Online game security

Sakai HK Kim
(hk.kim@hksecurity.net)
• Agenda

1. Online game security
2. Users’ PC security
3. Prevention Pirates Server
4. Special issues - game BOT
5. Academic approaches – selected papers
I. Online game security ??
0. what is the online game security?

- This term has many meanings
  - Information security for online game publisher and studios’ information assets (servers, network, DB and applications)
  - Security process or systems for online game users
  - Security process or systems for online game client and server programs

- To care about users’ PC security is going important

- Technology for protecting game client and server program is critical to online game publisher and studios
  - For detection/prevention BOT programs
  - For detection/prevention private (pirate) servers

- We’ll talk about one by one.
1. hacking phases against online game publisher

#1. direct hacking to IDC which runs live game service

- Hacking count is highly increased when the game is supposed to launch foreign country.
- The hacking is purposed to gain server programs for building their own private servers
- Or for blackmail (sometimes they use DDoS attacks)
- Or the hacking is purposed to change database record for creating online game items or cyber money *for real money*.

#2. hacking to game publisher’s office (virus, attack the office internal network)

- If they fail to penetrate into IDC directly, they change tactics.
- Attackers try to penetrate into office internal network for taking routes to the IDC
- Or for seizing source code and other property
- Sometimes they use well-crafted malicious code via e-mails for targeting internal users

#3. hacking to the famous web sites and spreading malicious codes

- For stealing gamers' id and passwords

#4. Sometimes attackers try to abuse personal information (e.g. SSN)

- for creating game accounts

- Glance a look at the Massive attack from China until 2003
• **2. for the Online game publisher, studio’s security itself**

• Be careful for internal intruders and internal leak.
  – Hackers have various strategy and tactics for getting their own goal.

• **Physical security must be considered when planning service for the foreign country**
  – Physical theft is real threat.

• Protect everything you can – auditing web and game source codes, applying all patches, building IPS and firewalls, enforcing access controls and everything
  – Everything can be exposed.
  – Everything can be analyzed.
  – Trust no one.

• **Establish Global security operation system.**
  – Most online games can be published to the foreign countries. (who knows? Your game can be published globally someday)
  – Legal review and cooperation system are highly required.
Physical security? Really?
3. for the Online game publisher, studio’s security itself

- If you don’t trust foreign people, then do it everything by your own person
- Study the foreign laws,
  - esp. intellectual propriety and telecommunication and cyber crime related laws.
  - Unfortunately, some countries do not have any adequate laws.
- Anti DDoS system must be deployed.
  - It’s not cheap, but it’s not expensive also.
- Choose global vendor’s security solution for resolving tech. support issues.
- DDoS with blackmail, attacking web sites, manipulating game packets for exploiting internal game bugs ... it’s just daily life.
- *The entire battle front line is very long. Hire more security experts.*
4. If you fail...

- **You’ll be mess.**
  - You will watch lots of private servers and BOTs around everywhere with your own eyes.
  - Some hacker will blackmail you.

- **In the extreme case, your company can go bankrupt because of lack of security**
  - Exposing customers private information (remember Korean a****** case, L****** company case) is extremely critical.

- **Your service cannot maintain service availability.**
  - Prepare anti-DDOS system
  - Establish fully coupled corporation relationship with IDC
  - Maintain hotline with KISA.

- **You’ll be fired. Or can be prosecuted.**
  - Rarely, but if you missed very important things, that can be happen.
II. Users’ PC security
• Online game publisher should consider customers’ security
  – It’s for you. It will save call center’s costs and men powers.
  – Also, it will give you competitive power and customer satisfaction.

• For users’ PC security, what can we do?
  - Protect your customer from the malicious codes for the purpose of stealing your user’s id and password.
    - On demand antivirus programs, anti key logging software and so forth.
  - Protect your possible customer from abusing personal information.
  - Support Windows patches for free. (A lot of users don’t have legitimate OS licenses. They give up doing windows updates because of the MS’s genuine validation policy)
    - 3rd party’s patch management software or KISA’s patch management software would be helpful.
  - Provide your customers many additional secondary authentication method.
    - Mobile OTP, Token type OTP, outbound call for secure login, security challenge numbers, login notification systems via SMS and etc.
1. Is it needed? Yes, absolutely

According to Ahnlab’s ASEC annual report 2008

<table>
<thead>
<tr>
<th>순위</th>
<th>악성코드 명</th>
<th>검수</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Win-Trojan/Xema, variant</td>
<td>1448</td>
</tr>
<tr>
<td>2</td>
<td>Win32/Virut</td>
<td>351</td>
</tr>
<tr>
<td>3</td>
<td>Win32/IRCBot,worm, variant</td>
<td>341</td>
</tr>
<tr>
<td>4</td>
<td>Dropper/QQPass,23599,B</td>
<td>298</td>
</tr>
<tr>
<td>5</td>
<td>Dropper/QQPass,23599,D</td>
<td>293</td>
</tr>
<tr>
<td>6</td>
<td>Dropper/OnlineGameHack,23087</td>
<td>272</td>
</tr>
<tr>
<td>7</td>
<td>Win-Trojan/KorGameHack,17920,BR</td>
<td>272</td>
</tr>
<tr>
<td>8</td>
<td>Win-Trojan/KorGameHack,26624,Al</td>
<td>267</td>
</tr>
<tr>
<td>9</td>
<td>Win-Trojan/KorGameHack,14848,FO</td>
<td>195</td>
</tr>
<tr>
<td>10</td>
<td>Win-Trojan/KorGameHack,6430</td>
<td>149</td>
</tr>
<tr>
<td>11</td>
<td>Win-Trojan/Downloader,38400,I</td>
<td>141</td>
</tr>
<tr>
<td>12</td>
<td>Dropper/OnlineGameHack,15988</td>
<td>130</td>
</tr>
<tr>
<td>13</td>
<td>Win-Trojan/OnlineGameHack,15360,I</td>
<td>120</td>
</tr>
<tr>
<td>14</td>
<td>Win-Trojan/Downloader,169984,D</td>
<td>116</td>
</tr>
<tr>
<td>15</td>
<td>Win-Trojan/KorGameHack,19456,BM</td>
<td>113</td>
</tr>
<tr>
<td>16</td>
<td>Win-Trojan/KorGameHack,7295</td>
<td>102</td>
</tr>
<tr>
<td>17</td>
<td>Win-Trojan/KorGameHack,43072</td>
<td>96</td>
</tr>
<tr>
<td>18</td>
<td>Dropper/OnlineGameHack,29743</td>
<td>95</td>
</tr>
<tr>
<td>19</td>
<td>Win-Trojan/KorGameHack,12800,EL</td>
<td>88</td>
</tr>
<tr>
<td>20</td>
<td>Win-Trojan/KorGameHack,15064</td>
<td>88</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>순위</th>
<th>악성코드 명</th>
<th>검수</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dropper/OnlineGameHack,20100</td>
<td>310</td>
</tr>
<tr>
<td>2</td>
<td>Win-Trojan/Downloader,16364,FS</td>
<td>267</td>
</tr>
<tr>
<td>3</td>
<td>Win-Trojan/Agent,60416,Z</td>
<td>221</td>
</tr>
<tr>
<td>4</td>
<td>Win-Trojan/Noupdate,36864</td>
<td>199</td>
</tr>
<tr>
<td>5</td>
<td>Dropper/OnlineGameHack,17143</td>
<td>183</td>
</tr>
<tr>
<td>6</td>
<td>Dropper/OnlineGameHack,17412</td>
<td>179</td>
</tr>
<tr>
<td>7</td>
<td>Dropper/OnlineGameHack,17799</td>
<td>178</td>
</tr>
<tr>
<td>8</td>
<td>Win-Trojan/KorGameHack,16121,D</td>
<td>169</td>
</tr>
<tr>
<td>9</td>
<td>Win-Trojan/OnlineGameHack,19208</td>
<td>159</td>
</tr>
<tr>
<td>10</td>
<td>Win32/IRCBot,worm, variant</td>
<td>153</td>
</tr>
<tr>
<td>11</td>
<td>Win-Trojan/OnlineGameHack,18768,B</td>
<td>150</td>
</tr>
<tr>
<td>12</td>
<td>Dropper/OnlineGameHack,17632</td>
<td>148</td>
</tr>
<tr>
<td>13</td>
<td>Win-Trojan/OnlineGameHack,19938</td>
<td>132</td>
</tr>
<tr>
<td>14</td>
<td>Dropper/OnlineGameHack,16767</td>
<td>129</td>
</tr>
<tr>
<td>15</td>
<td>Win-Trojan/KorGameHack,16972</td>
<td>113</td>
</tr>
<tr>
<td>16</td>
<td>Win-Trojan/OnlineGameHack,34304,P</td>
<td>104</td>
</tr>
<tr>
<td>17</td>
<td>Win-Trojan/Downloader,27136,BH</td>
<td>103</td>
</tr>
<tr>
<td>18</td>
<td>Dropper/OnlineGameHack,16531</td>
<td>103</td>
</tr>
<tr>
<td>19</td>
<td>Win-Trojan/KorGameHack,19589</td>
<td>97</td>
</tr>
<tr>
<td>20</td>
<td>Win-Trojan/Hidd,43008</td>
<td>94</td>
</tr>
</tbody>
</table>
2. So what’s the ideal methods for customers’ security

- **Technical way**
  - OS patch, antivirus, anti-key logger is just *baseline*. We need more.
  - secondary logon and audit system
    - 2 factor authentication for password verification should be provided. (mobile OTP is the powerful solution)
    - Outbound call for authentication

- **Strategic way**
  - Strategic alliance with government’s security agency will be the good solution
    - Use Sinkhole routing
    - We’ve implemented this routine to our major logon control and game client
  - Alliance with antivirus software company will be a good chance also.
3. Illustration for additional secondary authentication

1. Input id and password
2. Sending id and password
3. Outbound call
   - Announce Challenge randomly generated numbers
4. Challenge-response
   - Input the requested number
5. Validation result (true, false)

Diagram:

- Game auth server
- Outbound call (CTI machine)
- Gamers’ phone
- ARS
- PSTN
- CDMA
- Internet
- Game server
4. Illustration for sinkhole routing (ref. KISA)

- We’ve implemented this routine to our major logon control and game client program.
  - Game client program detects and alerts.
  - Redirect to the webpage for downloading free antivirus programs.
5. Illustration for PC subscription system

- Security System for restricting game login only from the pre-subscribed PCs from the web sites.
  - Generating specific unique information from the clients PC.
  - Users’ PC can easily hacked, easily infected with malicious codes.
  - Event though some hackers know about users’ id and password, if the hardware does not valid, then login will not be succeeded.
• 6. Illustration for customers security enforcing campaign

• Protecting users’ security costs much money, but don’t stop encouraging users.
7. Illustration for mobile OTP

NC OTP 서비스란? (이전 OTP, 이하 NC OTP로 읽어 통일)

NCSOFT Game OneTime Password의 작가로 개발 모디파이.
기본적으로 입력하면 일정과 비밀번호에 추가적으로 본인의 해독문에 다루므로 받은
NC OTP 코드가에서 매번 새로운 NC OTP 비밀번호를 발급한다고 하여 입력하고
로그인 되는 로직으로 보완서비스입니다.

기존 로그인 방법
통합 개정 (or 개입 개정)
비밀번호

NC OTP 로그인 방법
통합 개정 (or 개입 개정)
비밀번호 + NC OTP 비밀번호

다음로드 화면 통합 개정 리나즈/리나즈
개입 개정의 다 개정을 모두 응용 가능!
8. Why did hackers target on innocent users?

- **It is for gaining money**
  - Stealing online game users’ id, password ➔ stealing users’ game items and cyber money ➔ it can be traded to real money (RMT)

- **It also increases web sites attack massively.**
  - hacking to vulnerable and famous web sites. (online game web magazine, shopping mall, portal sites…)
  - Inject malicious codes for famous web sites.
  - Many PCs can be easily infected with malicious codes without installing MS security patches or antivirus software.

- **Attackers’ IP address, game workshops IP address, BOT makers IP address are highly correlated.**

- **If you enforce your company’s servers’ security then the attackers change the strategy to hack your customers’ PCs. If you care about your customers’ PCs’ security then they will change the target to your own servers.**
III. Prevention Pirates server
• Private server = Pirates server
• Insert hidden detection routine for detecting and preventing private servers.
  – Not all private servers are built with genuine one. Some reverse engineers make a server code via packet analysis.
  – Detecting genuine one will be the key.
• Clients program should be connected to the official servers only.
  – Encrypt configuration file.
  – Use client security products (e.g. Xbundler) for including resource file easily and safely.
• Server program should be run only for restricted conditions.
  – Under Restricted hardware information
  – Under restricted domain or IP addresses range
  – EFS encryption is useful only for physical theft.
1. For prevention and detection private servers

- **You should detect servers version**
  - Can you verify the remote servers are your own servers or not?
  - Create your hidden protocol for version checking.
    - The answer should return build number, distribution version, country information, system information, and so forth.

- **Insert your own signature onto binary file.**
- **Preparing legal reaction if the servers are genuine one.**
IV. Special Issue – Game BOT
0. BOT, the endless battlefields

1. Game BOT
   - Highly well crafted AI program
   - State of the art reverse engineered program

2. Game BOT taxonomy
   - By physical types - Software type, USB type, Mouse type
   - By running types
     - OOG BOT (out of game client BOT; a.k.a non game client BOT)
     - IG BOT (in game client BOT)
   ✓ Generally speaking, OOG BOT can be easily detected and protected relatively

3. Game BOT is not free. Monthly charge is expensive than game fee.
   - BOT program are now merging with service line. BOT provider supports remote installation, they are running call center for customer satisfaction, they hire travelling salesperson.
   - BOT makers are global company also.
• 0. BOT, the endless battlefields

• **To use a metaphor, It’s already cold game.**
  – We’re fighting with many malicious BOT programs. It’s outnumbered situation.
  – Always game programmers will lose if there is no innovational way.

• **We’re losing power.**
  – We don’t have enough resource to develop BOT-proofed games. It’s impossible.
  – Even small ~ mid sized online game publishing companies can not tell anything.
1. Some defense method will lead false-positive of antivirus programs.

2. We’re consuming with QA, antivirus’ false alarm – the more security, the more false alarm
2. Why BOT program is evil?

1. General theory
   - Destruction of in-game balance.
   - Increase non-BOT users’ claim
   - Increase game development cost for prevention BOT module.
   - Increase game development cost because game BOT consume in-game contents very speedily
   - Increase monitoring costs – hire more game master personnel, increase a lot of costs regarding customer satisfaction.
   - When BOT fails to update game protocol, that program repeatedly sends old protocol packets → it’s kind of DDoS, theoretically.

2. [이데일리] 환치기·명의도용...게임산업 좀먹는 `오토`

3. The truth?
   - It’s for money.
3. BOT, as of today...the features are..

1. Automated game play
2. Emulate game packets perfectly
3. Evasion for CAPTCHA authentication
4. Chatting response for evading GM’s monitoring
5. OCR recognition – hardware level operation. Cannot be detected.

Don’t be evil
4. Why commercial online game security fails?

- Already losing game. It’s running on Windows OS.
  - New approach is needed.
  - Sell 3rd party’s game security solution’s source code full license to game publisher and developer, we really need static compile.
  - One binary build including game security module’s source code is necessary
  - Dll loading and process can be avoided with many techniques.
  - One binary compile with code obfuscation and code virtualization will be a good solution

- Korea’s GameGuard and Hackshield are weaker than another game security solution?
  - Absolutely not. It’s just better known to BOT makers rather than other game security solutions for a long time enough to be analyzed.
4. Why commercial online game security fails?

- **New approach is needed.**
  - Without packing Game Client, without code virtualization (code obfuscation), just leaning on only commercial game security solution will give you endless pain. Today’s your job will be always updating signature, and it just costs network traffic fee.
  - But it’s not useless. Frequent update of patterns and authentication protocol will be a good method.
    - But…. Still we need QA process. We’re commercial online game service provider. We have a lot of things to lose but BOT makers do not.

- **New fast enough and secure enough encryption algorithm is needed.**
  - Communication with game client and server should be fully encrypted. And the key should be generated automatically and updated repeatedly several times in a day. (usually 3 hours are enough to be analyzed.)
  - 5,000~7,000 of concurrent sessions are processed in the one game server. How dare can apply strong encryption algorithm?
5. How can we stop the game BOT?

**BOT treatment method – 4 ways**

- **1. Technical way**
  - Third party solutions for memory protection, process protection, file protection and packet encryption.
  - Server logic check

- **2. Legal way**
  - BOT distributor, BOT maker

- **3. Operational way**
  - Monitoring and user banning, it can make conflict with users.
  - User volunteered restriction – self sanitizing eco-system.

- **Design way**
  - Make BOT meaningless and useless - Quest-based game and Highly Action-based game
6. BOT treatment methods – technical way

1. Technical way
   - Applying game security solution (e.g. GameGuard) for process protection, memory protection, file protection, packet encryption and additional authentication.
   - Applying the Binary packer (Winlicense/Themida, NPGE packer, yoda’s protector)
   - Server <-> client protocol packet shaping
   - Game client/server’s self verification
     - Checking resource files and information
   - Code obfuscation – code virtualizer

2. Limitation
   - There are no silver bullet – how can we handle all of OS kernel level debugging, process hooking, dll injection.
   - Users PC’s restriction – security safeguard needs more resources, conflict with antivirus or virtual device drivers.
• Then how the online game studios build the detection module?
  – Relying on company’s own method, usually it’s a top secret.
  – Relying on in-game monitoring and reaction

• Don’t skip to implement logic check on server side. It’s the last hope.
  1. In-game shop – point check, validation check
  2. FPS – magic bullet, magic wall, speed hack check
  3. Rhythm action game – investigating high scorer with ordinal points
  4. Racing game – speed hack, magic wall

• Include your own detection routine in the client program. And obfuscate it. ➜ game client itself cannot be avoided.
6. BOT treatment methods – technical way

- Don’t consider commercial online security product as perfect protection tool, just consider it as back data gathering tool for ban cheating users.

- Check every time repeatedly
  - check PID, PPID continuously
  - Protect game clients’ process and memory
  - Hash value checking

- Considering CAPTCHA?
  - CAPTCHA is not a always good solution
  - Massive human being can support this request
  - Sometimes humans can fail
• 7. BOT treatment methods – design

• Protecting BOT with in-game design. That’s the best way for stopping endless wars.
  – In-game CAPTCHA
  – Turing test with in-game QUIZ
  – Validating users with NPC.
  – Give penalty for users who does field hunting for a long time in a same zone.
    • Re-spawn NPC more stronger one.
  – Make cyber money and item useful in the cyber world, useless in the real world.
  – Many heuristics can be possible.
정정당당 오토 클린업!

지금보다 몇번 더 편리한 환경에서 게임을 즐길 수 있게 해주세요.
오토프로그램 제거, 배포 사이트 근절에 동참해주세요.

✅ 오토프로그램이 원요?
온라인 게임에서 사용되는 불법 프로그램으로, 정상적인 환경 없이 게임에 관여하여 게임의 속도를 줄이거나, 에러나 소요 시간 등의 불편을 줄여 하는 프로그램입니다. 이러한 피해는 많은 사용자에게 큰 손해를 끼치므로, 정상적인 게임 환경을 유지하기 위해 사용을 단속시켜야 합니다.

✅ 오토프로그램을 사용하지 않아야 하는 이유?
오토프로그램은 불법적인 입력을 해달게 하기 때문에 정상적인 환경에 비해 더욱 많은 성능을 낼 수 있도록 해주는 프로그램입니다. 게임의 품질과 성능의 저하를 방해할 뿐 아니라, 이를 사용할 경우가, 악성코드 및 바이러스에 노출될 가능성이 높습니다.

배포사이트 근절이 가장 중요합니다.
오토프로그램의 배포는 영리한 웹사이트와 각자의 위치에 위치한 업체의 이용을 통해 이루어집니다. 그러므로 높은 수준의 이용자들을 대상으로 조절하고 있습니다. 따라서 모든 불법적 중계자와 팔자의 행위를 억제하기 위해서 오토프로그램은 반드시 차단되어야 합니다.

이런 사이트 신고해주세요!
신고 대상: 오토프로그램 및 기타 유사프로그램 개발, 배포 사이트
신고 기간: 3월 3일 ~ 4월 30일
신고 방법: 신고용이란 오토프로그램 소개와 사이트명, 하고 싶은 말 등을 기재하여, 여러분을 보내주세요.

메일로 신고해주세요.
V. Academic approaches
- selected paper
Good papers

- **Can We Prevent Collusion in Multiplayer Online Games?**
  - Jouni Smed et al.

- **Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games**

- **Using Group Interaction of Players to Prevent In-game Cheat in Network Games**
  - Shaolong Li et al., E-Commerce, 2007. ISDPE 2007

- **Detecting and Controlling Cheating in Online Poker**
  - Roman V. Yampolskiy, 5th IEEE Consumer Communications and Networking Conference, 2008
- **Cheat Detection for MMORPG on P2P Environments**
  - Takato Izaiku et al., *Proceedings of 5th ACM SIGCOMM workshop on Network and system support for games*, 2006
- **Identifying MMORPG Bots: A Traffic Analysis Approach**
  - Kuan-Ta Chen et al.

### Table: Traffic Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Player</th>
<th>ID</th>
<th>Network*</th>
<th>Period</th>
<th># Conn</th>
<th>Pkt</th>
<th>Bytes</th>
<th>Pkt Rate‡</th>
<th>Avg RTT</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Player</td>
<td>Gino</td>
<td>A1</td>
<td>HiNet, 2M/512Kbps</td>
<td>1.8 hr</td>
<td>12</td>
<td>51,823</td>
<td>3.5 MB</td>
<td>0.9 / 3.9 pkt/s</td>
<td>82.0 ms</td>
<td>0.03%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A2</td>
<td>5.6 hr</td>
<td>14</td>
<td>147,814</td>
<td>10.5 MB</td>
<td>0.8 / 3.4 pkt/s</td>
<td>95.4 ms</td>
<td>0.03%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kiya</td>
<td>B1</td>
<td>0.4 hr</td>
<td>45</td>
<td>15,228</td>
<td>1.0 MB</td>
<td>1.2 / 4.5 pkt/s</td>
<td>81.6 ms</td>
<td>0.01%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B2</td>
<td>2.3 hr</td>
<td>108</td>
<td>59,247</td>
<td>3.8 MB</td>
<td>1.1 / 3.3 pkt/s</td>
<td>108.8 ms</td>
<td>0.12%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B3</td>
<td>2.1 hr</td>
<td>189</td>
<td>47,721</td>
<td>3.2 MB</td>
<td>0.9 / 2.8 pkt/s</td>
<td>125.5 ms</td>
<td>0.23%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B4</td>
<td>5.0 hr</td>
<td>326</td>
<td>129,177</td>
<td>8.4 MB</td>
<td>1.1 / 3.3 pkt/s</td>
<td>109.8 ms</td>
<td>0.09%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kuan-Ta</td>
<td>C1</td>
<td>0.8 hr</td>
<td>2</td>
<td>9,681</td>
<td>0.6 MB</td>
<td>0.8 / 1.4 pkt/s</td>
<td>191.8 ms</td>
<td>1.73%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jhih-Wei</td>
<td>D1</td>
<td>TANET</td>
<td>2.4 hr</td>
<td>28</td>
<td>48,617</td>
<td>3.2 MB</td>
<td>0.8 / 2.6 pkt/s</td>
<td>45.1 ms</td>
<td>0.01%</td>
</tr>
<tr>
<td>Bot</td>
<td>Kore</td>
<td>K1</td>
<td>TANET</td>
<td>13.4 hr</td>
<td>104</td>
<td>245,709</td>
<td>13.6 MB</td>
<td>0.7 / 2.3 pkt/s</td>
<td>33.0 ms</td>
<td>0.01%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>K2</td>
<td>26.5 hr</td>
<td>306</td>
<td>479,374</td>
<td>30.4 MB</td>
<td>1.0 / 2.1 pkt/s</td>
<td>45.6 ms</td>
<td>0.04%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>K3</td>
<td>32.7 hr</td>
<td>37</td>
<td>271,416</td>
<td>13.3 MB</td>
<td>0.6 / 0.7 pkt/s</td>
<td>96.5 ms</td>
<td>0.004%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>K4</td>
<td>ETWEBS-TW</td>
<td>13.0 hr</td>
<td>38</td>
<td>225,528</td>
<td>11.5 MB</td>
<td>0.9 / 2.0 pkt/s</td>
<td>65.7 ms</td>
<td>0.01%</td>
</tr>
<tr>
<td></td>
<td>DreamRO</td>
<td>R1</td>
<td>TANET</td>
<td>3.0 hr</td>
<td>7</td>
<td>46,381</td>
<td>2.6 MB</td>
<td>0.9 / 1.7 pkt/s</td>
<td>83.4 ms</td>
<td>0.03%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R2</td>
<td>4.8 hr</td>
<td>21</td>
<td>77,675</td>
<td>4.4 MB</td>
<td>0.9 / 1.9 pkt/s</td>
<td>65.2 ms</td>
<td>0.02%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R3</td>
<td>42.3 hr</td>
<td>42</td>
<td>652,877</td>
<td>34.1 MB</td>
<td>0.8 / 1.8 pkt/s</td>
<td>85.3 ms</td>
<td>0.05%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R4</td>
<td>ETWEBS-TW</td>
<td>11.2 hr</td>
<td>77</td>
<td>320,680</td>
<td>25.1 MB</td>
<td>1.7 / 3.5 pkt/s</td>
<td>85.2 ms</td>
<td>0.05%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R5</td>
<td>23.1 hr</td>
<td>176</td>
<td>672,325</td>
<td>53.3 MB</td>
<td>1.7 / 3.6 pkt/s</td>
<td>79.4 ms</td>
<td>0.16%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R6</td>
<td>10.5 hr</td>
<td>36</td>
<td>209,347</td>
<td>13.1 MB</td>
<td>1.0 / 2.4 pkt/s</td>
<td>87.7 ms</td>
<td>0.05%</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>2 B / 4 P</td>
<td>19</td>
<td>206.6 hr</td>
<td>1,599</td>
<td>3,821,509</td>
<td>241.6 MB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: *The table values are for illustrative purposes and may not reflect actual data.*
• Good papers (cont’)

• Detecting Cheaters for Multiplayer Games: Theory, Design and Implementation
  – S.F. Yeung et al.

Fig. 1. The DBN used for aimbot behavior detection.
Identifying MMORPG Bots: A Traffic Analysis Approach
[Chen, Jiang, Huang, Chu, Lei & Chen]

• **Backgrounds**

  - **General aspects of MMORPG**
    - Training characters, Obtaining better equipment, completing various quests → characters become stronger and better equipped
  
  - **Ragnarok**
    - One of most popular MMORPG game in the world
      - Well-defined comic style graphics
      - Encourages players to involved with other characters and the community
  
  - **Traffic analysis**
    - First study to analyze traffic to identify the use of BOT
  
  - **BOT-controlled characters can only be identified manually**
Mainstream BOTs for Ragnarok

- Kore and its derivatives (http://sourceforce.net/projects/kore/)
- DreamRO and its derivatives (http://www.ayxz.com/soft/1805.htm)
- Both Kore and DreaRO are standalone bots (they don’t need game client)

Analyze the traffic traces caused by bots and humans → find discrepancy between them

- Analyze BOT’s traffic vs. human novice’s game traffic vs. human expert’s game traffic
• **Results**

  - **Traffic of humans and that of bots are distinguishable**
    - Regularity in the release time of client command
      - DreamRO shows very quick response than human and Kore BOT
      - DreamRO, Kore BOT both show the discrete response time for server’s command.
      - DIP Test (unimodality test)
    - Trend and magnitude of traffic burstness
      - BOT always generate seamless and homogeneous traffic, generates even burst.
      - Human shows random burst situation (when human recognize monster or emergency event) – dramatically increasing mouse click and keyboard hit.
      - Fisher’s test (periodicity test)
Results

- Sensitivity to network conditions
  - When experiencing network lag, human rarely controls keyboard and mouse because human reacts visual changes on the monitor. So traffic generation is decreased.
  - BOT buffers command reaction and send queued packets, so traffic generation is increased with some time lag.