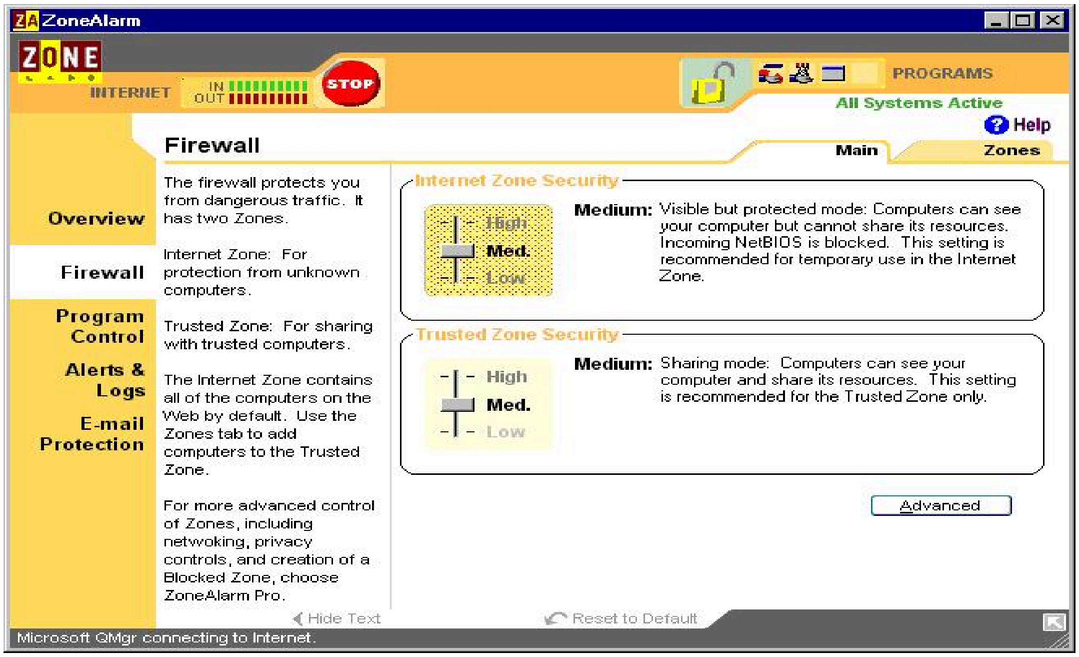
TCP's Evolution: From Secure Networks to Gaming Exploits in Halo 2

Authored by Michael Mendy

1. Introduction

The rapid advancement of network technology has brought forth a myriad of tools designed for security, analysis, and network management. This paper provides an in-depth examination of several key network tools and concepts—ZoneAlarm Pro (ZAP), Cain and Abel, CommView, DDoS attacks, and Router Standbying—while also exploring their unintended use in online gaming exploits, particularly on Xbox Live and in *Halo 2*. We delve into the technical aspects of these tools, their legitimate uses, and how they were misappropriated for cheating, with a special focus on the "Bridging Host" technique.

2. ZoneAlarm Pro (ZAP): The Rise of Personal Firewalls



Firewall

The firewall protects you from dangerous traffic. It has two Zones.

Internet Zone: For protection from unknown computers.

Trusted Zone: For sharing with trusted computers.

The Internet Zone contains all of the computers on the Web by default. Use the Zones tab to add computers to the Trusted Zone.

For more advanced control of Zones, including netwoking, privacy controls, and creation of a Blocked Zone, choose ZoneAlarm Pro.

Internet Zone Security

Medium: Visible but protected mode: Computers can see your computer but cannot share its resources. Incoming NetBIOS is blocked. This setting is recommended for temporary use in the Internet Zone.

Trusted Zone Security

Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone only.

Microsoft QMgr connecting to Internet.

Exhibit: ZoneAlarm Pro (ZAP) in 2005, in particular at the Firewall screen.

2.1 Core Features of ZoneAlarm Pro

- **Inbound/Outbound Traffic Monitoring:** ZoneAlarm enabled users to monitor both incoming and outgoing traffic, helping to protect against unauthorized access.
- **Application-Level Internet Access Control:** Users could control which applications had internet access, providing a layer of security against malware.
- **Real-Time Alert System for Connection Attempts:** This feature alerted users whenever an unknown connection is attempted, allowing for prompt action.
- **Stealth Mode to Evade Port Scans:** ZoneAlarm could hide open ports from potential attackers, reducing the risk of discovery.
- **Email Attachment Scanning:** Later versions introduced the scanning of email attachments to prevent malicious files from causing harm.

2.2 Historical Context

ZoneAlarm filled a critical gap before built-in OS firewalls became standard. It educated users about the importance of personal network security and helped shape the expectations for future security software. By offering a user-friendly interface, ZoneAlarm made firewall protection accessible to the average consumer, which was a significant advancement in personal cybersecurity.

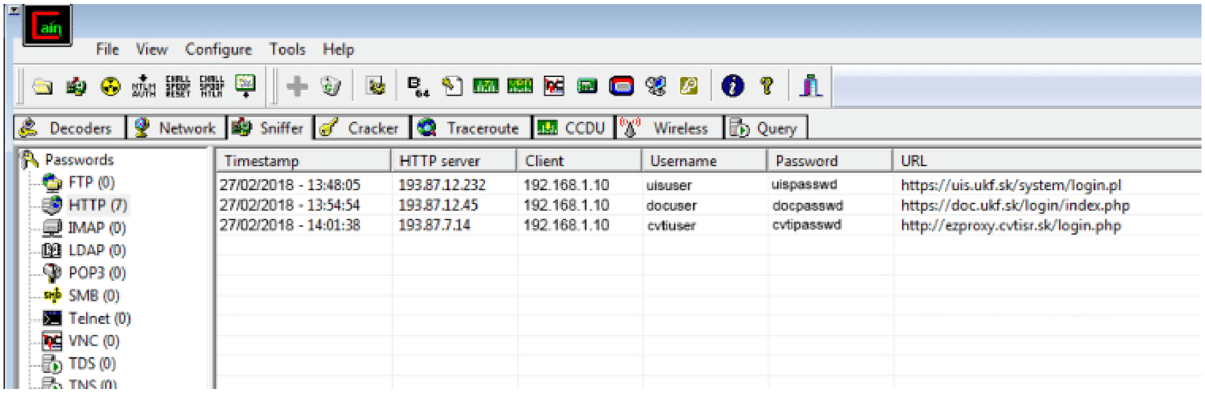
2.3 Technical Implementation

ZoneAlarm operated at the packet filtering level, inspecting both incoming and outgoing packets. It maintained a database of known applications and their expected network behavior, alerting users to any deviations. This packet-level inspection, combined with the ability to control application access, provided robust protection against unauthorized network activity.

3. Advanced Network Analysis Tools

As networks grew more complex, sophisticated tools emerged, offering deeper insights into network traffic.

3.1 Cain and Abel

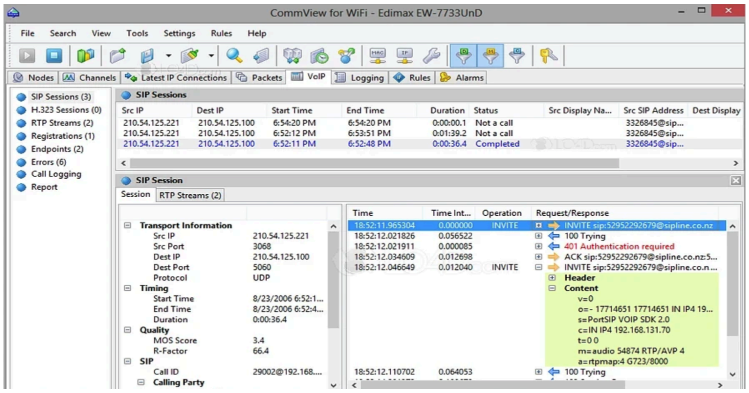


Timestamp	HTTP server	Client	Username	Password	URL
27/02/2018 - 13:48:05	193.87.12.232	192.168.1.10	uisuser	uispasswd	https://uis.ukf.sk/system/login.pl
27/02/2018 - 13:54:54	193.87.12.45	192.168.1.10	docuser	docpasswd	https://doc.ukf.sk/login/index.php
27/02/2018 - 14:01:38	193.87.7.14	192.168.1.10	cvtiuser	cvtipasswd	http://ezproxy.cvtisr.sk/login.php

Cain and Abel became notorious for its powerful capabilities:

- **Password Recovery:** Utilizing various methods, including dictionary attacks and brute-force attempts, to recover lost passwords.
- **Network Sniffing:** Capturing and analyzing network packets in real-time to uncover sensitive data.
- **ARP Poisoning:** Intercepting traffic between network nodes by manipulating ARP tables.
- **VoIP Call Recording:** Capturing and decoding voice data, allowing for eavesdropping on conversations.
- **Routing Protocol Analysis:** Examining and potentially exploiting routing information to manipulate network traffic.
- **Cryptanalysis Tools:** Analyzing and potentially breaking encrypted communications, posing significant security risks.

3.2 CommView



Src IP	Dest IP	Start Time	End Time	Duration	Status	Src Display Na...	Src SIP Address	Dest Display
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed		3326845@sip...	

Transport Information	
Src IP	210.54.125.221
Src Port	3068
Dest IP	210.54.125.100
Dest Port	5060
Protocol	UDP
Timing	
Start Time	8/23/2006 6:52:1...
End Time	8/23/2006 6:52:4...
Duration	0:00:36.4
Quality	
MOS Score	3.4
R-Factor	66.4
SIP	
Call ID	29002@192.168....
Calling Party	

Time	Time Int...	Operation	Request/Response
18:52:11.965304	0.000000	INVITE	INVITE sip:52952292679@sipline.co.nz
18:52:12.021826	0.056522		100 Trying
18:52:12.021911	0.000085		401 Authentication required
18:52:12.034609	0.012698		ACK sip:52952292679@sipline.co.nz:5...

18:52:12.046649	0.012040	INVITE	INVITE sip:52952292679@sipline.co.n ...
			Header
			Content
			v=0
			o=- 17714651 17714651 IN IP4 19...
			s=PortSIP VOIP SDK 2.0
			c=IN IP4 192.168.131.70
			t=0 0
			m=audio 54874 RTP/AVP 4
			a=rtpmap:4 G723/8000

18:52:12.110702	0.064053		100 Trying

Exhibit: CommView in or about March 2006.

Developed by TamoSoft, CommView offered a more user-friendly interface for network analysis:

- **Packet Capturing and Real-Time Analysis:** Capturing network packets for real-time or later analysis.
- **Protocol Decoding:** Decoding a wide range of network protocols, providing detailed insights into network traffic.
- **VoIP Traffic Analysis:** Including call flow reconstruction to analyze voice communications.
- **Wireless Network Monitoring:** (In CommView for WiFi) Monitoring wireless networks for security and performance.
- **Bandwidth Usage Tracking and Graphing:** Visualizing network bandwidth usage over time.
- **Custom Packet Generation:** Allowing users to generate specific packets for network testing and troubleshooting.

3.3 Legitimate Uses

These tools were invaluable for network administrators, security professionals, and researchers. They allowed for:

- **Troubleshooting Network Issues:** Identifying and resolving network problems efficiently.
- **Detecting Intrusions:** Recognizing unusual network behavior that could indicate a security breach.
- **Testing Network Security Implementations:** Assessing the effectiveness of security measures.
- **Analyzing Protocol Behavior:** Studying protocol behavior for research or optimization purposes.

4. The Dark Side: Misuse in Online Gaming

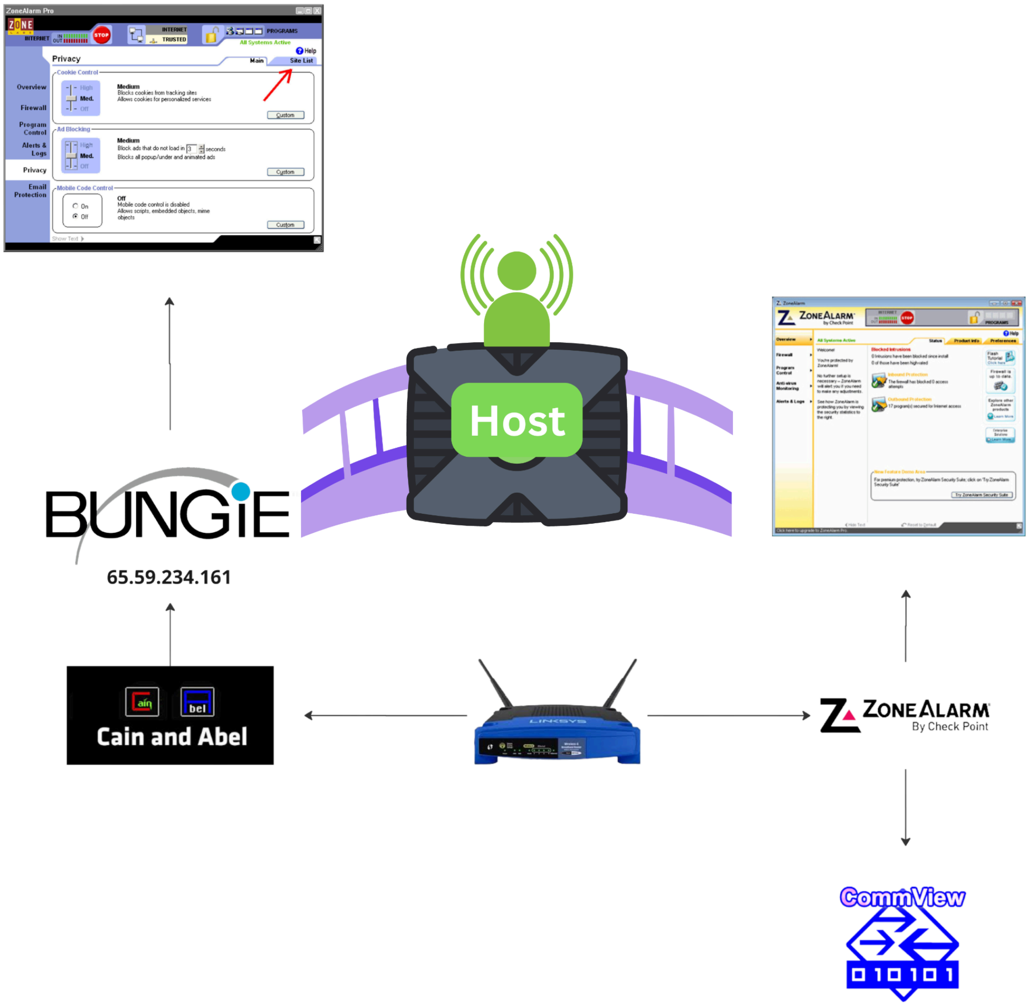
Despite their intended purposes, tools like Cain and Abel and CommView were widely misused for cheating in online gaming, particularly on Xbox Live and in *Halo 2*.

4.1 The Bridging Host Technique

This method became a popular way to manipulate game traffic:

- **Technical Setup:** A computer was configured as a network bridge between the Xbox console and the internet connection. This "bridging host" ran network analysis software like Cain and Abel or CommView. The Xbox's network traffic was routed through this computer, allowing for real-time manipulation.
- **Exploitation Methods:**
    - **Standbying:** Cheaters would momentarily interrupt the flow of packets to and from other players, causing lag for opponents while the cheater's game remained smooth. In fast-paced games like *Halo 2*, this provided a significant unfair advantage.
    - **Packet Sniffing and Information Extraction:** Game data packets could be intercepted and analyzed, allowing cheaters to extract information about player positions, health, or actions, which could be used to gain an unfair tactical advantage.
    - **Selective Packet Manipulation:** Cheaters could selectively drop or delay packets to and from specific players, enabling targeted disruption of opponent gameplay.

Below you will see a diagram on how online players would use it to bridge other people on their team. In particular for a rank gain, rarely was it for playing a game just legitimately:

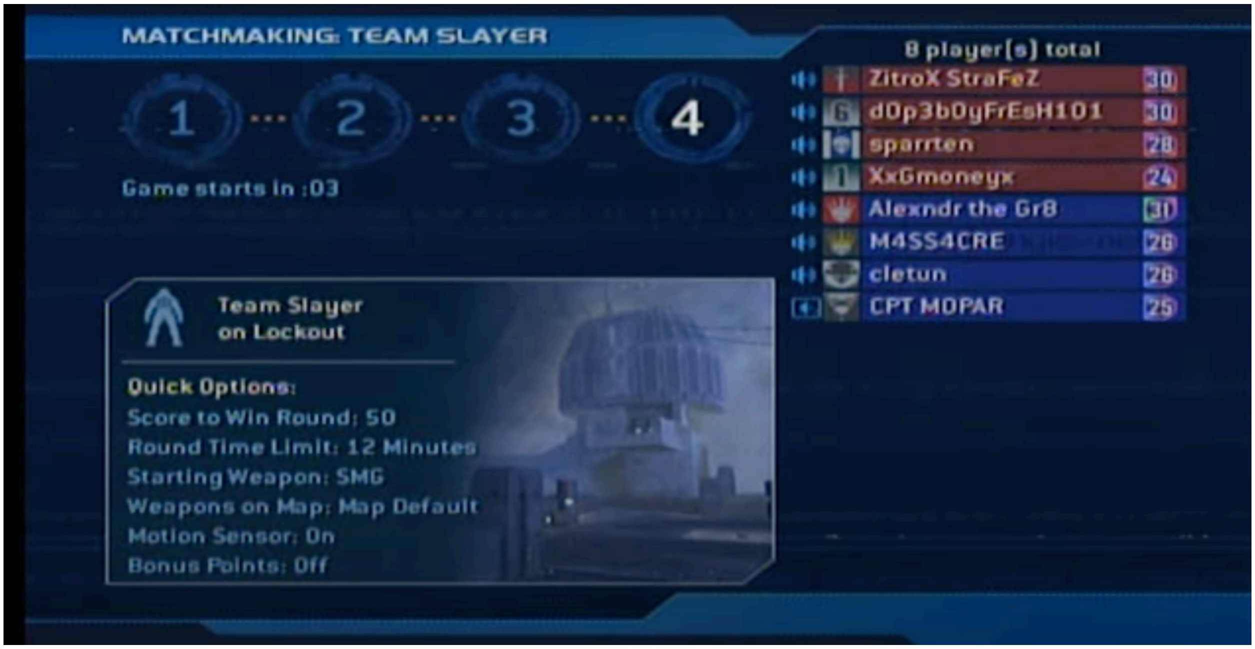


The Tools Behind Bridging Host, Standbying, Modding and DDoSing in Halo 2

This diagram showcases the software and tools used for network bridging in games like *Halo 2*. By manipulating the network connection, you can force a specific Xbox (IP Address) to become the host, granting various advantages. These advantages are especially impactful if you're also involved in other forms of cheating, such as modding or standbying.

In Cain and Abel, you'd ensure that Bungie's IP address is marked as "trusted." Back in 2006, Bungie's IP address was **65.59.234.161.** You then would either use ZoneAlarm or CommView. Once you've obtained his IP address, in this scenario we are using ZoneAlarm. You would add it to your trusted zone using the same method you used for Bungie's IP.

After doing this, click "Apply" in the bottom right corner. Next, navigate to the "Main" tab at the top right of the interface. In this section, adjust your firewall settings by setting the "Internet" firewall to "High" and the "Trusted" firewall to "Medium." With these settings in place, have your friend start the game. They will automatically be assigned as the host of the game you get put in via Matchmaking in Halo 2.



MATCHMAKING: TEAM SLAYER

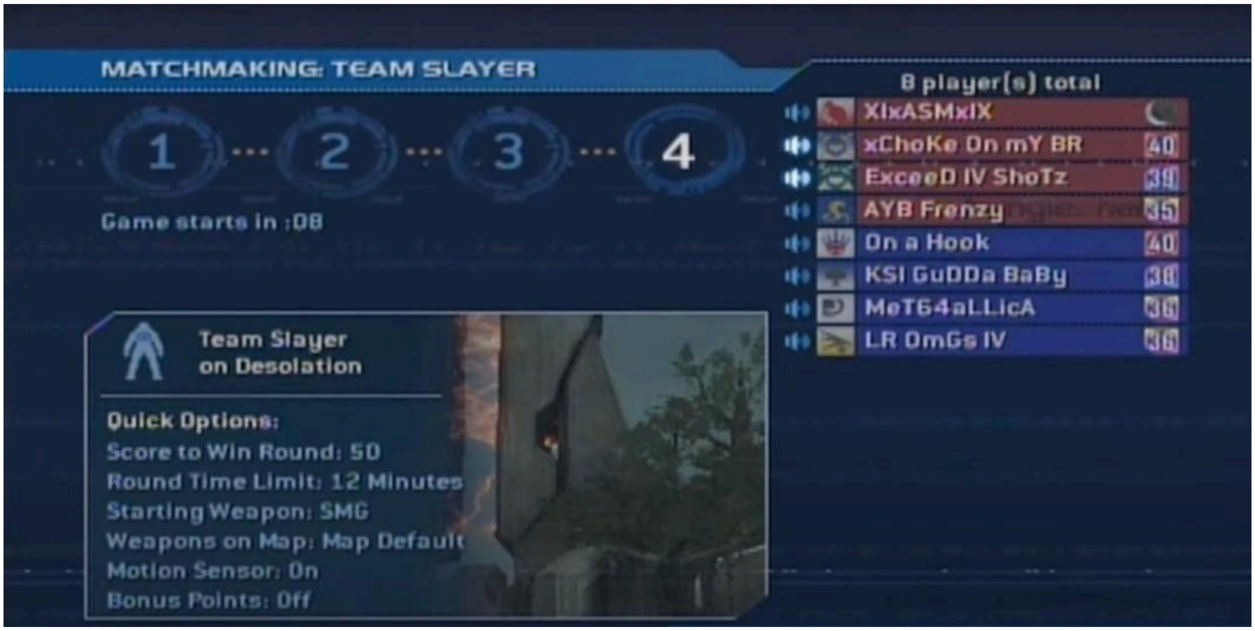
Game starts in :03

Team Slayer
on Lockout

Quick Options:
Score to Win Round: 50
Round Time Limit: 12 Minutes
Starting Weapon: SMG
Weapons on Map: Map Default
Motion Sensor: On
Bonus Points: Off

8 player(s) total	
ZitroX StraFeZ	30
d0p3b0yFrEsH101	30
sparrten	28
XxGmoneyx	24
Alexndr the Gr8	31
M4SS4CRE	26
cletun	26
CPT MOPAR	25

Exhibit: This is a typical pre game lobby. You can see the levels to the right.



MATCHMAKING: TEAM SLAYER

Game starts in :08

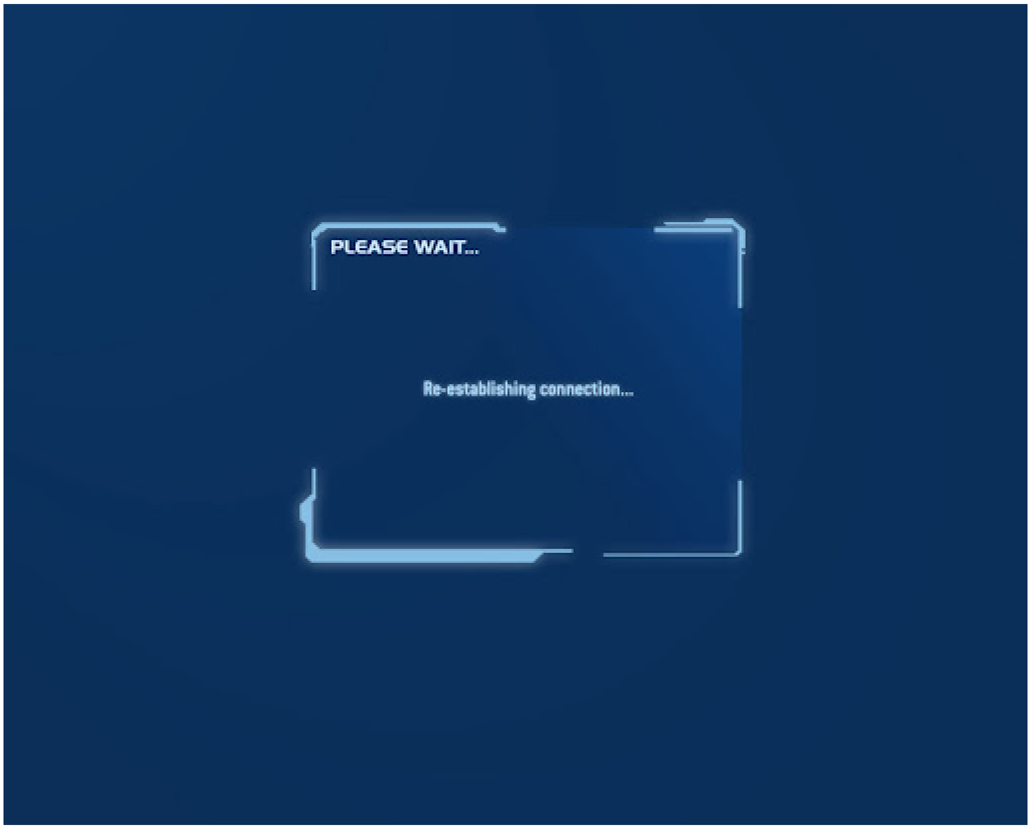
Team Slayer
on Desolation

Quick Options:
Score to Win Round: 50
Round Time Limit: 12 Minutes
Starting Weapon: SMG
Weapons on Map: Map Default
Motion Sensor: On
Bonus Points: Off

8 player(s) total	
XIxASMxIX	☾
xChoKe On mY BR	40
ExceeD IV ShoTz	39
AYB Frenzy	35
On a Hook	40
KSI GuDDa BaBy	38
MeT64aLLicA	36
LR OmGs IV	36

Exhibit: In this pre game lobby you can see people with “moons” (Level 44).

Exhibit: If the host of the game was using standby via their router.



PLEASE WAIT...

Re-establishing connection...

What others would see while the host is using Standby killing players.

Why?

Halo 2 had a very competitive leveling system. After about level 32 if you wanted to play a legitimate game with other online players without getting exploited in one of the various ways I've laid out - you would have to bridge hosts.

The Levels as shown below (1-50)

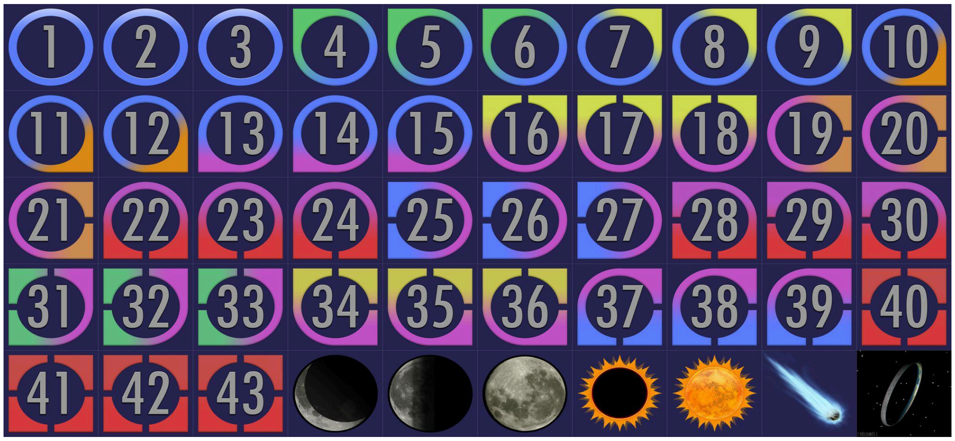
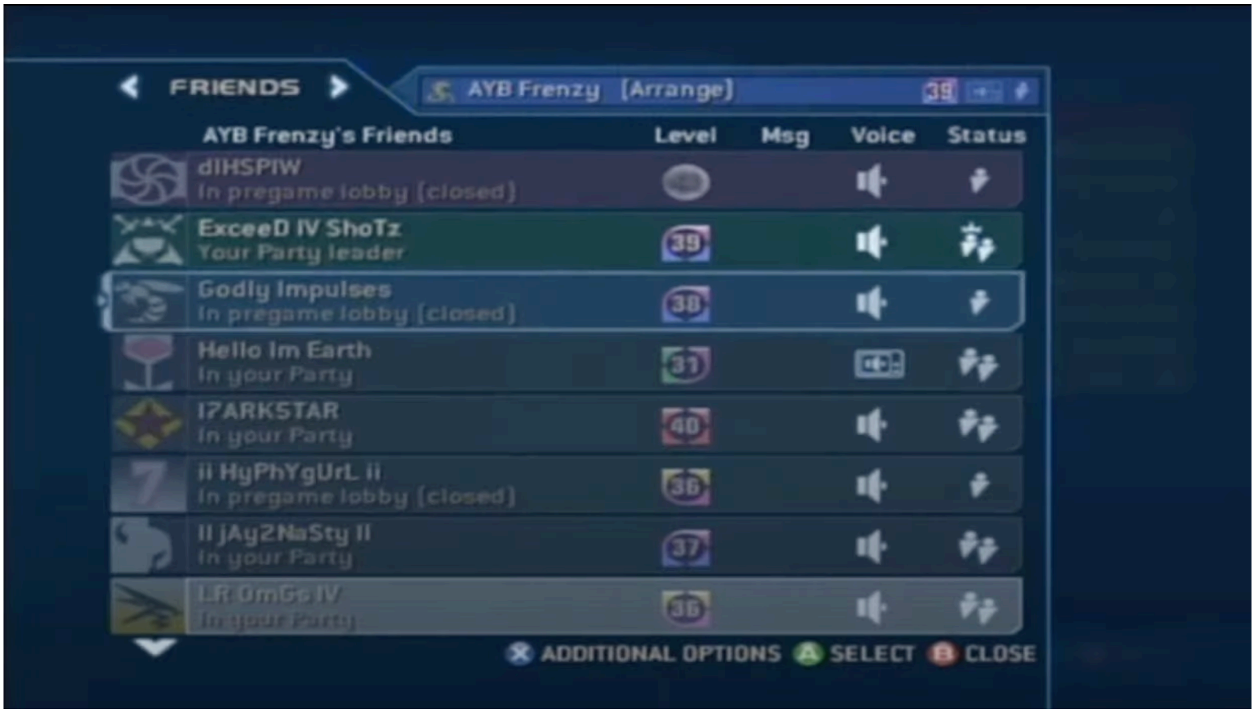


Exhibit: The Halo 2 Friends List; Pictured (Ranks, Usernames, Mics (On/Off)



AYB Frenzy's Friends	Level	Msg	Voice	Status
dIHSPIW In pregame lobby (closed)			🔈	👤
ExceeD IV ShoTz Your Party leader	39		🔈	👥
Godly Impulses In pregame lobby (closed)	38		🔈	👤
Hello Im Earth In your Party	31		⊡	👥
I7ARKSTAR In your Party	40		🔈	👥
ii HyPhYgUrL ii In pregame lobby (closed)	36		🔈	👤
II jAy2NaSty II In your Party	37		🔈	👥
LR OmGs IV In your Party	36		🔈	👥

4.2 Bypassing Security Measures

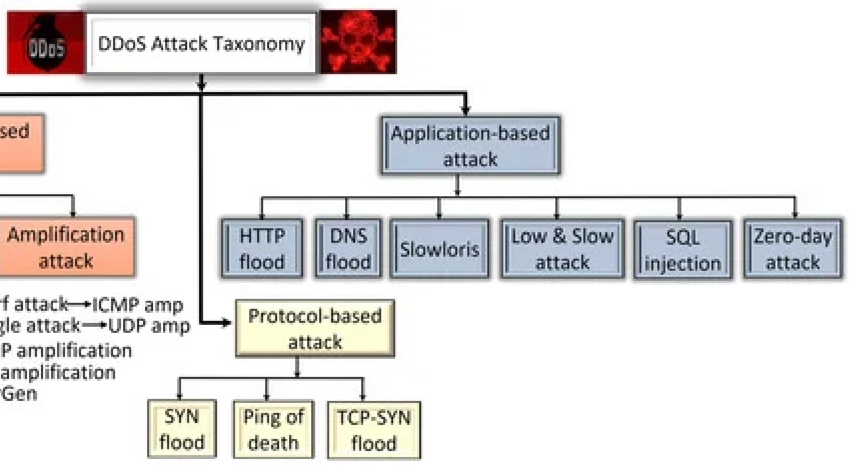
The bridging host setup often allowed cheaters to circumvent security measures:

- **Traffic Manipulation:** This occurred before reaching firewalls like ZoneAlarm, making it difficult for traditional security measures to detect and block such activities.
- **Initial Anti-Cheat Measures:** Game companies' early anti-cheat systems were often ineffective against these advanced techniques, leading to widespread abuse.

4.3 Impact on the Gaming Community

- **Widespread Cheating:** This led to frustration among legitimate players, undermining the fairness and enjoyment of online gaming.
- **Challenges for Game Companies:** Detecting and preventing these exploits required significant effort, often leading to delays in effective countermeasures.
- **Development of Anti-Cheat Technologies:** The situation spurred the development of more sophisticated anti-cheat technologies, including real-time monitoring and behavioral analysis.

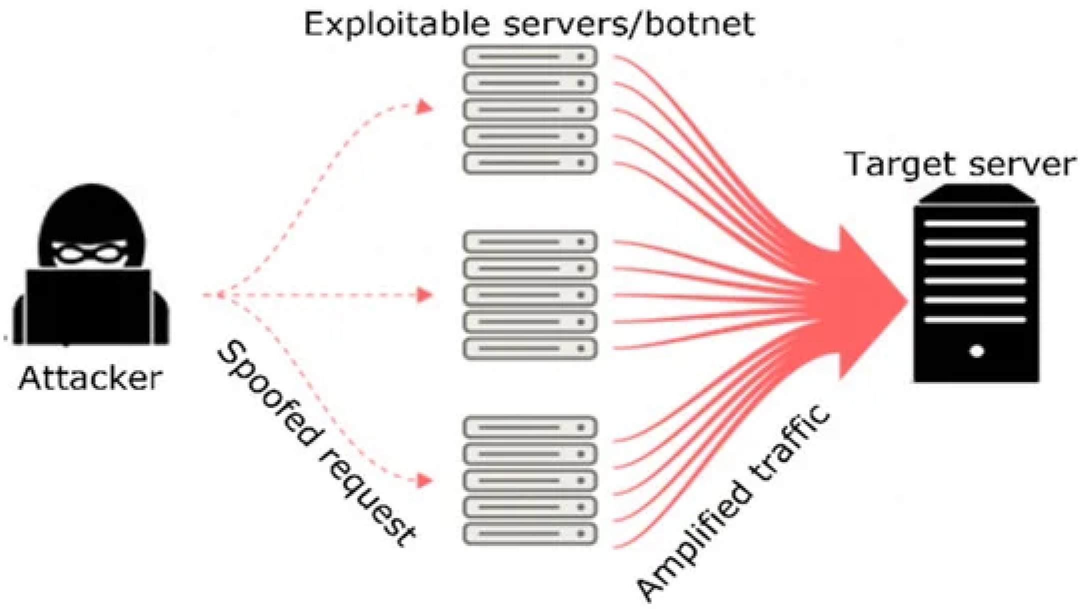
5. DDoS Attacks: A Growing Threat



As online services became more crucial, Distributed Denial of Service (DDoS) attacks emerged as a significant concern:

5.1 Technical Overview

- **DDoS Attacks:** Involve multiple compromised systems flooding a target with traffic, overwhelming its resources and making it unavailable to legitimate users.



5.2 In Gaming Contexts

- **Usage:** DDoS attacks were used to force opponents offline or disrupt gaming services, potentially manipulating online rankings or tournament outcomes.

5.3 Mitigation Strategies

- **Traffic Filtering and Rate Limiting:** To block or slow down suspicious traffic.
- **Anycast and Load Balancing Techniques:** Distributing traffic across multiple servers to minimize impact.
- **Cloud-Based DDoS Protection Services:** Using external services to absorb and mitigate attack traffic.

6. Router Standbying: Ensuring Network Resilience

In contrast to malicious techniques, Router Standbying represents a legitimate strategy for network resilience:

6.1 Technical Implementation

- **Protocols:** Utilizes protocols like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP).
- **Configuration:** Multiple routers are configured in a primary-backup relationship, ensuring automatic failover if the primary router becomes unavailable.

6.2 Benefits

- **Minimizes Network Downtime:** By ensuring continuous operation even if one router fails.
- **Allows for Maintenance Without Service Interruption:** Essential for businesses requiring constant network availability.

7. The Evolution of Network Security

The misuse of network tools in gaming sparked significant changes in both network security and game design:

7.1 Enhanced Encryption

- **Robust Packet Encryption:** Game companies implemented more robust encryption methods, making it more difficult to interpret or manipulate game data.

7.2 Improved Cheat Detection

- **Sophisticated Anti-Cheat Systems:** These systems included real-time monitoring and statistical analysis to detect and prevent cheating.
- **Behavioral Analysis:** Detecting unusual player behavior that could indicate cheating.

7.3 Stricter Penalties

- **Harsher Punishments:** Game companies instituted stricter penalties for confirmed cheaters, including permanent bans and, in some cases, legal action.

7.4 Hardware-Level Security

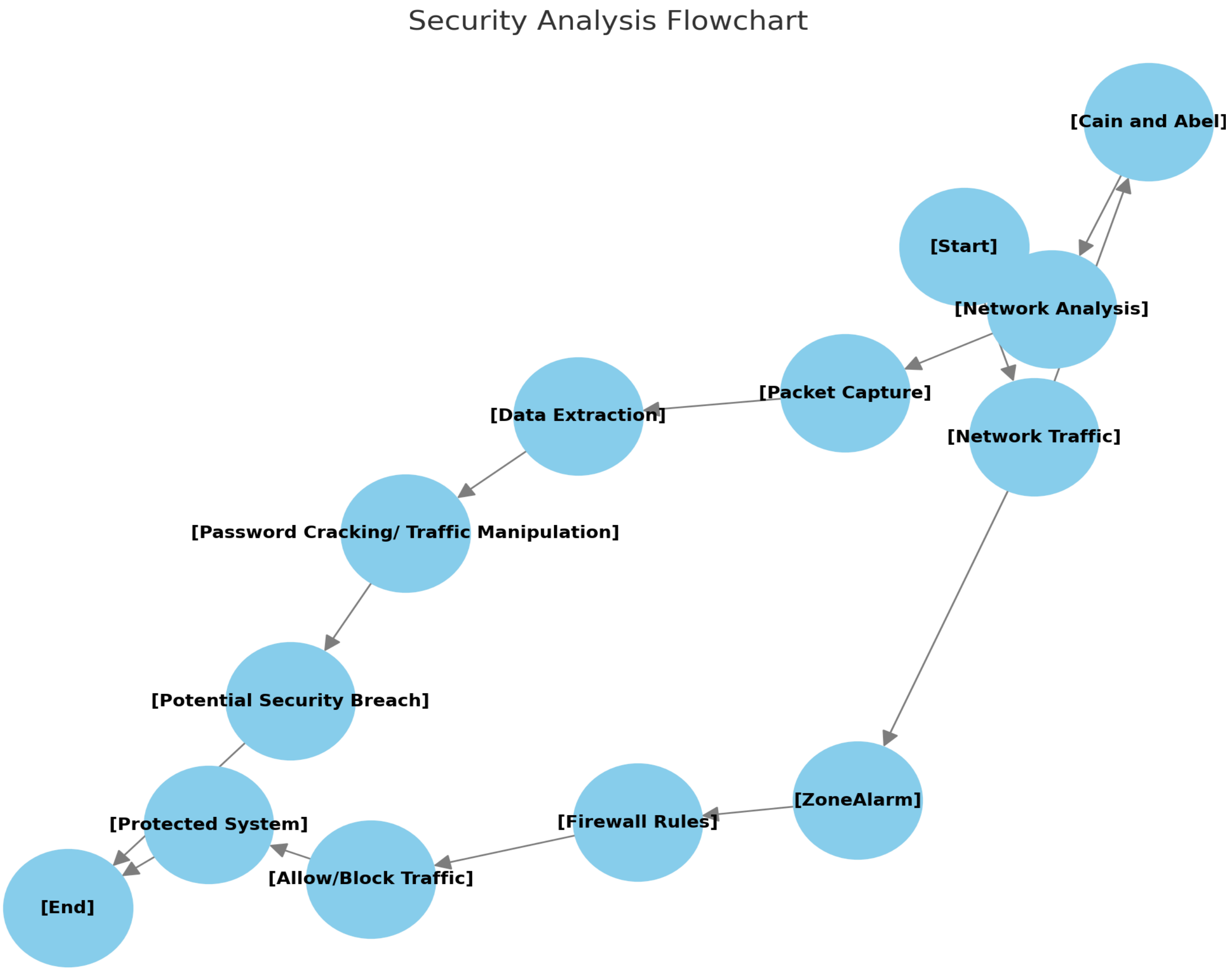
- **Console Security Features:** Manufacturers began implementing hardware-level security measures, making it more difficult to intercept or manipulate network traffic at the device level.

This history underscores the importance of ethical considerations in tool development and usage, as well as the need for continuous adaptation in security practices. As we move forward, the lessons learned from this era continue to shape both network security strategies and the design of online systems, emphasizing the need for robust, adaptive security measures in an increasingly interconnected digital world.

7.5 JuStCaLLMeGoD Fries Major Nelson's DNS in 2007

- **Law Enforcement:** This is one of the few times Law Enforcement got involved with people knocking other people offline via a DDoS or a packet flood. When Microsoft employee Major Nelson got his "DNS Fried", that was the red line. Infamous "account stealer" JuStCaLLMeGoD got raided and was ultimately arrested in 2008.

How ZoneAlarm Pro / CommView / Cain and Abel Interacted Through A Network


Security Analysis Flowchart
[Cain and Abel]
[Start]
[Network Analysis]
[Packet Capture]
[Data Extraction]
[Network Traffic]
[Password Cracking/ Traffic Manipulation]
[Potential Security Breach]
[ZoneAlarm]
[Firewall Rules]
[Protected System]
[Allow/Block Traffic]
[End]