UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Disciplina: INE 5680 – Segurança da Informação e de Redes
Professora: Carla Merkle Westphall

Tarefa Teórica – Handshake SSL/TLS (Secure Socket Layer/Transport Layer Security)

Material para fazer a tarefa: cap. 17 do livro do Stallings, software Wireshark, Internet, RFCs da versão 1.2 e 1.3 do TLS.

Entregar no moodle as respostas de todas as questões!

1) É possível verificar as possibilidades do SSL/TLS do seu browser e do seu servidor. Cole os resultados (screenshot) aqui e comente o que chamou a sua atenção em cada um dos resultados.
   d) https://www.ssllabs.com/ - Acesse este site e teste o seu browser (diferentes tipos de browser podem ter resultados diferentes na sua máquina).
   e) https://www.ssllabs.com/ - Acesse este site e teste um servidor que usa o SSL. Cuide para não acessar apenas um proxy de servidor real.

   Obs.: ***forward secrecy*** significa que se uma chave for comprometida durante uma sessão, esse conhecimento/fato não afeta a segurança de sessões anteriores. A troca de chaves RSA (RSA key Exchange) não fornece *forward secrecy* pois se alguma chave privada for comprometida, todo o tráfego anterior pode ser decifrado.

2) Leia as recomendações da página https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices e faça um pequeno resumo das seções 1 e 2 dessas recomendações.

3) Explique de forma geral as quatro fases do handshake de acordo com as páginas do livro do Stallings – 386, 387, 388 e 389 (o pdf do capítulo está anexado junto na tarefa).

4) **Coleta de um tráfego de handshake TLS**
   Você deve capturar um handshake do TLS no Wireshark: ative a captura de pacotes no Wireshark, abra a conexão com um site que usa HTTPS e capture o tráfego. Depois de estabelecer a conexão segura, pare a captura, salve a capture com seu nome (para entregar no moodle o arquivo). Comente um pouco o handshake do seu tráfego.

5) Compare **o handshake** dos protocolos TLS v1.2 e TLS v1.3 lendo o material dos seguintes sites e observando as figuras. Tente responder de forma resumida, como feito na questão 3.
   - https://www.cloudflare.com/learning-resources/tls-1-3/
   - https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/
   - RFC TLS 1.3: https://tools.ietf.org/html/rfc8446 (seção 2)
   - RFC TLS 1.2: https://tools.ietf.org/html/rfc5246 (seção 7.3)

Handshake TLS 1.2

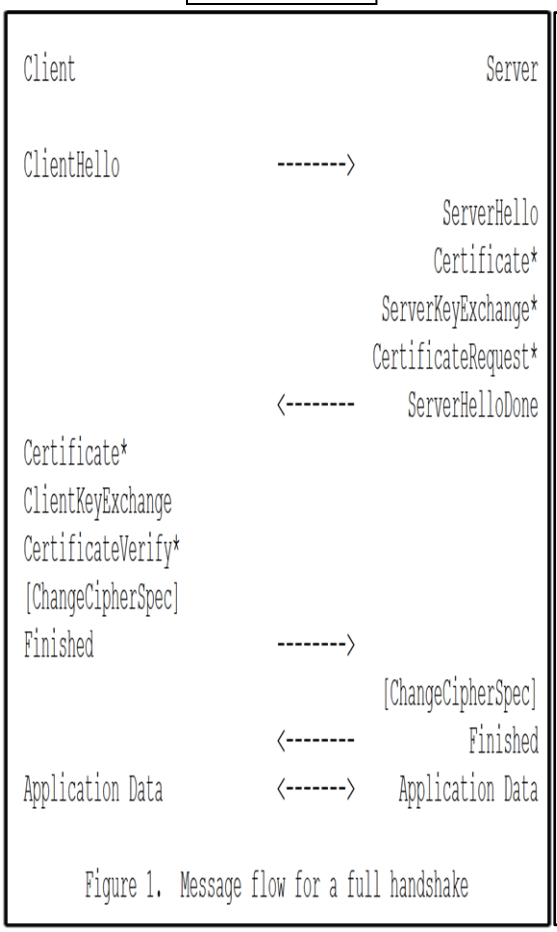

Figure 1. Message flow for a full handshake

Handshake TLS 1.3

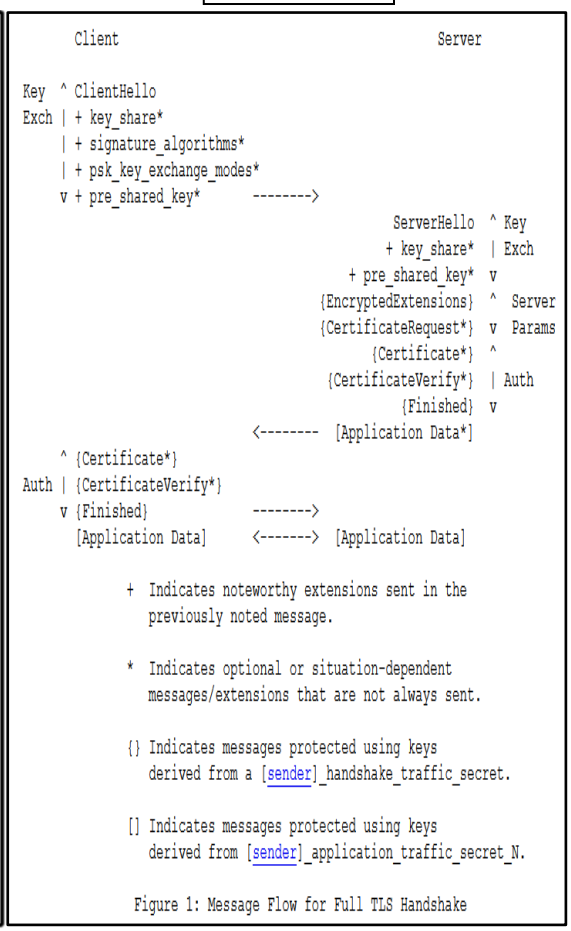

Figure 1: Message Flow for Full TLS Handshake

Você recebeu dois arquivos em anexo – gmail12 e facebook13. Esses arquivos contêm tráfegos de handshake estabelecidos com o gmail e com o facebook. Você irá analisar o handshake do TLS 1.2 no tráfego do gmail e o handshake do TLS 1.3 no tráfego do facebook. A análise do handshake será feita nas questões que seguem.

TLS 1.2: abra o arquivo gmail12

6) **Client Hello**: Responda: a) Qual o objetivo da mensagem Client Hello? b) Copie e cole um screenshot do campo Cipher Suites aqui na resposta.

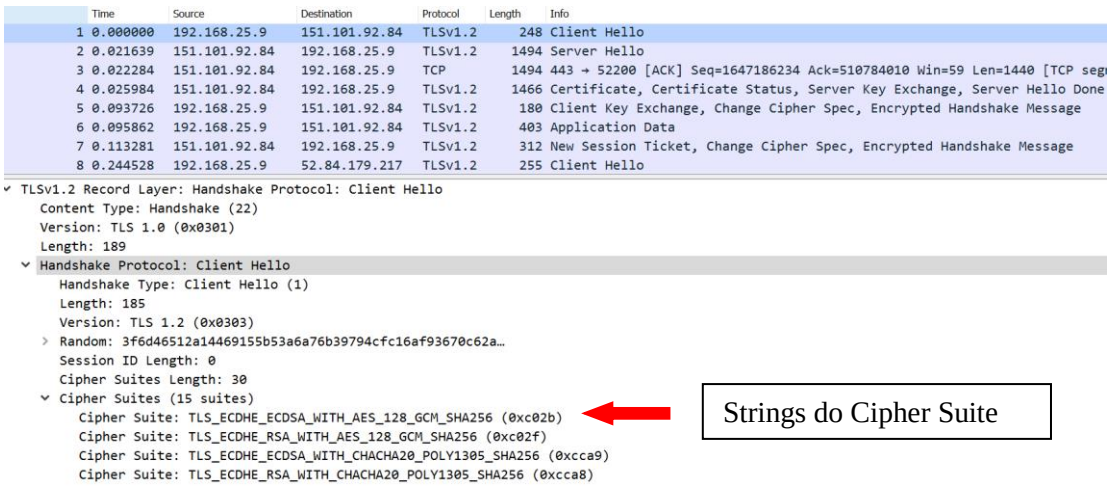

Figura 1 – Detalhes do Client Hello

7) **Server Hello**: a) Copie e cole o valor do Cipher Suite na mensagem Server Hello escolhido pelo servidor. b) Explique o formato da string usada no Cipher Suites (pode-se pesquisar na RFC ou na seguinte página web: https://wiki.mozilla.org/Security/Server_Side_TLS#Cipher_names_correspondence_table).
   c) Qual o algoritmo de troca de chaves (Kx)?
   d) Qual o algoritmo usado para autenticação (Au)?
   e) Qual o algoritmo de criptografia simétrica e qual o modo (Enc)?
   f) Qual o algoritmo de hash usado para o HMAC (Mac)?

8) **Certificate, Certificate Status, Server Key Exchange, Server Hello Done**: Copie e cole um screenshot (um pedaço) dos detalhes dos tráfegos aqui na resposta para cada questão abaixo. Você pode pesquisar detalhes em http://blog.catchpoint.com/2017/05/12/dissecting-tls-using-wireshark/.
   a) O que é enviado na mensagem Certificate? Explique.
   b) Qual o objetivo da mensagem Certificate Status? Pesquise e responda.
   c) Na mensagem Server Key Exchange foi usado o Diffie-Hellmann?

   O DH precisa ser entendido. Responda as seguintes perguntas:
   d) Qual o problema do DH anônimo de acordo com a página 387 do livro do Stallings?
   e) Como funciona o Diffie-Hellmann efêmero (DHE) de acordo com a página 387 do livro do Stallings?
   f) Existem parâmetros do Diffie-Helmann no seu tráfego? Quais os valores?
   g) O que é a chave pública (pubkey) no Diffie-Hellmann?
   h) Esses valores de Diffie-Helmann do tráfego são assinados?

No exemplo da figura 2 foi usado o ECDHE – Diffie-Hellmann com Curvas Elípticas. O nome da curva é secp256r1 e por isso os parâmetros "p" e "g" são os listados na figura 3 (Consultar: https://tlseminar.github.io/first-few-milliseconds/).

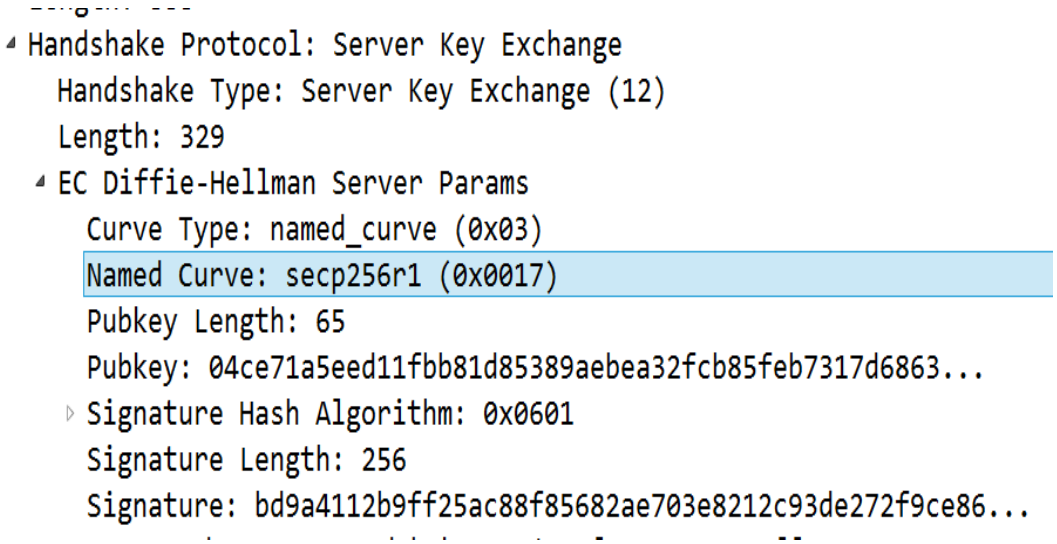

Figura 2 – Detalhes do Server Key Exchange.

```
p = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

G = 03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
```

Figura 3 – Valores de p e g para curvas elípticas secp256r1.

9) **Client Key Exchange:** copie e cole os valores usando seu tráfego. Copie e cole um screenshot dos detalhes do tráfego aqui na resposta para cada questão abaixo (quando possível).
   a) O que é enviado no Client Key Exchange a respeito do Diffie-Helmann?

TLS 1.3: abra o arquivo facebook13

Copie e cole um screenshot dos detalhes do tráfego aqui na resposta para cada questão abaixo (quando possível).

10) **Client Hello**: Responda:
   a) Qual o objetivo da mensagem Client Hello no protocolo TLS 1.3?
   b) Quais métodos de troca de chaves são usados no TLS 1.3?
   c) O que significa o campo key_share nas Extensions do Client Hello? O que trafega nesse campo?
   d) Como pode ser feita a autenticação no TLS 1.3?

11) **Server Hello**:
   a) Qual o objetivo da mensagem Server Hello no protocolo TLS 1.3?
   b) Qual foi o Cipher Suite escolhido pelo servidor?
   c) O que significa o campo key_share nas Extensions do Server Hello? O que trafega nesse campo?
   d) Existem parâmetros do Diffie-Hellmann no Server Hello?

Referências:

1. Atividade - http://en.wikiversity.org/wiki/Wireshark/HTTPS
2. Wireshark/HTTPS - http://wiki.wireshark.org/SSL
3. Capítulo 17 do Livro do Stallings
4. RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2 - https://tools.ietf.org/html/rfc5246
5. RFC TLS 1.3 - The Transport Layer Security (TLS) Protocol Version 1.3 - https://tools.ietf.org/html/rfc8446
6. TLS - https://hpbn.co/transport-layer-security-tls/
7. The First Few Milliseconds of an TLS 1.2 Connection - https://tlseminar.github.io/first-few-milliseconds/
8. NIST Special Publication 800-52 Revision 1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
9. A Detailed Look at RFC 8446 (a.k.a. TLS 1.3): https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/
10. TLS 1.3 (with AEAD) and TLS 1.2 cipher suites demystified: how to pick your ciphers wisely: https://www.cloudinsidr.com/content/tls-1-3-and-tls-1-2-cipher-suites-demystified-how-to-pick-your-ciphers-wisely/
11. Browsing Experience Security Check: https://www.cloudflare.com/ssl/encrypted-sni/