Developing Malicious Behavior in World of Warcraft

Akshay Patil
Stony Brook University

Julia Liu
Intelligent Systems Lab

Hossam Sharara
University of Maryland, College Park

Oliver Brdiczka
Computing Science Lab

World of Warcraft
Massively Multi-player Online Role-Playing Game (MMORPG) where players create different characters in a virtual world

Factions
• A group of allies formed on racial and ideological basis
• Opposite factions are at war against each other (Alliance vs. Horde)

Races
Each character in WoW has a race that determine its faction and abilities

Guilds
• An in-game association of characters of similar faction
• Facilitate interactions and organization for large battles
• Often used as social platform among players

Data: A complete census of three servers from WoW during a six-month period from 11/22/2010 till 05/29/2011

Problem Description
Characterizing and detecting anomalous user behavioral patterns in online environments for predicting future malicious activities

Characterizing Anomalous Behavior
Real World Analogies
• Factions: Hostile countries / countries at war
• Guilds: Competing companies/organizations

Target Anomalous Behaviors
• Espionage (Faction-level): Faction A → Faction B → Faction A
• Sabotage (Guild-level): Guild A → Guild B, Guild A falling apart

Faction Espionage
• Characters are allowed to change factions for a fee
• An average 0.8% of characters change faction at least once across the three servers during the observation period
• Feature can be exploited by malicious users for spying on characters from opposite factions, especially in PvP settings

Target Anomalous Behavior: (Faction A > B > A)
If associated with additional reward ⇒ Malicious

“Lossy” Guilds
Guilds losing more than 50% of their members over time

Identifying Malicious Characters
Leadership Identification among sub-groups leaving a guild in a short time frame, and causing it to be lossy

Raid Network
Raids: organized battles that are performed by a group of players (more than 5 and up to 40 characters) to attack fortified dungeons and strong bosses in the game

Future Directions
• Utilize information from raid networks and battle interactions to leverage the process of predicting guild sabotage.
• Identify precursors for target malicious behavior from the identified characters
• Build a predictive model that combine both activity traces and social network interactions for identifying anomalous characters and predicting future malicious actions
• Build psychological profiles for malicious characters

Identifying Malicious Behavior in World of Warcraft

World of Warcraft
Massively Multi-player Online Role-Playing Game (MMORPG) where players create different characters in a virtual world

Factions
• A group of allies formed on racial and ideological basis
• Opposite factions are at war against each other (Alliance vs. Horde)

Races
Each character in WoW has a race that determine its faction and abilities

Guilds
• An in-game association of characters of similar faction
• Facilitate interactions and organization for large battles
• Often used as social platform among players

Data: A complete census of three servers from WoW during a six-month period from 11/22/2010 till 05/29/2011

Problem Description
Characterizing and detecting anomalous user behavioral patterns in online environments for predicting future malicious activities

Characterizing Anomalous Behavior
Real World Analogies
• Factions: Hostile countries / countries at war
• Guilds: Competing companies/organizations

Target Anomalous Behaviors
• Espionage (Faction-level): Faction A → Faction B → Faction A
• Sabotage (Guild-level): Guild A → Guild B, Guild A falling apart

Faction Espionage
• Characters are allowed to change factions for a fee
• An average 0.8% of characters change faction at least once across the three servers during the observation period
• Feature can be exploited by malicious users for spying on characters from opposite factions, especially in PvP settings

Target Anomalous Behavior: (Faction A > B > A)
If associated with additional reward ⇒ Malicious

“Lossy” Guilds
Guilds losing more than 50% of their members over time

Identifying Malicious Characters
Leadership Identification among sub-groups leaving a guild in a short time frame, and causing it to be lossy

Raid Network
Raids: organized battles that are performed by a group of players (more than 5 and up to 40 characters) to attack fortified dungeons and strong bosses in the game

Future Directions
• Utilize information from raid networks and battle interactions to leverage the process of predicting guild sabotage.
• Identify precursors for target malicious behavior from the identified characters
• Build a predictive model that combine both activity traces and social network interactions for identifying anomalous characters and predicting future malicious actions
• Build psychological profiles for malicious characters