TURUN YLIOPISTO
Informaatioteknologian laitos

VANAMO, LAURI: Pelaajan tunnistaminen hiiri- ja näppäimistödynamiikan avulla

Pro gradu -tutkielma, 55 s.
Tietojenkäsittelytiede
Toukokuu 2016

Usein tietokonepeleissä on tarpeen erottaa tai tunnistaan tunnettu pelaaja (esimerkiksi pelitilin omistaja) jostakin toisesta pelaajasta. Toinen pelaaja saattaa olla esimerkiksi hakkeri, kultafarmari, tai jopa jokin kolmas taho jolle pelitilin alkuperäinen omistaja on tilinsä myynyt. Tämän tyyppinen tunnistaminen (autentikointi) voidaan tehdä pelaajan biometriikkaan perustuen käyttämällä luokitteluun koneoppimisalgoritmeja. Epäilyksen herättyä pelaajan hiiri- ja näppäimistödynamiikkaan perustuva biometrinen data kerätään ja luokitellaan vertaamalla sitä pelitilin omistajan tunnettuun biometriseen dataan. Jos hiiren ja näppäimistön käytössä on merkittäviä eroja, voidaan tilanteessa epäillä epärehellisyyttä ja aloittaa tarkempi selvitys aiheesta.

Pelaajan näkökulmasta tämänkaltainen datan kerääminen ja analyysi on huomaamatonta ja huoletonta. Se ei häiritse pelikokemusta, eikä se ole myöskään uhka pelaajan yksityisyydelle tai tietoturvalle. Datan keräys voidaan tehdä taustalla pelaajan huomaamatta, ja ainoastaan hiiren ja näppäimistön käyttö pelin sisällä voidaan tallentaa; tästä pitää huolen käyttöjärjestelmän tietoturvakäytännöt. On hyvä myös huomata, että tietokonepeli käyttää tätä samaa dataa joka tapauksessa pelin ohjaamiseen, joten datalle ehdotetaan nyt vain uutta käyttötarkoitusta. Pelaaja hyötyy tästä lisääntyneen tietoturvan muodossa, jolloin pelitili on paremmin turvassa luvattomalta käytöltä.

Gradussa hiiri- ja näppäimistödynamiikkadata kerättiin kahdelta pelaajalta, joilla on hieman eritasoinen kokemus tietokonepeleistä (kokenut pelaaja, vähemmän kokenut pelaaja). Näin kerätty raakadata muokattiin sitten lopulliseksi datajoukoksi ja analysoitiin. Luokittelu tapahtui k:n lähimmän naapurin koneoppimismenetelmällä käyttäen jätä-yksi-pois riistiinvalidointia.

Avainsanat: tietokonepelit, jatkuva biometrinen tunnistaminen, hiiri- ja näppäimistödynamiikka, k:n lähimmän naapurin menetelmä, luokittelu

UNIVERSITY OF TURKU
Department of Information Technology

VANAMO, LAURI: Player Authentication Based on Mouse and Keyboard Dynamics

Master's Thesis, 55 p.
Computer Science
May 2016

Often in online games it is necessary to be able to recognize or authenticate a known player (for example owner of the game account) from some other player. The other player might be, for example, hacker, gold farmer, or even some third party to whom the original owner has sold her account. This kind of authentication can be done by biometric means, using machine learning algorithms for classification. Suspected user's biometric data, that is, data collected from user's mouse and keyboard usage, can be classified towards known data. If mouse and keyboard usage patterns of the game account owner and the suspected user differ enough, foul play can be suspected, and more thorough investigation by other means can be started

From player's point of view this kind of data collection and analysis is inconspicuous and non-intrusive. It does not disrupt the gaming experience nor is threat to player's privacy or information security. The data collection can be done in background without user noticing, and only the mouse and keyboard usage inside game can be collected because of restrictions enforced by the operating system. It is also noticeable, that any game that uses mouse and keyboard, uses the input data anyway, so now only one more usage for that data is proposed. Player also gets an extra layer of game account security in form of continuous biometric authentication.

In master's thesis, mouse and keyboard data is collected from two players, that are in a slightly different skill level (experienced gamer, less experienced gamer). Granular raw data was then transformed into a dataset, prepared, and analyzed. Classification was carried out with k-Nearest Neighbor classification with leave-one-out cross-validation.

Keywords: computer games, continuous biometric authentication, mouse and keyboard dynamics, k-nearest neighbor classification