Secure Computing Cwk1

Question 1)

One way would be through spoofing. A user could accidentally download a fake version of the App that has malicious software inside it. The app however produces the same MD5 hash as the legitimate software as a result, when the AppCheck goes to assess the downloaded executable, it will not flag it as the hash exists in its database.

Another way the attacker may attempt to prevent AppCheck from issuing a warning for the malware is Tampering. By exploiting a weakness in how the software updates, a Man-in-the-Middle attack involves the attacker getting access to the AppCheck Database. Once access has been achieved the attacker can Tamper with the database, modify its contents and include the hash code of the illegitimate software disguising it from AppCheck and allowing it to run uninterrupted.

Alternatively, an attacker carries out an attack categorised as an Elevation of privileges. If the attacker gained higher privileges to the user's system, then they could interfere and alter the AppCheck software to stop it producing the notification altogether. It could even alter the database in which it stores the legitimate hashes, placing the hash code of the malicious software inside of it. As a result, preventing AppCheck from recognising it as illegitimate software.

Question 2)

A security policy states precisely what goals a protection mechanism is supposed to achieve. In this example one of the main threats are caused by unauthorised access to the Hash database. The security policy should therefore be to encrypt the database so that if an attacker was able to gain access through a man in the middle attack, they would not be able to write the hashes within it without the appropriate level of permissions. With the hash code of the legitimate software now protected, the system is at a much lower risk of a tampering attack.

A security model to implement this policy would be the Biba model. The Biba integrity model preserves integrity, restricting any ability to write "up" negating an attacker's ability to write hash codes into the database to inhibit AppCheck from recognising the illegitimate software. This would therefore protect the system from attacks to its database through unauthorised access.