TCSS 483 Google Chrome Threat Model

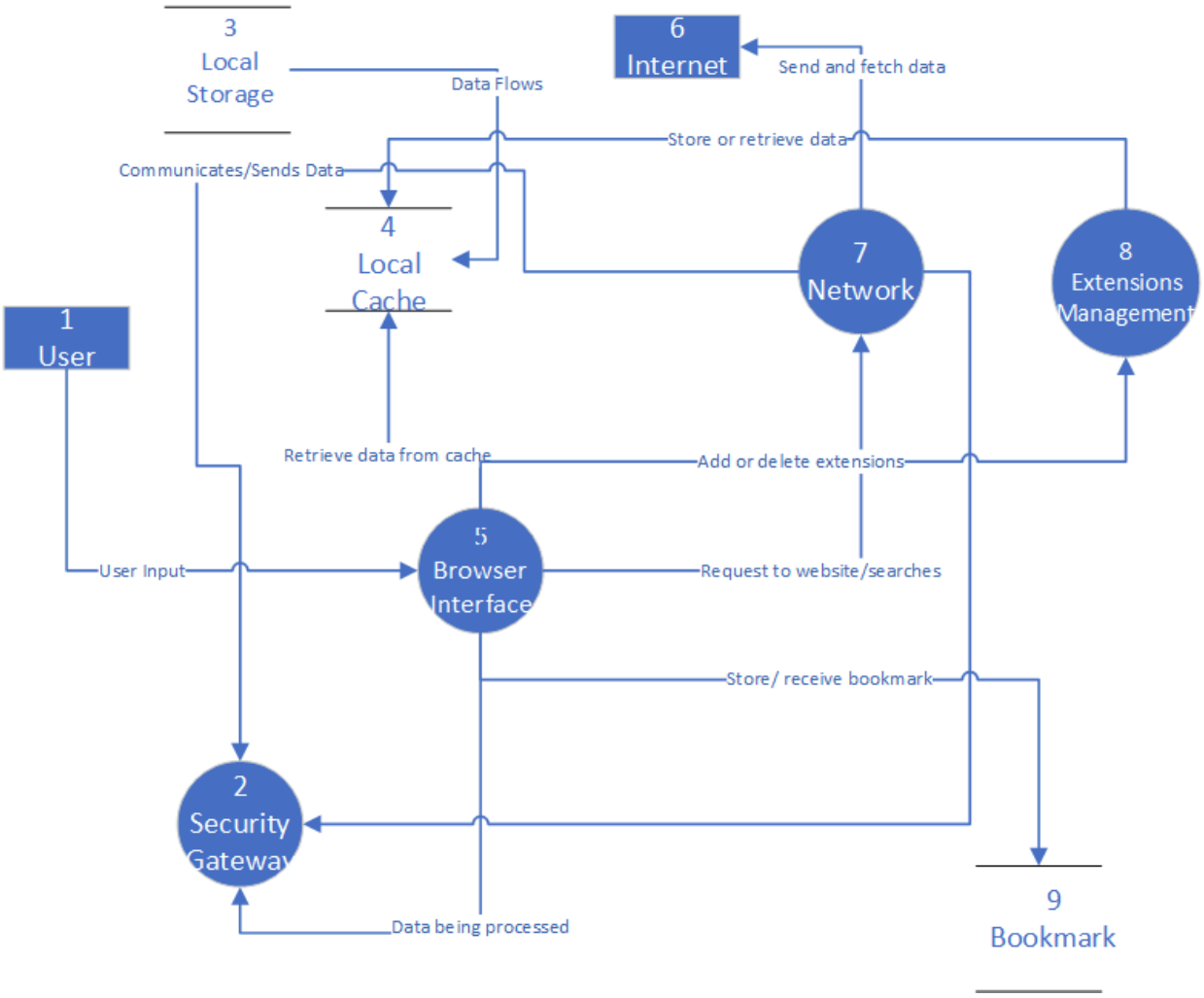
By Ahmed Mohamed

2/22/24

Description

Google Chrome is a widely-used web browser renowned for its speed, simplicity, and feature set. Developed by Google, Chrome offers users a streamlined and intuitive browsing experience with a clean interface. It supports essential features such as tabbed browsing, bookmarks, and synchronization across devices when signed in with a Google account. Its speed and efficiency is rated the highest of all search engines. The browser undergoes regular automatic updates, ensuring users benefit from the latest security enhancements and feature improvements. Its popularity stems from a combination of user-friendly design and Google's commitment to maintaining a secure and efficient browsing environment. Users can easily bookmark pages, categorize them with labels, and access their bookmarks through their Google account. Browser extensions, enhance the browsing experience by offering features and added functionalities. These extensions allow users to tailor their browsing to personal preferences. Also the local cache stores recently accessed web page elements on the user's device, improving page load times by retrieving content locally.

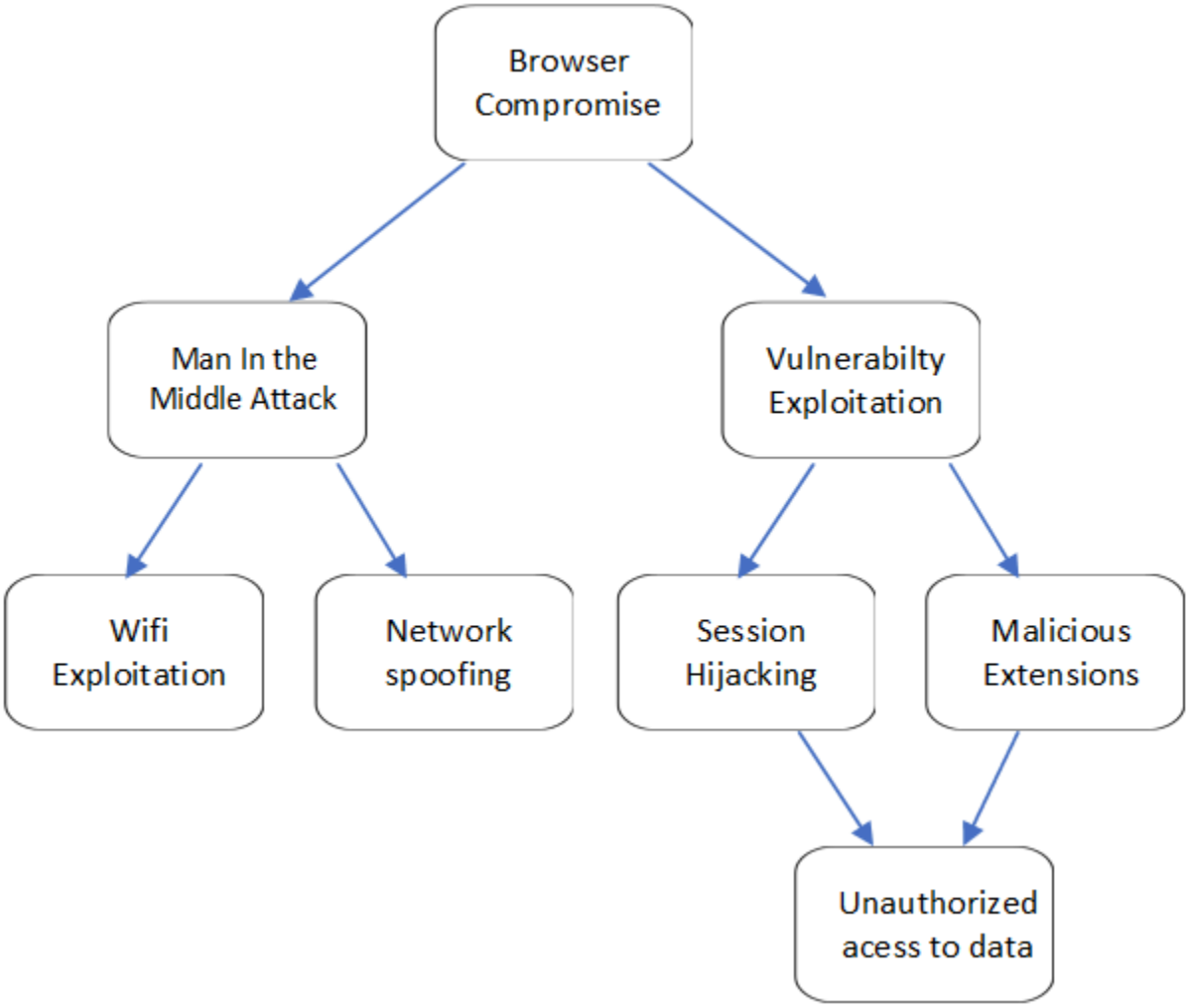
Data Flow Diagram:

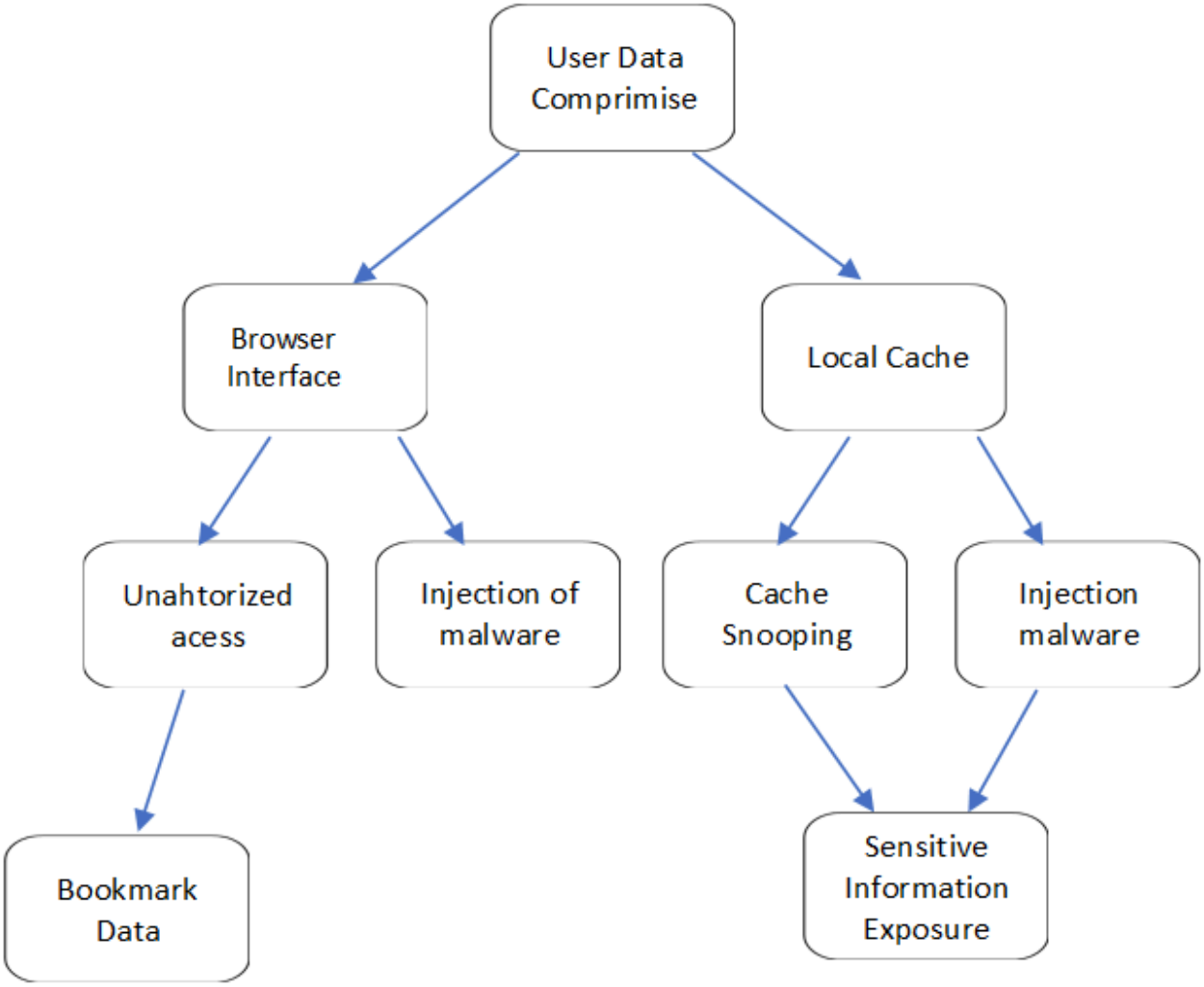


I used the data flow diagram in visio studio and it wouldn't let me use a double sided arrow so I couldn't show relationships that go both ways because of it. Also it wouldn't let me show the trusted boundaries so I am going to just state what they are.

Trust boundary 1: Browser Interface, local Cache, Local Storage, and Security Gateway.
Trust boundary 2: Network, Internet, Browser Extension
Trust boundary 3: User
Trust boundary 4: Extension

Threat Trees:




User Data Comprimise
Browser Interface
Local Cache
Unahtorized acess
Injection of malware
Cache Snooping
Injection malware
Bookmark Data
Sensitive Information Exposure

Breakdown of threats:

Threat	STRIDE Letters	Number in Diagram
1. Malicious extensions	S(Spoofing)	1. User (External), 5. Browser Interface (Process)
2. Network exploitation	S(Spoofing)	7. Network (Process)
3. Data tampering in cache	T (Tampering)	4. Local Cache (Data Store)
4. Modification of browser extensions	T (Tampering)	8. Extension Management (Process)
5. Data tampering in Storage	T (Tampering)	3. Local Cache (Data Store)
6. Leakage from local storage	I (Information Disclosure)	3. Local Storage (Data Store), 5. Browser Interface (Process)
7. Leak from local Cache	I (Information Disclosure)	4. Local Cache (Data Store), 5. Browser Interface (Process)
8. Network overload	D (Denial of Service)	7. Network (Process)
9. Browser exploitation	E (Elevation of Privilege)	5. Browser Interface (Process)

Ranking of threats:

Threat	D	R	E	A	D	Total	Rating
1	10	6	9	9	7	8.2	High
2	7	6	5	7	6	5.2	Med
3	6	7	7	6	6	6.4	Med
4	7	6	6	5	5	5.8	Med
5	7	7	7	6	7	6.8	Med
6	9	7	9	7	7	7.8	High
7	8	7	7	6	6	7.6	High
8	9	7	8	8	8	8	High
9	8	7	7	8	7	7.2	High