CIS6370 – Computer and Internet Security

CIS6370 - Computer and Internet Security

Written by:

Christopher Foley
Z15092976

Academic Year: Fall 2017

Q1: An attacker in a local site of a large company managed to break the WEP encryption of the cell phone of an important employee. This company only deals with partners and known customers.

- He then captured some IDs and passwords for the owner of the phone and for some other employees of the site (found in the phone).
- He then accessed some SQL-based forms in the web site of the company that let employees access the database. Using the passwords and SQL injection he accessed a large amount of files of the company (many records), including information about customers, partners, orders, and new products.
- He transferred those files to several collaborators in various locations around the world to be sold to hackers to be used in identity theft and industrial espionage.

a) List the vulnerabilities that allowed the attackers to steal this information.
b) Indicate what security mechanisms would have stopped the attack. Relate your defenses to the corresponding vulnerabilities.

Vulnerabilities	Defenses
WEP encryption broken	Use WPA2[1]
Personal and Company data stolen	Store personal and company data in separate partitions on phone with different encryption[2] [3]
User Id and Passwords belonging to phone owner stolen	Encrypt user id and passwords with different key.[2]
Passwords and IDs for non phone owner stored on phone	Policy should be established prohibiting storage of other employee data on device.[2]
SQL Injection used to access data base	Multiple defenses possible[4] such as: • Use of Prepared SQL Statements on forms • Use of Stored Procedures • White List Input Validation

1 "What is WEP Wireless Encryption", Netgear, https://kb.netgear.com/1141/What-is-WEP-wireless-encryption
2 Kandia Johnson, "Three Ways to Separate Work from Personal on Your Mobile Device", http://www.blackenterprise.com/mobilizing-you-5-ways-separate-work-from-play/
3 Ian Paul, "Security To Go: Three Tips to Keep Your Mobile Data Safe", https://www.pcworld.com/article/2052810/security-to-go-three-tips-to-keep-your-mobile-data-safe.html
4 OWASP, "SQL Injection", https://www.owasp.org/index.php/SQL_Injection

Vulnerabilities	Defenses
	• Modifying All User Supplied Input to eliminate special characters not related to fields • DB Least Privilege
Customer partner order and product data stolen	• Data Base should be designed to provide minimum data access to users needed to perform job.[5] • Data Base should be in multiple locations depending on job function(s). • Database should be monitored to sound alarm when large amounts of data are transferred.[6]

5 Eduardo Fernández-Medina, Mario Piattini, Designing secure databases, In Information and Software Technology, Volume 47, Issue 7, 2005, Pages 463-477, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2004.09.013. (http://www.sciencedirect.com/science/article/pii/S0950584904001429)

6 Muller, Roy, “Top Database Security Threats and How To Mitigate Them”, https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx

Q2: Compare the security levels of the most popular browsers: Google Chrome, Mozilla Firefox Quantum, and Microsoft Edge. Use the same approach as in Assignment 3, a comparison table, relating each feature to the existence of a corresponding pattern

Feature	Google Chrome[7]	Mozilla Firefox Quantum[8]	Microsoft Edge[9]
Current Major Version	62	57	11
Tasks to Render Pages	Each web page renders content in separate app.	Configurable number of apps that render pages	Each page renders content in a separate app.
Web Extensions API	supported	Now supported	supported
Tracking Protection	Off by default, uses blacklist to determine malevolent sites.	Off by default, uses blacklist to determine malevolent sites	Off by default, uses IE11 safe sites white list
Privacy Mode (commonly called Porn Mode)[10]	Incognito Browsing: Processes run at lower priority, more restrictions	Privacy Browsing: Lower priority, tasks run faster.	In Private Browsing: Orginally urls visited may remain in cache[11] Note: Fixed 9-Feb-2016 (KB3135173)[12]

- Tasks to render pages: all three browsers use separate tasks to render pages, thus using standard system security to prevent a page from capturing or corrupting another page in the browser.
- Web Extensions API: API used to extend web browsers. Firefox now supports the WebExtensions API, similar to the chrome.* API's. Formerly Extensions to Firefox could access and modify core code, now only the API is supported.

7 Security Overview - The Chromium Project, https://www.chromium.org/chromium-os/chromiumos-design-docs/security-overview
8 Firefox Quantum – Security and Privacy improvements, https://www.helpnetsecurity.com/2017/11/15/firefox-quantum-security/
9 Microsoft Edge – Deployment Guide for IT Pros, https://docs.microsoft.com/en-us/microsoft-edge/deploy/
10 How to use your browser's 'porn mode', http://www.zdnet.com/article/how-do-you-use-your-browsers-porn-mode/
11 Windows 10 - Microsoft Edge Browser Forensics, http://bsmuir.kinja.com/windows-10-microsoft-edge-browser-forensics-1733533818 (from data published in 2015).
12 Microsoft Edge's InPrivate Mode No Longer Reords Your Browsing History, https://betanews.com/2016/02/10/microsoft-edges-inprivate-mode-no-longer-records-your-browsing-history/

- Tracking Protection: warns or does not load sites known to have code that will attempt to capture data on another page.

Website Security	**Google Chrome[13]**	**Firefox Quantum**	**Microsoft Edge[14]**
Secure Indicators (SSL, Certificate, HTTPS)	Indicators present [15]	Indicators Present[16]	Indicators Present
Malicious Site Detection	Present	Present	Present
Privacy Settings	Configurable	Configurable	Configurable
History Deletion	Single or all sites	Single or all sites	Single or all sites

13 Chrome: Privacy and Security In Chrome, https://www.gcflearnfree.org/chrome/privacy-and-security-in-chrome/1/
14 Edge: Privacy and Security in Edge, https://www.gcflearnfree.org/edge/privacy-and-security-in-edge/1/
15 Check if a site's connection is secure, https://support.google.com/chrome/answer/95617?hl=en
16 Unpdated Firefox Security Indicators, https://blog.mozilla.org/tanvi/2016/01/26/updated-firefox-security-indicators/