		Security Concerns and their Solution: an Overview							
		Goal	Anti-Goal	Security Problem	Specific example	Security pattern (from implementation side)	Security pattern (from our side)	Solution	Solution location
T	1	Tamper proof data	Gain ability to tamper with data	unauthorized actors tampering with local data	users accessing local data on their phone, changing their score	Encryption pattern	Encryption pattern	Provided by the android phone itself --> it encrypts stored data	Physical storage
T	2			unauthorized actors tampering with cloud data	hostile accessing the cloud server to change the goal location to current location	Encryption pattern	Using third party sever.	Handled by amazon: their security measures are quite extensive	Software architecture
T/S/I(depends on attack)	3	confidentiality	Gain access to confidential information	unauthorized actors listening to the transmissions to and from the server	man in the middle attack	Transmission pattern	Secure transmission security pattern (not sure about exact name)	API automatically uses SSL and can be set to use a VPN	Software implementation
I	4			information disclosure	hostile user releases a list of goal locations	Encryption pattern, Authentication and (architectural solutions: firewall, server layout and configuration)?	Using third party server	similar to tamper proof data --> same solution	Software architecture
E	5			elevation of privilege	a user pretends to be an administrator which gives him unlimited access to all game data	Authentication pattern, (limitaion of access), transmission pattern	Using third party server	Player can only get access to the database through software, which is limited by premission levels of third party server	Software architecture
S	6	non-repudiation	Gain ability to work anonymously	identity spoofing	user changes their identity and has several games running at once	Authentication pattern	Using third party authentication sevice.	Handled by API: allows users to log in using their google account	Software implementation
R	7			Repudiation	user able to change data anonymously making it impossible to trace	Authentication pattern	Using third party authentication sevice.	similar to identity spoofing --> same solution	Software implementation
D	8	Availiability	Bring down the servers	denial of service	server gets flooded by non legitimate messages meaning packets by legitimate users get dropped	firewall, patterns for Ddos	Using third party server	unlikely to be an issue: this game is very small scale. However, the usage of Amazon servers means that some measure of protection is in place against a DoS	Software architecture
	9	Reliability of third-party services	Exploit usage of third party services	unsecure integration of third party services	third party authentication service is not integrated properly thus resulting in a decrease in security by making elevation of privilege easier to achieve		probably exists but an API is a kind of BlackBox --> hard to confirm	already handled: that is what an API is for	Software Implementation