

StarForce FrontLine for MMOG

StarForce solution to protect MMO games.

*«StarForce» company
is a recognized expert in the field of protection
of games, educational, entertaining
and business software*

TABLE OF CONTENTS

Introduction.....	3
Threat categories	3
Invasive threats:	3
Non-invasive threats:	4
StarForce FrontLine for MMOG.....	6
Capabilities and features.....	7
Protection integration	9
Protected files types.....	10
System requirements for StarForce Products	10
CONTACTS:.....	11

StarForce presents: Protection of Massive Multiplayer Online Games (MMOG)

It is no secret that MMOG is becoming a priority for PC games industry today. Unprecedented success of World of Warcraft urges the developers and publishers all over the world to pay more attention to this genre. New MMOG releases are announced quite often, which promises reasonable profit to their copyright holders. However, the issue has its drawbacks that reduce customers' interest in this genre and can reduce profit as well:

- Bots
- Cheating tools
- Server/client hacking
- Farming
- Pirated servers

With the above-mentioned in hand, dishonest users can make significant modifications in game balance, which leads to reduction of subscribers' interest in the game and reduction of profit of the copyright holders.

Keeping up with the times, StarForce has developed a special solution to prevent cheaters and hacker from attacking MMOG. The solution includes such elements as protection of game servers against reverse engineering, modifications and running the servers on unauthorized sites, protection of the game code against reverse engineering and cracking, protection against running and executing cheat programs and bots, protection of traffic between an MMOG server and a client.

Threat categories

For convenience, all the threats can be divided into two categories¹:

- Invasive
- Non-invasive

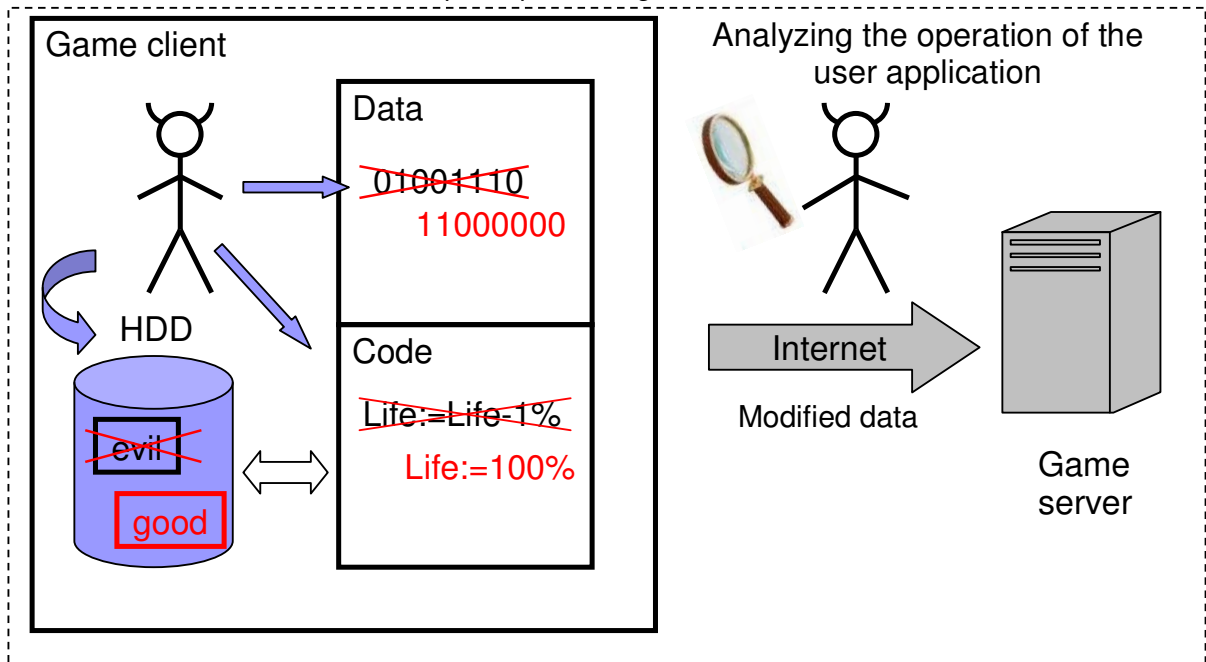
Invasive threats:

Invasive threats are associated with the game client modification. They include:

- Code modification
- Modification of files
- Data modification

¹ StarForce terminology

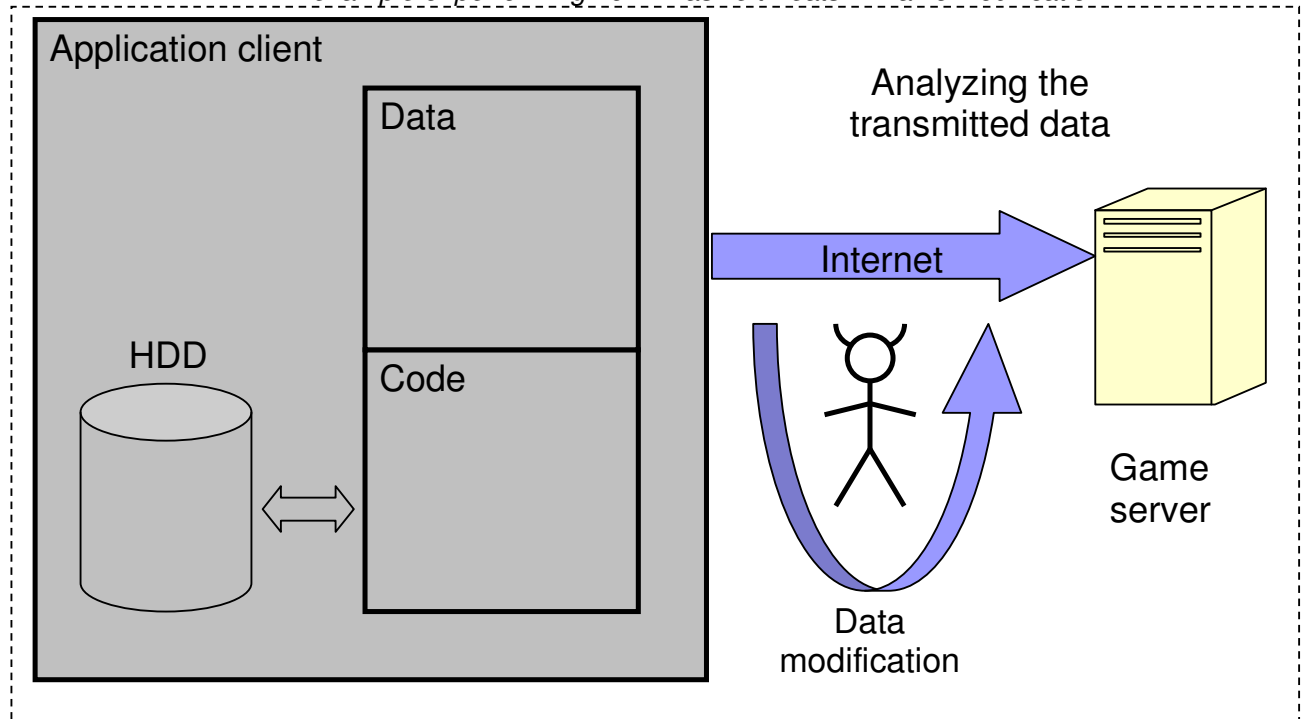
An example of performing an invasive threat



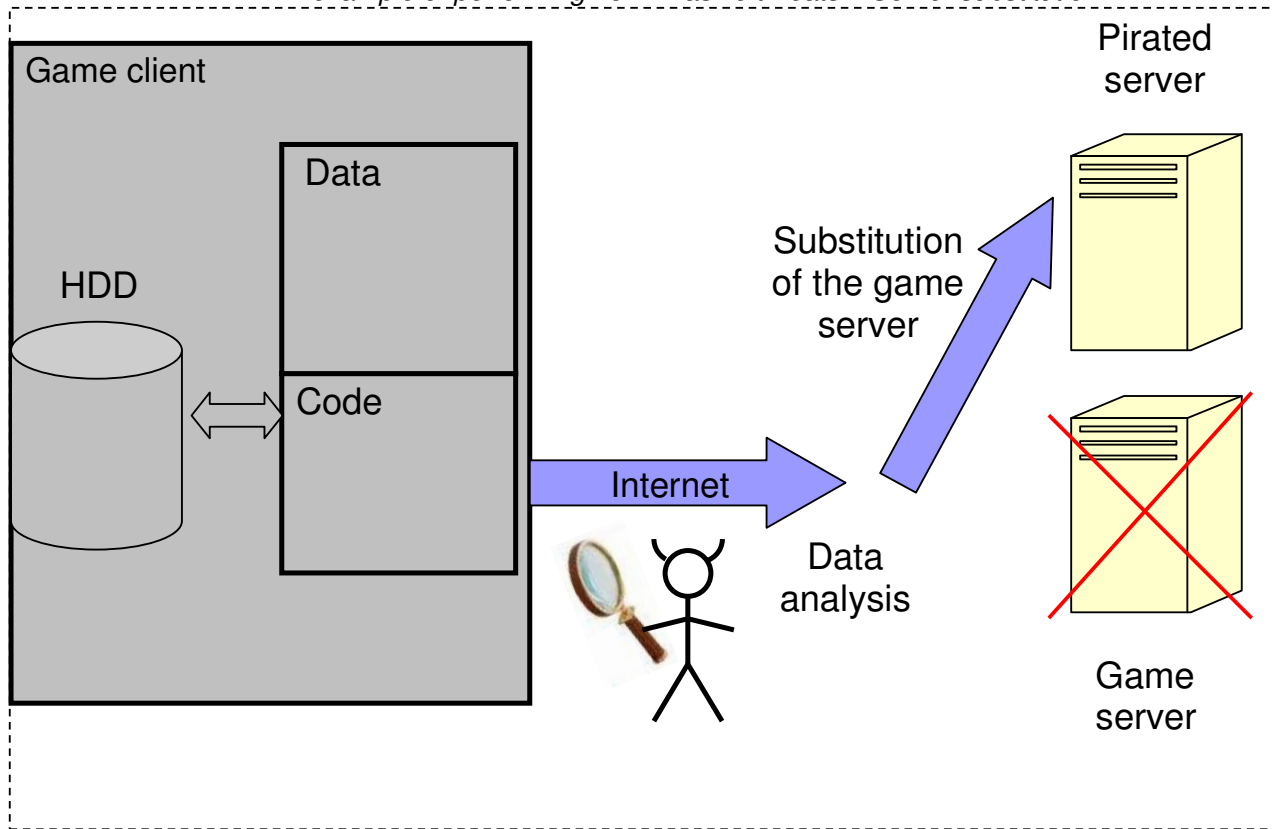
Non-invasive threats:

- Non-invasive threats are not associated with the modification of the game client directly. They include:
- Traffic modification
 - Server substitution (pirated servers)

An example of performing non-invasive threats – Traffic modification



An example of performing non-invasive threats – Server substitution



On the basis of the threats analysis, StarForce experts along with the MMOG market leaders have developed the requirements for MMO games protection, which resulted in a brand-new company's product. The product meets the following main requirements:

- It makes non-invasive and invasive attacks difficult to perform
- It does not have a strong effect on the game operation
- It provides simple protection implementation

Besides, there is a number of differences between MMO games and ordinary computer games, which StarForce took into account during the product development, and which influences the protection solution:

- MMOG protection counteracts reverse engineering and modification of the application source code
- MMOG protection counteracts traffic analysis and modifications
- MMOG protection does not require binding to any object (optical media or computer)
- MMOG requires no activation.

StarForce FrontLine for MMOG comprises:

- **Integrity control**
MMOG files and data integrity control, ability to receive updates from the server.
- **Launch control**
Executable modules must be launched only by authorized processes.
- **MMOG code protection against analysis and modification**
Game code obfuscation for considerable complication of its analysis. Using of control sums to protect against modification.
- **MMOG data protection against analysis and modification**
Game variables encryption using StarForce SDK.
- **RAM protection**
Protection against direct memory access, protection against new memory thread creation etc².
- **Traffic control**
Securing traffic modification impossibility between server and client.
- **Server authenticity check**
Protection against server substitution via constant authentication between server and client.

Together we preserve the integrity and uniqueness of your virtual universe and make your game interesting and fascinating for everybody!

² Using Safe'n'Sec® behaviour analyser technology from S.N.Safe&Software® company.

Capabilities and features of the StarForce FrontLine solution for MMOG

- **RAM Protection against direct access, new thread creation and more**
 Using the Safe'n'Sec® behavior analyzer technology game developer received a wide range of flexible and useful tools for deep RAM protection against multiple threats: Write process memory protection, Remote process thread manipulation (Suspend, Stop, Create), Kill process protection.
 Safe'n'Sec® SDK usage is required.
- **Checking the integrity of executable files of the protected game during game start**
 Such check is designed for additional protection of the protected game modules against modification. To do so, digital signature of the protection is added to a module. The protection system checks this signature in its loader during module loading. The check is performed automatically when the game runs. Besides, the protection operates if executable modules of the game are infected.
- **Checking the integrity of executable files during the operation of the protected game**
 Checking the integrity of read-only code and data in memory. This method is designed to check a protected executable file during game operation. The integrity of the read-only elements of the protected file is checked, i.e. game variables are not checked. To do so, the protected game calls the corresponding SF API function. This operation greatly complicates the modification of the protected file during game operation.
- **Possibility to protect certain variables of the game against unauthorized access/modification**
 To protect variables, 'secure classes' from the SF API (SF Uint) are used instead of the built-in classes (Uint). This operation greatly complicates the modification of the game variables during game operation.
- **Providing the integrity of the application data files**
 Checking the integrity of read-only files (the protected game checks digital signatures of the data files). The check is performed via StarForce API.
 This operation complicates analysis and modification of the data files of the protected game.
- **Protection of the application data that can be modified**

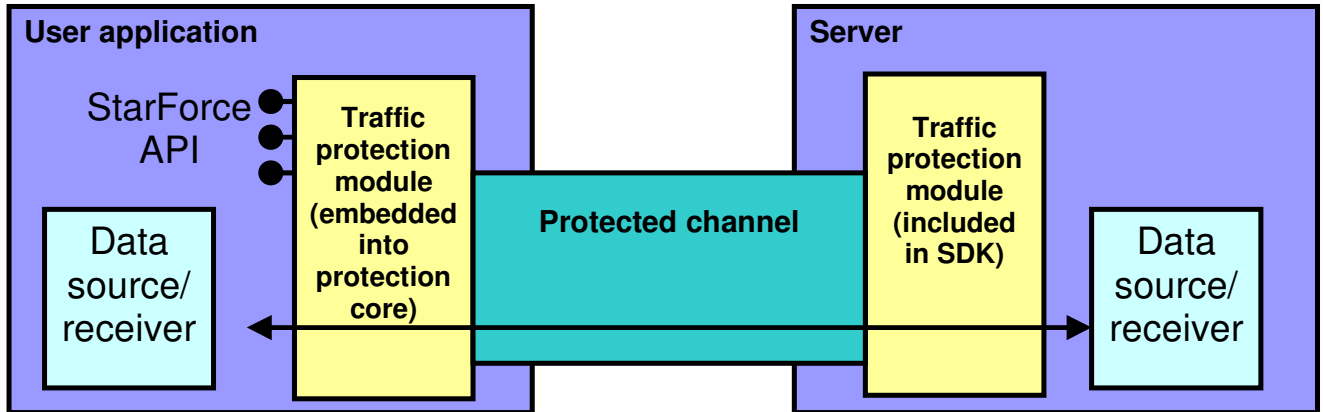
 - Protection is implemented via the variables encryption
 - 32-bit integer variables are supported
 - C++ and C# are supported
 - SDK is required

This operation complicates the analysis and modification of the application data in memory.
- **Checking the parent process**
 This method allows running the protected game from the authorized processes only. If a process (a file of malicious software) is in the black list, an error is displayed. Such files are checked according to signatures. The black list can be supplemented with time.

- **Protection of traffic between client and server**

This method consists in encrypting traffic between game client and server and greatly complicates traffic modification or substitution. The main point of the protection is that the communication channel between client and server is cryptographically protected.

Installation of an additional StarForce Java-module on the game server is required.



- **Server authenticity check**

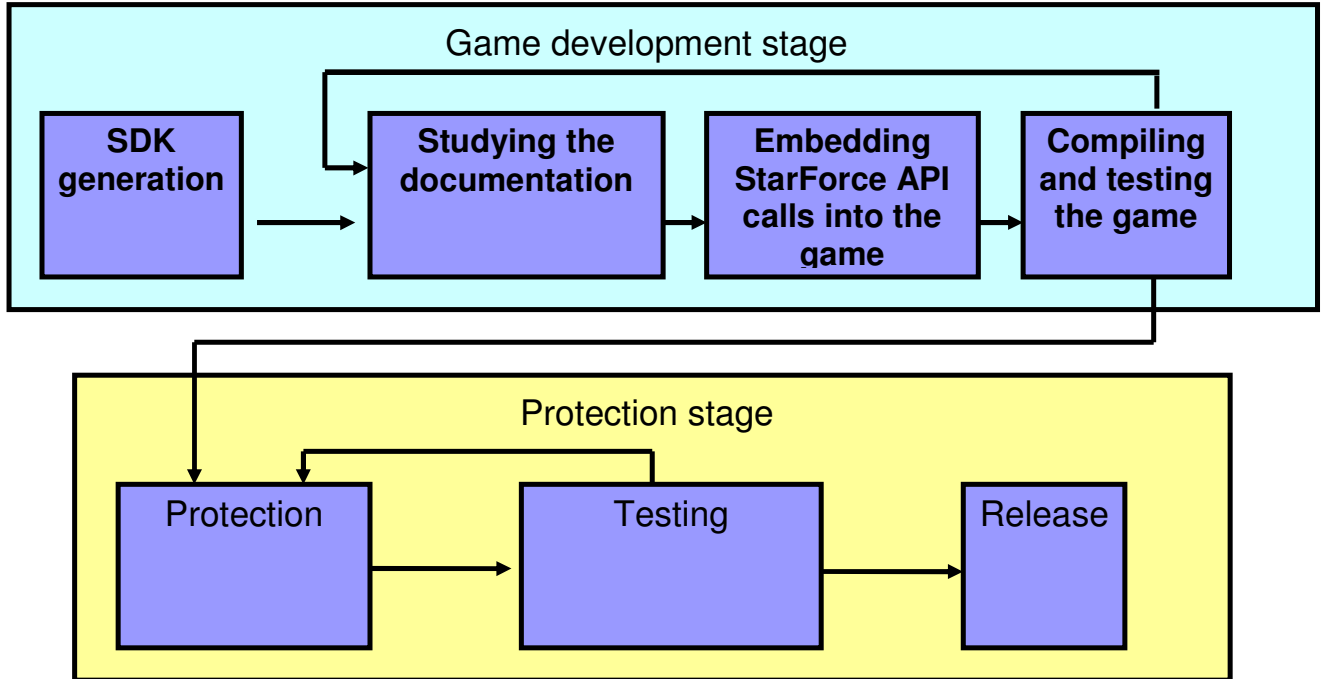
Protection against server substitution via constant authentication between server and client.

- **Protection system does not use driver**

All the methods are implemented without the use of the protection driver, which provides maximum compatibility of the solution.

Protection integration

Protection integration should be started during the application development. The scheme of the integration is as follows.



Protected files types

- x86/x64 executable files
- .Net executable files

*Protection does not cover executable files which have preliminary been packed or ciphered.

System requirements for StarForce Products

For the protection:

- Intel Pentium x86/x64 or 100% compatible processor
- Microsoft Windows 2000 SP4, Windows XP 32 (SP2)/64, Windows Vista 32/64
- Internet connection

For protected program:

- Intel Pentium or another 100% compatible processor
- Microsoft Windows 2000, Windows XP 32/64, Windows 2003 Server, Windows Vista 32/64.
- CD-ROM, DVD-ROM, CD-RW, DVD-RW (in case of distributing and binding protected application to optical disc)
- Internet connection

CONTACTS:

- **StarForce Moscow - Headquarters**
Altufevskoe shosse, 5/2
127106 Moscow, Russia
Tel: +7 (495) 9671451
Fax: +7 (495) 9671452
E-mail: sales@star-force.com
www.star-force.com

- **StarForce America**
San Ramon, CA.
Tel: +1-925-272-4515
Email: sales@star-force.com
Http: www.star-force.com

- **StarForce Asia Pasific**
StarForce Technologies, Ltd. (Asia-Pacific Office)
SI-1802, Guanhuoguoji Building No.105 Yao Jia Yuan Road,
Chaoyang Dist., Beijing China
Zip: 100025
Tel.: 86-10-59623093 59623052 82856017
Fax: 86-10-59623052
www.star-force.com.cn

- **StarForce France**
20, rue Malar
F-75007 PARIS
Tel : +33 (0)1.44.18.37.05
Fax: +33 (0)9.56.72.07.47
Email: olivier.duran@star-force.com
www.fr.star-force.com