Hwyl

Online FPS Games Social Steganography Communication Protocol

Prerequisites: Hwyl is an overt steganography communication protocol idea that I've had about a week ago. The protocol should respect the following guidelines:

- be very easy to use, without the need of using a scripting language nor inject anything in the game's runtime executables or DLLs.
- have a minimum footprint on the game's playability (ie no behavior that can be regarded as deviant by a 3rd party spectator)
- do not require any special equipment (that is, can be used even if you don't have a microphone)

Structure: The ways of encoding information by playing an FPS can be boiled down to several categories:

1. Equipment used
2. Actions performed
3. Commands issued
4. Team dynamics

The best game fit for this scenario is CS: GO – Counter Strike Global Offensive by Valve.

I will demonstrate the PoC in a short series on a video sharing platform. For now, we will address each category mentioned above and define the building block of our communication protocol.

1. **Equipment used:**

Glock-18 = s1
Dual Berettas = s2
P250 = s3
Tec-9 = s4
CZ75-Auto = s5
Desert Eagle = s6
R8 Revolver = s7

USP-S = s8
P2000 = s9
Five-Seven = s10

Nova = p1
XM1014 = p2
Sawed-Off = p3
M249 = p4
Negev = p5
MAG-7 = p6

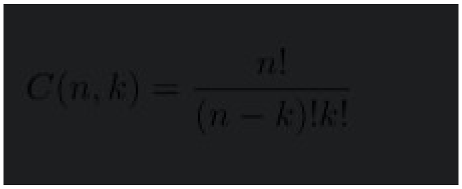
MAC-10 = p7
MP7 = p8
UMP-45 = p9
P90 = p10
PP-Bizon = p11
MP9 = p12
MP5-SD = p13

Galil AR = p14
AK-47 = p15
SSG 08 = p16
SG 553 = p17
AWP = p18
G3SG1 = p19
FAMAS = p20
M4A4 = p21
M4A1-S = p22
AUG = p23
SCAR-20 = p24

Molotov = e1
Decoy Grenade = e2
Flashbang = e3
High Explosive Grenade = e4
Smoke Grenade = e5
Incendiary Grenade = e6

We have a grand total of 40 items.

The total combinations formula for the first category is:



$$C(n,k) = \frac{n!}{(n-k)!k!}$$

What needs to be remembered is that not all weapons can be part of a said combination, for instance, in reality, we have several roadblocks:

We can carry only one secondary and one primary weapon at the time. Thus, our options are limited to a certain degree. Let us analyze it further:

We can pick only one out of 10 secondary weapons.

We can only pick one out of 24 primary weapons.

We can only pick one out of 6 auxiliary equipment, with the exception of flashbangs where we can pick 2.

The C4 is awarded randomly each round on T side, thus we have one added element of luck, which is much desired in such protocols. We couldn't ask for a fair SRNG coin toss aren't we:)?

Let us now reevaluate our options.

We will name the secondary weapons group S = {s1, s2, … s10}. We will call primary weapons group P = {p1, p2, … p24}. Auxiliary equipment E = {e1, e2, … e6}. C4 = {1, 0}.

Note that the C4 group, while binary, it's still available to both teams since CTs have defuse kits.

Auxiliary equipment is not mandatory, nor is the primary weapons group.

In total, we have the following number of options:

10 options for basic secondary weapons.

Adding 10 * 24 = 240 options for basic primary + secondary weapon config.

Then, we have the auxiliary equipment were we have 5 options per team, but where we can actually have 4 of them at all time. That makes it a combination of 5 elements → 5 + 10 + 10 + 5 = 30.

We then add those last 30 combinations (I didn't count the double flash … :D) to the previous 240 and we have a staggering 240 * 30 = 7200 options just for the first category.

2. **Actions performed:**

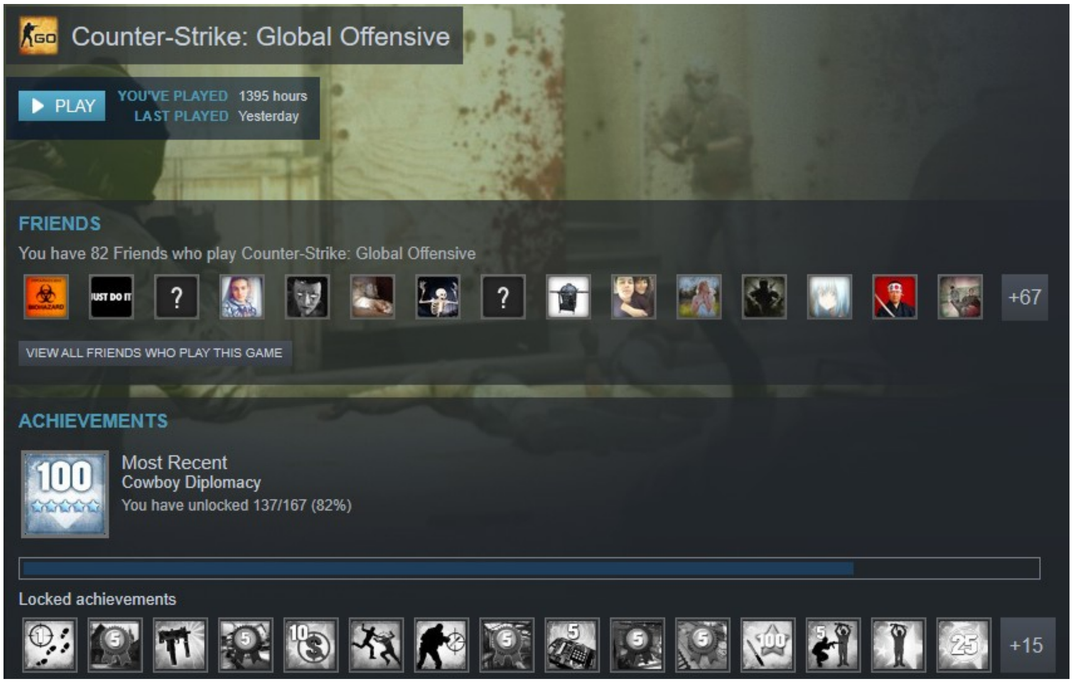
T side has two big advantages: the coin toss (C4) and the ability to choose the site. We can thus add the A and B option to the pool, making it 7200 * 2 = 14 400

Several actions can be performed during the game. One of them is the applying of graffitis which can add even more encoding options. We will add another 200 options for these, mainly because they vary with tournaments and whatnot. This gives us a whopping 2 880 000.

Another binary action can be performed is using the Zeus, randomly shooting it at various positions and rounds.

Next up, we have the number of rounds, which is 30 maximum or the first team that reaches 16. Based on my experience, 16 0 is pretty rare so we will pick 19, that is a 16 – 3. This further raises our options to 1 039 680 000.

BTW, I mentioned experience:



Counter-Strike: Global Offensive

YOU'VE PLAYED 1395 hours
LAST PLAYED Yesterday

FRIENDS

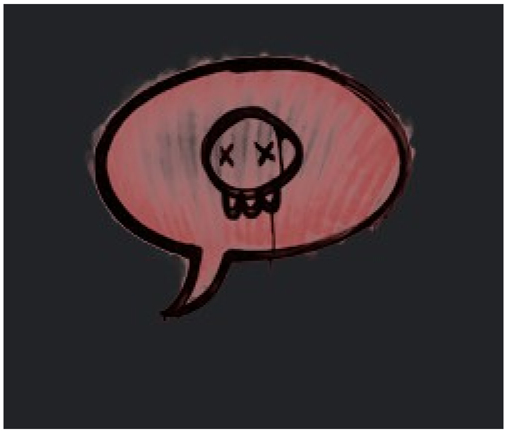
You have 82 Friends who play Counter-Strike: Global Offensive

ACHIEVEMENTS

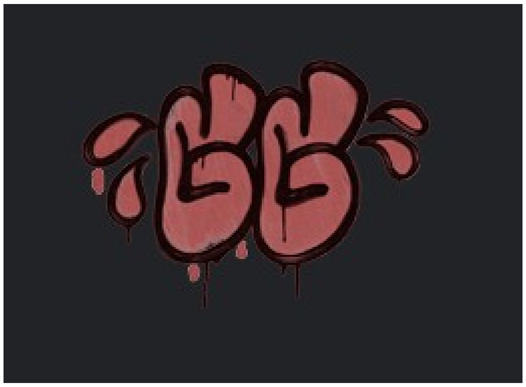
Most Recent
Cowboy Diplomacy
You have unlocked 137/167 (82%)

Locked achievements

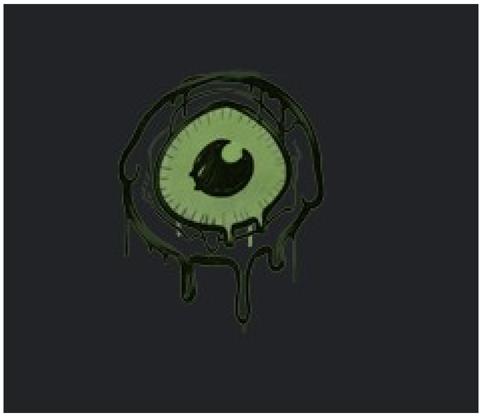
For example, graffiti can be used for different meanings:



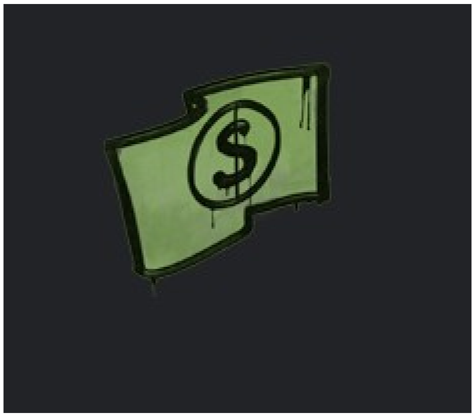
- Silence, or shut up



- well done, good job



- you are being watched, surveilled, etc



- more funds required, send money

- deal is over (L sign for loser, losing)

3. **Commands issued:**

The CS: GO radio commands can be issued at all times. This can be timed accordingly to a schedule set up before by the team.

The list of commands is rather simple and intuitive and can be used in the context or with the intent specified beforehand by the communicating parties. I am pretty sure you are tired of Alice and Bob being used all the time, so let’s get down to it.

```
"go"
"fallback"
"sticktog"
"holdpos"
"followme"

"roger"
"negative"
"cheer"
"compliment"
"thanks"

"enemyspot"
"needbackup"
"takepoint"
"sectorclear"
"inposition"
"coverme"

"enemydown"
"takingfire"
```

```
"regroup"
"getout"
```

Radio commands can be used to create a virtual dialogue:

- go
- negative

- enemydown
- roger

- takingfire
- roger

- takepoint
- thanks

- coverme
- roger
- cheers

- followme
- negative
- sticktog
- roger

- getout
- roger
- thanks
- inposition
- roger
- go
- negative
- fallback
- roger

4. **Team dynamics**

Everything from passing the C4, to “drop me a weapon” to schemes regarding positioning (eg 2 A, 1 mid, 2 B) can be used to exchange intel.

Leaving a site clear can signal a bail, so is rushing together mid or playing an “eco” round. This can add even more options to the list but we will stop counting them, you get the point.

Hwyl protocol decoding example:

1. Download the match
2. List down all variables for each round in particular
3. List down all actions performed for each round
4. List down all radio commands issued
5. Use the decoding table that you have agreed upon with your communication partner

In order to save time, I just recorded a 10 min video where I just showcased the demo replay feature. **What I wanted to show there was the capability to get the other's player equipment list, actions performed and radio commands (even chat commands).**

I did not showcase the use of friendly touches etc (harming teammates or cyka blyat).

A full match should look like this:

R1 = {[s1, p13, e2, 1] + {getout + thanks} + 'GG' (grafitti) + [2a, 1m, 2b]}
R2 = {[s4, 0, 0, 0] + {negative} + 'noscnope' (grafitti) + [1a, 2m, 2b]}
.
.
.
.
R19 = {[s5, p20, e3 + e2 + e1] + {cheers} + no grafitti + [3a, 1m, 1b]}

Well, there you have it :)

Have fun :)

Chelalau Ionut Mihai, R&D Engineer
c.ionutmihai@protonmail.ch