2 توضيح البروتكولات الفرعية ضمن الطبقات

- Handshake protocol: وهي المسؤولة عن التأسيس الاتصال الأمن الذي يتوثق من الطرفين ويتيح القدرة للطرفين على التوثق من بعضهما، والمفاوضة على ال cipher suite و أسلوب الضغط، تدل ال cipher suite على خوارزميات الأمن المستخدمة في التشفير و التوثق و السلامة
- Change cipher spec protocol: الذي يتيح للطرفين المتصلين للإشارة لبعضهما لتغير المعيار المسخدم، وهو المسؤول عن وضع البارميترات المتفق عليها في مرحلة ال Handshake
- Alert protocol: يتيح الطرفين المتصلين بالارسال إشارات لإحتمال وجود مشاكل ضمن الاتصال او قبل تأسيسه وإرسال التنبيهات التي تشير الى الخطء المحتمل وحودة
- Application data protocol: وهو المسؤول عن تحميل المعلومات من الطبقات العليا ووضعها ضمن ال record protocol والذي بدورة يقوم بأمين المعلقمات خلال النقل.

وأحد اهم الخصائص التي يتمتع بها بروتوكول ال SSL هو استقلاليته عن طبقة التطبيقات، والذي يعطيه القدرة على العمل على اي تطبيق اساسه هو البرتوكول TCP، ويفر له خدمات الأمن المطلوبة[2].



شكل 1.3 رسالة التنبيه

البروتكول الفرعي alert protocol : وهو أحد البرتوكلات الفرعية ضمن ال SSL، وتتكون بنيه الرسالة الخاصة به من 2 byte كما يوضح الشكل 1.3 ويحوي درجة خطورة التنبيه alert level و توصيف التنبيه.

1.3 المشكلة العلمية

تحقيق الاتصال يتطلب عدة من الخطوات التي يتوجب على المستخدم المرور خلالها وخلال هذة الخطوات قد يحصل العديد من الأخطاء مما يسبب بإرسال إشارات لإنهاء الاتصال وكثرة هذة الأخطاء تؤدي الى:

- تقطع في الخدمة
- مخاظر أمنيه
- وتقل وثوقية المستدم بالمنتج

ومن ناحية أخرى وبعد التعدبلات على بتوكول التنبيه اصبح وصف التبيه اقل وضوحا مما أدى الى دقة اقل عند عمليات موجهة الأخطاء وحل الثغرات.

1.4 الهدف من البحث

ايجاد حلول عملية لرفع مستوى الأمن باستخدام برتوكول التنبه الفرعي من خلال اضافة تحسين على بيئة العمل ومن الاحتمالات المتوقعة:

- اضافة تنبيهات جديدة.
- اضافة extension توفر القدرة على تحسين المستوى الأمني.
- تحسن وصف التنبيهات للأ ستفادة منها عند اللزوم.

1.5 الدراسة المراجعية:

في هذه الفقرة نقارن بعض المنشورات والأوراق المنشورة في ما يتعلق ببرتوكول ال SSL/TLS التعديلات عليه خلال الزمن منذ صدوره، و أبحاث تسع الى تحسين عمله أو تحسين واقعة الأمني وأبحاث اخرى كان هدفها تسليط الضوء على الإختراقات التي قد تستغل نقاط الضعف الموجودة في البتوكول.

في البحث الذي قام به سوهيل [4]، قام البحث على شرح البتوكول وعملة في تأمين الاتصال بين المخدم والمستخدم، وقام بالمقارنة بين جميع نسخ البتوكول من صدوره الى وقتنا الحالي ، وبين أهم الثغرات وأنوع الهجوم التي يمكن أستخدامها، وكيف تم التصدي لكل منها في كل نسخة من نسخ البتوكول، وثم اقتر بعص التحسينات والتوصيات التيي بمكن إضافتها لتحسين من من الواقع الأمني للبتوكل في الاتصال الفعلي.

اما بحث بينجامن وأخرون [5]، بدء بتحليل وشرح نسخة البرتوكول TLS 1.3 فقط، وتحديدا البرتوكول الفرعي handshake، حيث شرح اسلوبي تبادل المفاتيح والتوثق المستخدم، الاسلوب الاول التبادل الكامل وهذه الطريقة كانت قائمة على طريقة الرحلة الواحدة، مع استخدام التوقيع للتوثق، و استخدام elliptic curve Diffie-Hellman ephemeral (EC(DHE)) لتبادل المفاتيح، واما الاسلوب الثاني كان يحقق التوثق عبر استخدام ال PSK (pre-shared key)، مع (EC)DHE بشكل اختياري واستخدام ال 0RTT (zero round-time trip)، جوهر البحث كان الدراسة حول استخدام أسلوب تطبيقي لتبادل المفتاح براحل متعددة وكان الهدف هو حماية المفتاح الأساسي من ال replay attack، واها البحث بعرض النتائج ومقارنتها مع المعاير العالمية الخاصة بأمن الشبكات ISO 27001، وتحقيقه خصائص الأمن المرغوب فيها.

في البحث التالي [6] الذي قامت به ماري و جوسيفا، كان هدف البحث تحسين وقت خوارمية تبادل المفاتيح (EC)DHE، حيث بدء البحث بشرح خوارزميات التشفير و التوثق المستخدمة في برتوكول TLS 1.3، وثم شرح خوارزميه تبادل المفاتيح، وبعد ذلك قامو بشرح التعديلات على الخوارزية وذلك باستخدام التحويل الرياضي Chinese Remainder Theorem(CRT) على (EC) لتوليد المفاتيح، وبذلك التطبيق تم مضاعفة فعالية خوارزميه ال hash، وتم توضيح فعالية التعديل على الخوارزمية بتخفيف الخطورة من كلا هجومي ال PAA (Power Analysis Attacks) و SCA(Side Channel Attack)، و إنهاء البحث كان بعرض نتائج تطبيق ومقارنتها مع التطبيق الحالي للخوارزميات المستخدمة.

البحث [7] الذي قام به جاكوب، الذي تمحور بحثه حول فعالية برتوكول TLS[2] و برتوكول mTLS (mutual TLS) ضمن بيئة (IOT(internet of things، حيث قام بالتركيز على الفوائد الأمنيه و العوائق و المقايضة التي كانت بين الأمن وفعالية الاستخدام، و عمل ضمن بيئة اختبار للتحكم بفعالية المفاتيح مضمنا معاملات المقارنة التاخير بين طلب والحصول على المفتاح و كميه الطلبات خلال ثانيه و استهلاك عناصر المعالجة، بيئة الاختبار تمثلت بمخدم Apache و Raspberry Pi و حواسب وهمية بنظام Ubuntu لمتمثيل أجهزة

[2] "TLS provides one-sided authentication and ensures secure communication. However, the reliance on one-sided authentication may expose it. mTLS enhances TLS by introducing mutual authentication providing that both need to be authenticated. This however comes at a higher cost."[7] :page2

الأشياء، وبعد الاختبار تم التأكد أن برتوكول TLS الذي وفر التوثق من طرف واحد قد استطاع تحقيق وقت افضل من mTLS مقارنة بالمعاملات المختارة، مما يجعله اخيار أفضل للأستخدام ضمن IOT، وضمن البحث اقترح استخدام نظام مؤقت لتنظيم دورة حياة الشهادت الرقمية باستخدام البروتوكول المقترح (automatic certificate Management Environment)ACME، وتوصياته بأهمية معايير NIST بما يتعلق بخوارزميات التشفير خفيفة العبء التي تعمل على تحقيق أعلى مستوى أمن بأقل التكاليف الحوسبيه.

ونرى في البحث [8]، حيث يعمل أندروو وأخرون على أستخدام الذكاء الصنعي للتعرف على التصرفات الغير مئلوفه، وتوقع حالات سوء تعريف الشهادات الالكترونيه، والتصدي للهجمات التي تتعلق بالشهادات الإلكترونيه، وكان العمل والتركيز على نمذجة التوقعات و كشف التصرف الغير طبيعي و نظام مؤقت لاتخاذ القرارات ضمن بيئات االشبكات الضخمة، تحوي خوارزملات التعلم الخاصة بالذكاء الصنعي أسلوبي التعلم الملراقب وغير المراقب، ويحوي طرق وخوارزميات التدريب (شجراات القرار، الشبكات العصبونيه) لمعالجة المعلومات الضخمة من قواعد البيانات، والتعرف على نمط الخطر المتوقع، وينتهي البحث بالمقارنة بين عدة نماذج تعليم ونتائج كل منها والمقارنة بين الأقضل منها.

وأما البحث [9] المكتوب من قبل أندريا واخرون، فيدرس فكرة توحيد مركز توزيع الشهادات الإلكترونيه، فكرة البحث نابعة من قلة ال (certified authority) CAs والتي والتحكم بها من قبل جهة الدولة المسؤولة عنه وهذا قد يؤدي الى بعض مشاكل التوزيع التوثق من قبل دول اخرى تبعا للمصالح الدوليه والسياسية، وبذالك تظهر قوة كون المرجع ل CAs بكونه مرجع واحد موثوق من قبل جميع جهات الدوليه، وتأثيره على تجربة المستخدم.

وفي البحث [10] نرى أن كودروباتي، قام بتسليط الضوء على محاولة الكشف عن أخطاء التي قد تحصل بسبب الشهادات الرقميه، وقد تؤدي الى عدم تاسيس الاتصال، باستخدام منبهات تعمل على فحص الشهادة الرقمية قبل بدء بمرحلة ال handshake، وبالتالي الحفاظ على الشهادة بحالة متابعة للتحديثات، و استخدام مراقب على دورة حياة الشهادة الرقمية، وكان دور هذا المراقب إرسال التنبيهات ومن هذه التنبيهات: الشهادة الرقمية ستنتهي صلاحياتها، ويتم إرسال التنبيه قبل 30 يوم من الإنتهاء الفعلي، وذلك لتفداي حالات عدم تأسيس الاتصال.

والبحث [11] من قبل كاسبر واخرون، درس أحد أهم الهجمات التي قد تصيب برتوكول TLS 1.3، وهو هجوم Downgrade، وتم ذكر أول حالات الهجوم ومدى تأثير الهجوم على البتوكول (القدرة على تأسيس الاتصال، استخدام نسخ قديمة ذات مخاطر عاليه، وأيضا ذكر المتحولات التي يستغلها المهاجم عند محاولات الهجوم، نوع ودرجة الثغرة التي تم استغلالها خلال الهجوم والتي أدت بشكل اساسي الى إمكانية حدوث الهجوم، ايضا وضح البحث أن الهجوم لايقتصر على استخدام نسخة قديمة من البتكول غير مستخدمة، وإنما أيضا يمكن استخدامة لكي يتم استخدام خواروميات أقل أمنا، مما يتيح للمهاجم الحصول على المعلومات ضمن اتصال فعال، وانها البحث بمقارنة عدة أنواع من الهجوم ذات هدف الحصول على downgrade.

البحث الذي يليه [12] قام بدراسته مارتن وآخرون، قام البحث على أهميه التنبيهات ومؤشرات الأمان المستخدمة في تطبيقات الويب والتي بدورها كان من واجب تلك التطبيقات نقل هذه التنبيهات الى المستخدم ما يحصل من أخطاء تمنع تأسيس الاتصال، أكد الباحث على

أهمية تلك التنبيهات والمؤشرات كي يستطيع المسخدم وحتى المبرمج فهم سبب الخطء ومواجهته، وثم انهى البحث بتوضيح كيف تم تطوير هذه التنبيهات عبر النسخ المستخدمة من البروتوكول

ونستعين بأحد الأبحاث القديمة [13] للمقارنة العلمية وكيف تطور البرتوكول خلال السنين الأخيرة، حيث قام الباحثون بالعمل على دراسة الأخداء التي حصلت مع المستخدمين وشرح أسباب حدوثها، وكيفيه مواجهتها والحد منها.

1.5.1 مقارنة بين الأبحاث

	البحث [4]	البحث [5]
هدف البحث	تقديم توصيف عام للبرتوكول والتطويرات عليهو توضيح المخاطر العامة و التوصيات لأفضل استخدام	لإثبا أن نسخة البتوكول TLS 1.3 تحقق المتطلبات الأساسية للأمان خلال الاتصال
مواطن قوة البحث	وصف واضح غير معقد للبروتوكول و مقارنة بين النسخ	وصف دقبق ل Handshake

	البحث [6]	البحث[9]	البحث [10]
هدف البحث	تحسين TLS عبر استخدام ECC-based scheme معدلة وذات خطوات أقل	دراسة جدوى حول فوائد استخدام CA مركزي لجميع الدول	دراسة مشكلة عملية في تنظيم شهادات ال SSL، و وصف الحلول لتلك المشكلة
Methodology	تصميم مخطط ECC جديد باستخدام توابع رياضية أبسط	دراسة وتحليل نظري حول موزع الشهادات الرقمية	التعديل الهندسي على دورة حيلة الشهادات الالكترونيه
مواطن قوة البحث	يدعم الأهاداف الأمنيه المطلوبة مع وقت تكلفة أقل	توصيف مشكلة عامة و مدى تأثيرها على الدول	توصيلت عملية قابلة للتطبيق الفعلي على البتوكول لتحسينه

	البحث [11]	البحث [12]	البحث [13]
هدف البحث	بناء بحث حول downgrade ومقارنة بين حالات هجوم سابقة	تتبع كيف يتعامل عارض الويب مع أحطاء ال TLS	دراسة ردة فعل المستخدم وهل تحسنت ردة الفعل بعد تطوير تصميم مفسر الأخطاء
Methodology	دراسة وتحليل ل 15 حالة سابقة	جمع معلومات حول كيفية تفسير كل عارض للأخطاء	دراسة ما يزيد عن 400 حالة
مواطن قوة البحث	القدرة على التعرف على الهجوم في المرات القادمة	فهم كيفيه تطور التفسير الاخطاء من قبل عارض الويب	الدراسة كانت علمية تفاعلية مع المستخدم مما قدم نتائج حقيقية

1.6 التطبيقات العملية

بينما يمكن وصف بروتكول SSL بأبحاث ودراسات نظريه، هذا لم يكن كافيا ابدا لمواجهة المخاطر ة الاختراقات المتجددة كل ساعة، لذلك قام العديد من المطورين والخبراء بتطبيقات عمليه لدراسة قدرة البرتوكول على مواجهة الأخطار والهجمات المختلفة، وحتى القيام بتحسينات وتطبيقها ضمن مخابر عمليه.

ومنها كان التطبيق [14]، حيث درس ماثارو أساليب وطرق لتخفيف من خطورة الهجمات المنتشرة، وقام بالعمل على مخابر لتوضيح صعوبة اختراق الثغرات الأمنيه و تاثيرها على النظام و التكنلوجيا المستخدمة، ويبين خصائص وقوى البروتوكول في الوقت الحالي

وأما التطبيق [15]، فتعمق بتوضيح الثغرات المستغلة من قبل الهجمات (Logjam, Freak, SKIP-TLS, downgrade, timing attack, side channel attack) وقام بالتنبه لمدى خطورتها و تأثير كل منها على نظام الضحية.

وبالتالي قام بينجامين بتصميم أداة لفحص التطبيق الصحيح لبروتوكول TLS [16]، والتي عاجت الكثير من حالت سوء التعريف من طرف المستخدم والحد من مخاطر الاصابة بهجمات ك (SKIP-TLS, FREAK, Logjam).

وقام أيضا حسين وآخرون بالعمل على طريقة حماية للبروتوكول للحماية من Session Hijacking Attacks [17]

1.7 التحديات

أحد أهم التحديات التي تواجة التحسين الأمني على البروتوكول الفرعي Alert protocol هي صعوبة إيجاد تحسين فعال يوازن بين عمل البروتكول الفرعي حيث لايحد التحسين المضاف من أداءة ولا يزيد بالوقت المحاسبي للمعالجة الخاصة بالبرتكول الفرعي.

وأيضا يجب على التحسين المضاف أن لا يتعارض مع عمل باقي البروتوكولات الفرعية من جهة، ويؤدي عمله بكفائة من حهة اخرى.

ومن أهم الملاحظات أن يتفادى التحسين المضاف أضافة معلومات قابلة للتسريب تحت مفهوم تحسين بيئة التسجيل.

ولا ننسى أن يكون التحسين المضاف قابل للتطبيق الواقعي وللتعامل اليومي، أخذا بالعلم أستخامه في ال IOT، وموخرا اضافة بروتوكول ال DTLS.

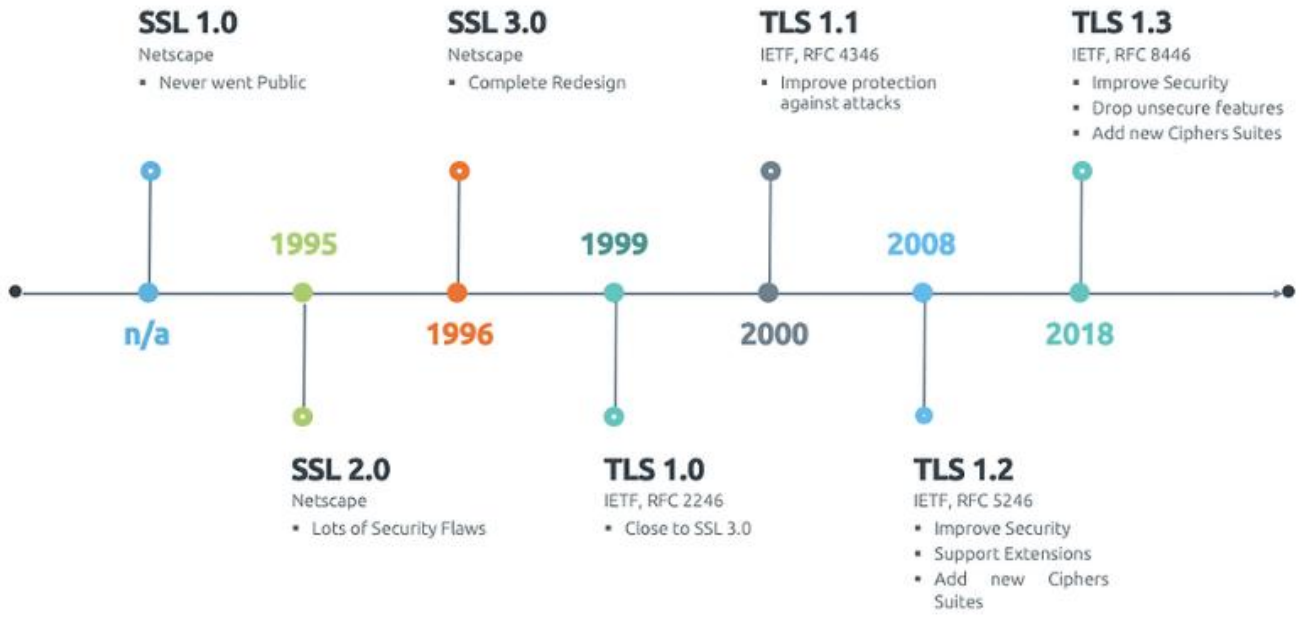
2 الفصل الأول: الدراسة النظرية

بروتوكول ال SSL/TLS هو بروتكول قائم على بوتوكول ال TCP ومنفصل عن الطبقات العليا، مما يتيح القدرة على إنشاء اتصال لاي تطبيق، ويحوي البروتوكول على برونوكولات فرعية Handshake, Change Cipher, Application, Alert كل بروتوكول له عملة في تأسيس الاتصال، وتتمحور الدراسة الحالية على البروتوكول الفرعي Alert.

في هذا الفصل سنقوم بشرح البروتكول بشكل عام، ثم بذكر التعديلات والنسخ التي صدرت له و كيف تطور وكيف اصبح TLS 1.3، وسنناقش كل بروتوكول فرعي متى يتم أسخدامة ولماذا و ما أهميته لتأسيس قناة الاتصال، وثم نتعمق في البروتوكول الفرعي Alert، كيف يعمل ومتى يتم اطلاقة، وكيف يتم استغلاله بالهجمات وتأثيراته على الاتصال قبل التاسيس وبعده.

SSL/TLS 2.1

اول من بدء بتطويربوتوكول الSSL كان Netscape، والذي طور في متصف التسعينات لحماية بيانات HTTP، لكن ومع التطور السريع والأخطاء الثغرات في البروتوكول قامت IETF (The Internet Engineering Task Force) بإعادة تسميه وتصميم البروتوكول الى TLS وصدرت أول نسخة في 1999، ومن وقتها أصبح أحد المعاير الأساسية في الاتصال عبر الشابكة.[4]



history 2.1.1

في منتصف العام 1994 كانت اول نسخة من البروتوكول تعمل لكن ضمن شبكة Netscape Communication الداخلية فقط وذلك بسبب الأخطاء والثغرات العديدة، كمثال البروتوكول لم يكن يستطيع تأمين سلامة البيانت، ولم يكن أيضا يحوي على أرقام تستسلة مما عرضة الى العديد من هجمات ال Replay Attack، ورغم إضافة CheckSums الا أنها لم تكن كافيه لاستخدامها اسلوب CRC(cyclic redundancy check)، عوضا عن استخدامها لخوارميات ال Hash لتأمين السلامة.

لم تقتصر المشاكل على ذلك وكان على المصممين حل العديد من المشاكل قبل اطلاق البرتوكول للعمل الحقيقي، وفي آواخر ال 1995 اطلقت NetScape النسخة الثانية من SSL 2.0، ومن صمن التعديلات كان استبدال CRC ب MD5 التي كانت خلال ذلك الوقت تعتبر أمنة، لكن كان اطلق البرتوكول فعليا وسيلة للحصول على براءة اختراع.

وتلتها نسخة SSL 3.0 والتي اطلقت في ال 1996، وتم نشرها على أنها Internet-Draft entitled RFC 6101[21] في اواخر ال 1996، ومن التحسينات التي ظهرت في SSL 3.0:

- السماح للمستخدم باستخدام certificate chains،والتي كانت في SSL 2.0 تقتصر على شهادة الكترونية من ال ROOT فقط
- استخدام نفاتيح مختلفة في التشفير والتوثق، حيث أنه في SSL 2.0 أدى ذلك إلى مشاكل حيث أنه عند استخدام RC4 في نمط التصدير كان من المجدي محاولة استنتاج المفتاح.
- استبدل ال MD5، ب SHA-1 واستخدام MAC(message authentication code).

وبعد 3 سنين وفي عام 1999 اطلقت ال IETF أول اصدار ل TLS 1.0، وتم نشره ضمن RFC 2246[22]، لكن رغم تغير الاسم في الواقع هناك اختلافات أقل بين ال SSL 3.0 و TLS 1.0 مايوجد بين SSL 3.0 و SSL 2.0.

وحتى بعد إصدار TLS 1.0 توبع العمل على البرتوكول حتى عام 2006 تم اطلاق TLS 1.1 ونشره في RFC 4347[23]، ومن أهم التحسينات كانت مشاكل ال Cryptographic التي وجب حلها، ومن أهمها Padding Oracle Attack، وبعض المشاكل في نمط عمليات ال CBC، وأيضا نشر أول نسخة من DTLS 1.0 تحت RFC 4347 [].

وبعد عامين من المراجعة تم اطلاق ونشر TLS 1.2 أسفل المراقب RFC 5246 [24]، كان أهم تعديل في هذه النسخة جمع TLS extensions، و تعريف باراميترات في registries يتم متابعتها من قبل IANA[3] (Internet assigned Numbers Authority)، و الاستخدام الاختياري لأنماط التشفير المتناظر الذي وفر التوثق وبعد أربع سنين أضيف DTLS 1.2 أسفل المراقب RFC 6347 [].

[3] The IANA is responsible for the global coordination of the domain name system (DNS) root, IP addressing, and other Internet Protocol resources.

ورغم أن TLS 1.2 كان متوجد من 2008 لم يكن هناك اي عجلة في التحديث للنسخة التاليه لأجل ال backward compatibility، لكن كثرة الثغرات الأمنيه جعلت من الضروري إيجاد حلول لذلك، وعندها صممت ال IETF النسخة التاليه من البرتوكول TLS 1.3، لكن لم يكن من الممكن استخدامها للتعديل الكبير الذي حصل في هيكلية البرتوكول، والتي جعلت من الصعب على ال proxy server و ال middleboxes التعامل مع نقل البيانات مما أدى إلى إنهيار التجهيزات، لذا ظهر نمط التوافق الذي جعل حركة البيانات الخاصة ب TLS 1.3 تبدو وكأنها حركة بيانات تابعة ل TLS 1.2، وبعد ما يقارب العشر سنوات وفي عام 2018، استطاع ال TLS 1.3 الحصول على مكانه اسفل RFC 8447 [25]، وبعدها ي أربع سنين ظهر DTLS 1.3 أسفل المراقب RFC 9147.

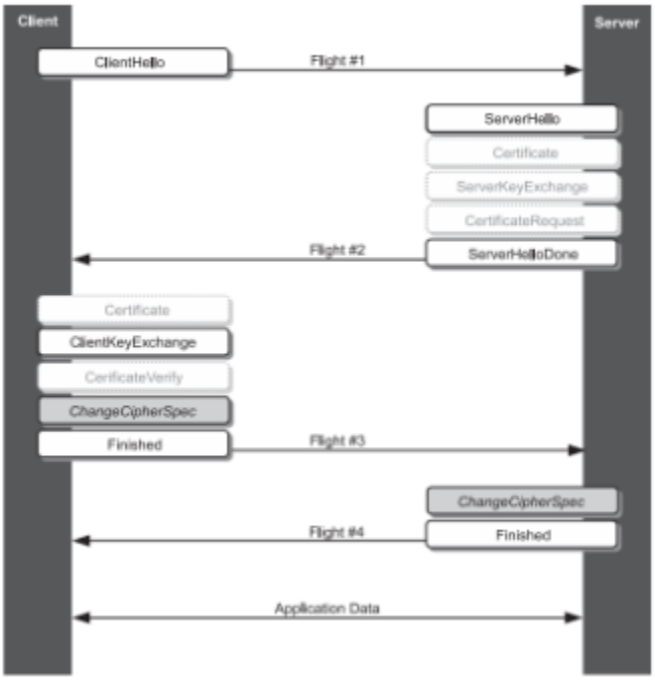
Above allegedly ready for 80% review

Work & Sup protocols 2.1.2

Simple sup chapter intro

- Handshake

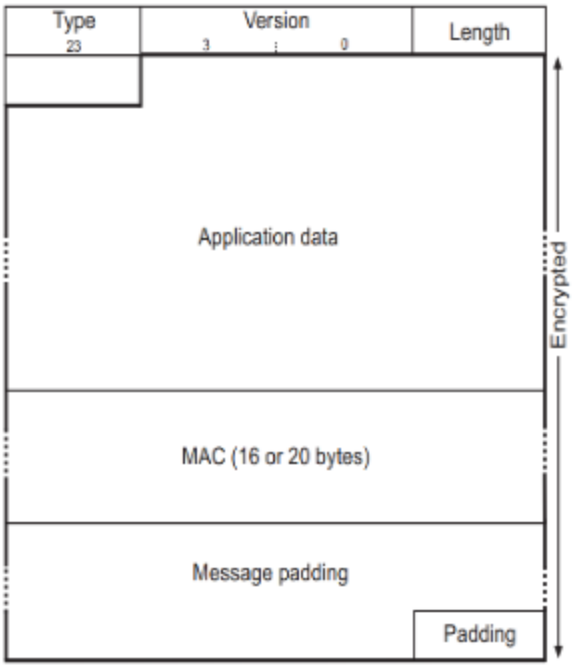
Here goes explaining the handshake



- Change cipher spec

Here goes explaining the change cipher spec

- Application | record



Her goes explaining the application

Alert 2.2

Explain the alert works

The structure and all the alerts (IANA)

History review(upgrades, TSL upgrades effect, new alert and why, unused alerts and why)

Each alert (triggered by [exploit, miss use, bad configuration], how to use it as an exploit)

3 الفصل الثاني: تجهيز بيئة العمل

TO_ADD

each alert how is it triggered really and why

The custom extinction

How versions work with each other

تحتوي بيئة العمل على قسمين أساسين قسم العتاد الفيزيائي والقسم الداخلي وهي أكواد البروتوكول المعدلة

3.1 الأدوات المستخدة

WireShark: وهو تطبيق وظيفته اصتياد ال packets المارة عبر الشابكة المراقبة وتحليلها باقصى دقة ممكنة، ويمكن أيضا التفكير به على أنه جهاز يقوم بتفسير ال traffic المارة من خلال كبل الاتصال.[18]

openSSL: المكتبة الأساسية المستخدمة (libcrypto) والتي تدعم الصلاحية الى العديد من الخوارزميات والتي تستخدم في العديد من معاير الانترنت، الخدمات التي توفرها هذه المكتبة تعطي OpenSSl القدرة على التعامل مع التطبيق العملي ل TLS.[19]

التوابع المستخدمة تحوي التشفير المثماثل، والتشفير باستخادم المفتاح العام والخاص، تبادل المفاتيح، التعامب نع الشهادات الرقمية و MAC والعديد من التوابع الخاصة بأمن الاتصالات

3.2 القسم الفيزيائي

يتكون من 3 أطرف أساسية:

حاسب على أنه مخدم: يحوي على مكتبة ال OpenSSL وعلى أكواد المعدلة لفتح قناة الاستماع لتأسيس الاتصال

حاسب على أنه المستخدم: يحوي مكتبة ال OpenSSL وايضا يحوي على نفس الأكواد لكي يستطيع الطرفين استخدام نفس التعديلات، ويستطيع لبمستخد ايجاد ال port وتتحقيق الاتصال.

حاسب بين المستخدم والمخدم: يحوي على Wireshark لكي نستطيع الأمساك وتحليل ال trafiic بين جهتين الاتصال.

Where to add some attacks and the effects and behavior

[1] Shirey, R., “Internet Security Glossary, Version 2,” RFC 4949 (FYI 36), August 2007.
[2] OPPLIGER, Rolf. SSL and TLS: Theory and Practice. 3rd ed. Norwood, MA: Artech House, 2023.
[3] ISO/IEC 7498-2, Information Processing Systems—Open Systems Interconnection Reference Model—Part 2: Security Architecture, 1989.
[4] Chakkour, Souhail. "Secure Socket Layer (SSL)/TLS in Transport Layer Security", Mississippi State University, 2025. https://www.researchgate.net/publication/391705106_Secure_Socket_Layer_SSLTLS_in_Transport_Layer_Security
[5] Dowling, Benjamin, Marc Fischlin, Felix Günther, and Douglas Stebila. "A cryptographic analysis of the TLS 1.3 handshake protocol." *Journal of Cryptology* 34, no. 4 (2021): 37. https://doi.org/10.1007/s00145-021-09384-1
[6]Menandas, Josepha, and Mary Subaja. "An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL." *International Arab Journal of Information Technology (IAJIT)* 22, no. 5 (2025). https://doi.org/10.34028/iajit/22/5/2
[7]Hallin, Jakob. "Evaluation of TLS and mTLS in Internet of things systems." (2025). https://www.diva-portal.org/smash/record.jsf?pid=diva2:1937634
[8]Miller, Johnathan, Samantha Reed, Michael hompson, Emily Carter, and Andrew James."Machine Learning Approaches for Predicting and Preventing SSL/TLS Certificate Vulnerabilities." (2025). https://www.researchgate.net/profile/Andrew-James-42/publication/394460370_Machine_Learning_Approaches_for_Predicting_and_Preventing_SSLTLS_Certificate_Vulnerabilities/links/689c2fd0a645d8252ba43311/Machine-Learning-Approaches-for-Predicting-and-Preventing-SSL-TLS-Certificate-Vulnerabilities.pdf
[9]Azevedo, Andrei Cordova, Eder John Scheid, Muriel Figueredo Franco, and Lisandro Zambenedetti Granville. "Assessing SSL/TLS Certificate Centralization: Implications for Digital Sovereignty." (2025). https://arxiv.org/abs/2504.16897
[10]Kodurupati, Prashanth. "Handling SSL Certificate Challenges &Solutions Properly For Improved NetworkSecurity." Journal of Technological Innovations 4, no. 3 (2023). http://jtipublishing.com/jti/article/view/71
[11]Alashwali, Eman Salem, and Kasper Rasmussen. "What’s in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS." In *International Conference on Security and Privacy in Communication Systems*, pp. 468-487. Cham: Springer International Publishing, 2018. https://link.springer.com/chapter/10.1007/978-3-030-01704-0_27
[12]Kraus, Lydia, Martin Ukrop, Vashek Matyas, and Tobias Fiebig. "Evolution of SSL/TLS indicators and warnings in web browsers." In *Cambridge International Workshop on Security Protocols*, pp. 267-280. Cham: Springer International Publishing, 2019. https://link.springer.com/chapter/10.1007/978-3-030-57043-9_25
[13]Sunshine, Joshua, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. "Crying wolf: An empirical study of ssl warning effectiveness." In *USENIX security symposium*, pp. 399-416. 2009. https://www.usenix.org/event/sec09/tech/full_papers/sec09_browser.pdf
[14]Matharu, Simreen Kaur. "Exploiting SSL/TLS Vulnerabilities in Modern Technologies." (2021). https://era.library.ualberta.ca/items/64c6bab3-2bec-4b62-af71-42580bb4dd10
[15]Ćurguz, Jelena. "Vulnerabilities of the SSL/TLS Protocol." *Computer Science & Information Technology* 6 (2016): 245-256. https://csitcp.net/paper/6/66csit20.pdf
[16]Beurdouche, Benjamin, Antoine Delignat-Lavaud, Nadim Kobeissi, Alfredo Pironti, and Karthikeyan Bhargavan. "{FLEXTLS}: A Tool for Testing {TLS} Implementations." In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. 2015. https://www.usenix.org/conference/woot15/workshop-program/presentation/beurdouche
[17] Hossain, Md Shohrab, Arnob Paul, Md Hasanul Islam, and Mohammed Atiquzzaman. "Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks." *Netw. Protoc. Algorithms* 10, no. 1 (2018): 83-108. https://www.researchgate.net/profile/Arnob-Paul-2/publication/324448404_Survey_of_the_Protection_Mechanisms_to_the_SSL-based_Session_Hijacking_Attacks/links/6022f588299bf1cc26b5462d/Survey-of-the-Protection-Mechanisms-to-the-SSL-based-Session-Hijacking-Attacks.pdf