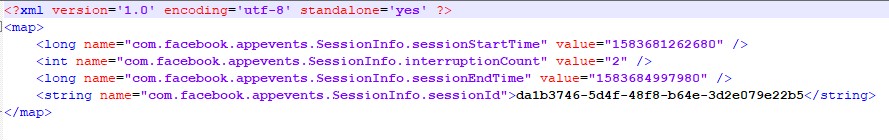
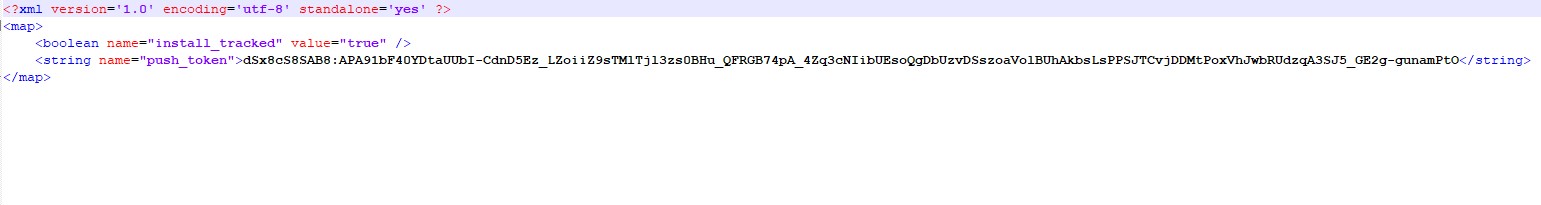
1. For additional authentication this app has an option to link your account to one of your social networks accounts, which is actually mandatory. When trying to authenticate, client cannot intervene in any way possible since it’s always using SDK’s provided by Twitter, Facebook or Yostar to authenticate. There is only 1 server for the game on the global cluster (there is separation between JP/CN and other world), so it’s enforced on this server’s endpoints.
2. Let’s look at TwitterSession for example:



All the data comes from Twitter server (probably). For the point of how complex is session identificators and secrets:





4

Seems pretty safe – long, probably uuid8 type ids, not really guessable, tokens are probably encrypted strings.

The only problem that this things were stored in backup data, so I guess they are stored somewhere in the permament memory for some time.

Each time user purchases something in store for currency, that you mainly only can get through real money, his session is checked again.

1. I’ve found usage of hmac-sha1 signatures, but have not found any jwt token mentions in code, which leads me to believe, that it’s stateless authentication is not used in this app or I’m blind.