XJCO3911 Secure Computing

Coursework 1

This is a very short threat modelling exercise, worth 15% of your overall grade. It shouldn't take you more than a couple of hours to complete.

Scenario

A popular software application is distributed to its users via a website. A particular user downloads this application to run on their PC.

The user's PC is running a security tool named AppCheck, designed to detect the presence of suspicious executable files on the system. AppCheck works by computing the MD5 hash of each downloaded executable file that it finds on the system, comparing that hash with a database of known hashes for popular software applications. If a computed hash does not match the value found in the database, AppCheck will display a warning to the user.

This database of known hashes is maintained and regularly updated by the developers of AppCheck. An up-to-date copy of the database is downloaded automatically by AppCheck, once a day.

The Task

Consider the threat that the user in the scenario above might download malware pretending to be the popular software application, and that AppCheck will fail to issue a warning about this.

Construct an attack tree to investigate this threat. Your tree should use the correct syntax as shown in the Threat Modelling lecture and should feature at least 3 valid and distinctly different attack approaches.

When constructing your tree, remember that attack trees describe the conditions needed for a threat to be realised, decomposing those conditions to successively finer levels of detail as we progress down the tree. They are *not* flowcharts describing steps in a process! Decomposition of threat conditions should be sufficient to make it reasonably clear what an attacker has to do to make the attack work. Two or three levels of decomposition should be enough in most cases.

After constructing the tree, identify the attack path that you consider would be most likely to succeed, and provide some justification for your choice. Then explain briefly how this attack path could be mitigated.

Deliverables

Use a drawing tool (e.g., `https://app.diagrams.net`) to create the attack tree; alternatively, sketch it neatly by hand and scan or photograph your sketch. Scans/photos should be clear and easy to read.

This diagram plus your discussion should be provided as a PDF document, *not* the original Word document or other editable format. This document should be no more than two A4 pages in length.

There are **12 marks** available for the attack tree and **10 marks** for the accompanying discussion.

In marking the tree, we will take into account the overall clarity of the diagram, the variety of attack paths you've considered, whether you've decomposed the threat properly and sufficiently, and whether you've recognised any AND constraints that exist between branches.

Submission

Use Minisign to sign the PDF file with your digital signature—see Exercise 9 if you need a reminder of how to create a detached signature file. **2 marks** will be awarded for a submission that meets the requirements above *and* has a valid and verifiable signature.

Create a Zip archive containing both the PDF file *and* the signature. Submit this via the link provided in the 'Submit My Work' section in Minerva. The deadline for submission is **8 AM on 24 October**.