UTN
Facultad Regional Córdoba

TUP

Tecnicatura Universitaria en Programación

INGLÉS I

Trabajo Práctico Integrador N° 4:
Fixing a Hole in the Web

Trabajo Práctico Integrador III
1° Año – 2° Cuatrimestre

Trabajo Práctico Nº 4

Fixing a Hole in the Web (Erica Naone)
1. Late last week, the Internet Engineering Task Force (IETF) approved a fix to the protocol that guards most sensitive transactions and communications online. But experts expect it to take a year for the fix to be fully applied.
2. The patch repairs a flaw in the protocol that encrypts sensitive communications, including most banking and credit-card transactions. ***It*** repairs the Transport Layer Security (TLS) protocol, which has superseded the Secure Socket Layer (SSL) protocol. TLS is built into Web browsers and Web servers and protects high-value information.
3. The current flaw, discovered by Marsh Ray and Steve Dispensa of a Kansas-based authentication company called Phone Factor, gives an attacker the ability to hijack the first moment of the encrypted conversation between a Web browser and a Web server. This allows the attacker to add a command of his own, which could be as serious as an order to withdraw money from the victim's account. One security researcher demonstrated the attack on Twitter, showing that the flaw could be used to command the server to reveal a user's password.
4. "The reason it's striking is that it's actually a TLS error, or at least arguably so," says Eric Rescorla, a security consultant at a company called RTFM and one of the authors of the draft fix to the protocol. Rescorla says the flaw shows how difficult it actually is to design security protocols for the Internet.
5. To make use of the flaw, an attacker would first have to set up a "man in the middle attack" and intercept traffic between the client and the server. ***This*** might be done by hijacking a particular server on the Internet, for example.
6. The attacker could then exploit a feature of TLS called "renegotiation," which allows a Web server or client to change some of the parameters of an encrypted session while that session is happening. Dispensa explains that the protocol does not make sure that the parties communicating after renegotiation are the same ***ones*** as before.
7. Ray and Dispensa admit that exploiting the flaw would require considerable technical skill, but they say it is significant because it affects servers and clients even if they've implemented the protocol perfectly. "It's pretty clear that nobody understood this property of TLS," Rescorla says.

8. Frank Breedijk, a security professional at a provider of mission critical outsourcing services called Schuberg Philis, based in the Netherlands, says that Rescorla's draft does fix the protocol, but notes that it effectively creates two versions of TLS. If either the client or the server haven't yet installed the fix, he says, the attack is still possible. "TLS/SSL clients and servers are omnipresent," he says. "It's not just browsers and Web servers. Mobile phones, wireless access points, DECT phones, home security systems, and so on, all have the technology in ***them***."
9. "If you believe that you need SSL at all, then you need this fixed," says Ben Laurie, a founding director of the Apache Software Foundation and an OpenSSL developer. That may be easier said than done, however.
10. Ray and Dispensa disclosed the flaw to affected vendors in late September, and Laurie says it's been "no big deal" to write software that fixes it. What's tricky, he says, is getting the patch installed everywhere it needs to be. The fix is "unprecedented," Laurie says, because no one is fully protected until both the client and the server have installed the patch. As a result, browser makers working to fix the problem have to allow for a period when the client will continue to communicate with unpatched and possibly vulnerable servers.
11. "***You*** can't have the clients say, 'Evil old server, can't connect to that,' because that would break the whole world," Laurie says. This means that a second patch will have to be applied to clients later, when experts determine that enough servers have been patched.
12. The process of getting out all the patches is complex enough that Joe Salowey, TLS working group co-chair and a technical leader at Cisco Systems, believes it will be a year or more before the fix will be fully in place.

Actividades:

1. PREPOSICIONES. Extraer cuatro ejemplos diferentes de preposiciones. / Prepositions. Extract.
   (1) _____
   (2) _____
   (3) _____
   (4) _____

2. FRASE PREPOSICIONAL. Extraer dos frases preposicionales. / Prepositional Phrase. Extract.
   (1) _____
   (2) _____

3. CLÁUSULAS CONDICIONALES. Extraer dos ejemplos de cláusulas de condición. Detallar de qué *tipo* o *caso* son. / Conditional Clauses. Extract.
   (1) _____
   (2) _____

4. CLÁUSULAS RELATIVAS. Extraer dos instancias de cláusulas relativas (sin repetir el pronombre relativo). / Relative Clauses. Extract.
   (1) _____
   (2) _____

5. AFIJOS. Encontrar en el texto palabras derivadas de las siguientes. / Affixes. Find.

	Palabra Derivada	**No. de Párrafo**
negotiate		
precedent		
source		
effect		
patch		
encrypt		
present		

6. CONECTORES. Extraer dos conectores diferentes e indicar su relación lógica. Connectors.

7. REFERENTES. Leer en el texto y reconocer a qué/quién hace REFERENCIA el ***ítem lexical subrayado***. Reference.

Bibliografía

MIT Technology Review. (12.01.2010). Fixing a Hole in the Web. n/a. Recuperado de: https://www.technologyreview.com/s/417070/fixing-a-hole-in-the-web/