FIT 3173 Software Security
Week 3 Tutorial Sheet on Threat Modelling

The goal of this tutorial is to practice and think about the threat modelling process discussed in the lectures.

1) The following table lists some of the common threats you will come across when developing software applications. In the tutorial class, for each threat, your task is to identify the type of threat according to the STRIDE classification, potential mitigation technique(s), and issues related to the threat and/or its mitigation.

THREAT	THREAT TYPE	MITIGATION TECHNIQUE(S)	DESCRIPTION OF ISSUES
Access to or modification of confidential HTTP data	Tampering		
Access to or modification of confidential RPC or DCOM data	Information Disclosure		
A device that contains confidential data might be lost	Information Disclosure		
Flood service with too many connections	Denial of Service		
Attacker attempts to guess passwords	Tampering		
Read confidential cookie data	Information Disclosure		
Tamper with cookie data	Tampering		
Access private, secret data	Elevation of Privilege		
Attacker spoofs a server	Spoofing		
Attacker posts HTML or script to your site	Tampering		

Attacker opens thousands of connections but does nothing with them	Denial of Service		
Unauthenticated connection can consume memory	Denial of Service		
Your data packets can replayed			
Attacker attaches debugger to your process			
Attacker gains physical access to hardware	Elevation of Privilege		
Attacker shuts down your process			
Attacker modifies configuration data			
Error message leaks too much information and helps an attacker learn what to do next	Information Disclosure		
In a shared work-station environment, an attacker accesses or uses data cached by a previous user	Spoofing		
A malicious user accesses or tampers with lookup data on the web server	Elevation of Privilege		

Denial of Service
Denial of Service

2) In the lecture, we introduced the following frequent flyer update operation of an airline as an example software security scenario. Frequent flyer points of valid customers are updated by a separate program. As soon as the plane lands at the destination, it triggers a program (say copy program) which copies (transmits) the frequent flyer information of the passengers in that flight into another area. An update program takes this data and updates the frequent points of the passengers. There was a breach detected where an individual who had access to the system which updates the frequent flyer info was able to rack up millions of miles without even flying!

Draw a DFD for this sub-system and how it interacts with other parts of the system, identify the threat(s) and describe mitigation strategies.