Whisper Leak: Side-Channel Attack on Language Models

Cybersecurity · Answer Key · 5 Questions

1. What type of attack is 'Whisper Leak'?

A) Denial-of-Service Attack
B) Side-Channel Attack
C) Phishing Attack
D) Brute-Force Attack

2. What is the potential impact of the Whisper Leak attack?

A) Data corruption
B) Exposure of language model conversation topics
C) System crash
D) Hardware damage

3. What encryption protocol does Whisper Leak bypass?

A) Secure Shell (SSH)
B) Transport Layer Security (TLS)
C) Internet Protocol Security (IPsec)
D) Wired Equivalent Privacy (WEP)

4. Who discovered the Whisper Leak attack?

A) Google
B) Microsoft
C) Amazon
D) Apple

5. What is Microsoft doing to address the Whisper Leak vulnerability?

A) Ignoring the problem
B) Working with vendors to mitigate the risk
C) Publicly disclosing user data
D) Demanding money from users