TFM – Desenvolupament d'una solució per a l'anàlisi de la seguretat *web*

Estudiant: Oriol Secall i Gasulla

Tutor: María Francisca Hinarejos Campos

Programa: Màster universitari en la seguretat de les tecnologies de la informació i de les comunicacions

Any: 2018-19

Justificació del TFM

- Creixement generalitzat utilització serveis *web* a nivell mundial.
- Creixement vulnerabilitats i atacs en les comunicacions.
- Conscienciació seguretat informàtica i de les comunicacions en ascens per part usuaris.
- Seguretat *web* amb implementacions variables.
- Informació (navegadors) a l'usuari insuficient per conèixer qualitat seguretat.
- Solucions incompletes i/o inexistents per a navegadors moderns.

Objectius del treball

- Proporcionar informació de valor per a l'usuari sobre la seguretat implementada en el lloc *web* que es s'accedeix.

- Establir un criteri per obtenir i mostrar una valoració global i detallada del nivell de seguretat del lloc *web* que s'accedeix.

- Desenvolupar una extensió compatible amb la versió més recent de *Mozilla Firefox* (57+).

Anàlisi

- Anàlisi per a la implementació extensió
  - Estudi dels paràmetres de seguretat a analitzar
    - Certificat digital X.509 de tota la cadena de certificació
      - Algoritme de firma
      - Període de validesa
      - Algoritme de clau pública
    - Protocol SSL/TLS (versió)
    - Conjunt d'algoritmes utilitzats (c*ipher suite*)
      - *Key Exchange*
      - Autenticació
      - *Bulk cipher*
      - *MAC hash*

- Estudi extensions per a *Mozilla Firefox*
  - *WebExtensions*: millora la portabilitat a altres navegadors, es perden funcionalitats (nova API publicada Novembre del 2017) i compatibles amb navegadors actuals.
- Estudi extensions actuals semblants a la solució desitjada
  - Calomel SSL Validation (solució parcial)
  - SSLeuth (*add-on* **no** compatible navegadors actuals, solució parcial)
  - CipherFox (solució parcial)
- API WebExtensions
  - Permet accedir a la informació sobre la seguretat (TLS) amb certes carències de interès:
    - Informació directa de la clau pública del certificat.
    - Accés a les extensions del certificat (excepte EV).
    - Algoritme i mida de la clau firma certificat.
  - S'usen mòduls externs a la API per solucionar necessitats de informació
    - pkijs
    - asn1js
  - Utilització de JS WebPack per poder incloure mòduls externs.

Anàlisi algoritmes i característiques

- Les fonts consultades més destacades per determinar puntuació i pesos:
  - Qualys
    - Servei de test servidor *web* a nivell de seguretat.
  - OpenSSL
    - Informació sobre els *cipher suites* i seguretat.
  - CCN-Cert
    - Bones pràctiques a nivell de seguretat *web*.
  - RFC
    - Estudi d'algoritmes i protocols per a la seguretat de les comunicacions.
  - BlueKrypt
    - Informació sobre recomanacions algoritmes i mida clau a implementar.

Anàlisi algoritmes i característiques

- Extensió actual com a model
  - SSLeuth
    - S'ha contrastat puntuació i estructura del format amb combinació de les fonts consultades per determinar les puntuacions i pesos.
    - S'ha valorat els càlculs de puntuació implementats amb canvis:
      - Càlcul puntuació certificat per a tota la cadena de certificació.
      - S'han agregat més algoritmes.
      - S'ha agregat el protocol TLS v1.3 de forma més consistent (SSLeuth amb *workaround*).
    - S'informa de més informació sobre els certificat i la cadena completa.

Criteri de puntuació

- Comprovacions crítiques (puntuació 0) i no crítiques
  - Crítiques:
    - Domini no coincideix
    - Certificat auto-firmat
    - No es confia en el certificat (o no instal·lat en el navegador)
    - Autenticació anònima
    - Restricció bàsica del certificat entitat final invàlida
    - Ús de la clau invàlida
    - Cadena de certificació incorrecte

Criteri de puntuació

- No crítiques:
  - *Cipher suite*
    - *Protocol + Key Exchange + Autenticació + Bulk cipher + MAC Hash*
  - *Perfect Forward Secrecy*
  - *Extended Validated*
  - Per a cada certificat de la cadena:
    - Algoritme i mida de la clau de la firma
    - Algoritme i mida de la clau pública
    - Validesa certificat

Càlcul puntuacions

- **Puntuació total** = (Puntuació connexió · Pes connexió) + (Puntuació cadena certificació · Pes Cadena certificació);
- **Puntuació connexió** = (Puntuació *cipher suite* · Pes *cipher suite*) + (Puntuació EV · Pes EV) + (Puntuació PFS · Pes PFS);
- **Puntuació *cipher suite*** = (Puntuació protocol TLS · Pes protocol TLS) + (Puntuació *Key Exchange* · Pes *Key Exchange*) + (Pes Autenticació · Puntuació Autenticació) + (Puntuació *Bulk Cipher* · Pes *Bulk Cipher*) + (Puntuació *Hash* · Pes *Hash*);
- **Puntuació cadena certificació** = Σ certificats ((Certifitat· Pes Certificat) · (Puntuació validesa · Pes Validesa) + (Puntuació Algoritme Clau Pública · Pes Algoritme Clau Pública) · (Puntuació Algoritme Firma · Pes Algoritme Firma));

Taula Pesos

Variable	Pes (0% a 100%)
Cadena de certificats	
Certificat entitat final	50%
Certificat CA (*intermediate*)	25%
Certificat CA *root*	25%
Certificat	
Validesa certificat	20%
Algoritme clau pública certificat	30%
Algoritme firma certificat	50%
Cipher suite	
Versió protocol SSL/TLS	10%
Algoritme intercanvi de claus (*Key Exchange*)	30%
Algoritme firma (Autenticació)	10%
Algoritme xifrat en bloc (*Bulk Cipher*)	20%
Algoritme *hash* (MAC *hash*)	30%
Connexió	
Cipher suite	70%
Extended Validation (EV)	15%
Perfect forward secrecy (PFS)	15%
Puntuació total	
Connexió	60%
Cadena de certificació	40%

Informació no accessible

- Informació sobre l'estat de revocació del certificat.
  - Impossibilitat d'usar protocol OCSP a través de la API de les *WebExtensions*.
  - Cap mètode de la API per accedir a la informació OCSP *staple*.
  - Solucions trobades de tercers incompletes i/o no implementables.
  - Navegadors moderns comproven estat OCSP per defecte.
  - Majoria navegadors per defecte no accepten certificat revocat.
- Mida de la clau emprada en algoritmes no ECC
  - Pels algoritmes per al intercanvi de la clau i autenticació tals com DH, DHE, RSA, DSA (DSS) la API no retorna la mida de la clau.

Joc de proves i verificació

- S'ha provat l'extensió en llocs web amb diferents escenaris
  - Protocol TLS.
  - Estats certificat
  - Validesa certificat
  - Certificat auto-firmat
  - Certificat no confiable
  - Diferents algoritmes d'intercanvi de clau, *bulk cipher*, firma, clau pública…
- S'ha provat l'extensió en els 5 primers dominis més consultats a nivell mundial
  - Facebook, Twitter, Google, Youtube, Instagram.
- S'ha provat l'extensió a qualys.com (servei *web* test seguretat).

Anàlisi *World Wide Web*

- S’ha analitzat els 500 dominis més consultats a nivell mundial per treure una puntuació global Mitjana

  - Pels 500 dominis amb només protocol HTTPS (439 dominis) la puntuació global mitjana és de 8,44.

  - Pels 500 dominis (es consideren protocol HTTP i HTTPS) la puntuació global mitjana és de 7.44.

Definició possibles millores futures

- Inclusió comprovació estat revocació a través del protocol OCSP.
- Analitzar i considerar la mida de la clau emprada per a l'autenticació i el intercanvi de claus en la puntuació en els casos que la API actualment no proporciona la informació.
- Automatització per poder valorar en *batch* varis dominis.
- Inclusió del concepte 'Certificate Transparency' en l'algoritme de càlcul de la puntuació quan es consideri adequat.
- Possibilitat de modificar la puntuació dels algoritmes per part de l'usuari.
- Mostrar puntuació global sense prémer botó extensió.

Conclusions

- S’ha aconseguit complir amb els objectius establerts.
- Deficiències parcials per poder valorar totalment la qualitat de la seguretat en una connexió a un servidor *web* en alguns escenaris *(revocació certificat i mida clau alguns algoritmes)*
- Dificultats per implementar la solució amb la API *WebExtensions*.
- Extensió en continu actualització (vulnerabilitats, nous algoritmes i protocols) de les puntuacions.
- Seguretat de la ‘WWW’ alta (HTTPS), seguretat protocol HTTP(S) mitg-alta (12’2 % dominis consultats no son HTTPS). Millor lloc *web* consultat és qualys.com.