3-21-2012

Pandorabots for Mobile App Developers

If you are developing a mobile app for Android, iPhone, or other mobile OS, or if you are building a proxy service for mobile apps, and you are trying to connect your app to Pandorabots, please follow these steps:

1. Create an account on the Free Community Server (at www.pandorabots.com). You can create an account on our free server www.pandorabots.com to develop and test your pandorabot, but when it goes "live" you will quickly use up too much of the Free Community Server resources. So when you are ready to go live, please sign up for the Shared Hosting Service and we will move your pandorabot to the shared hosting server.

2. Create a pandorabot - After creating your account, follow the easy steps (find more details here) to create your own pandorabot(s). This can be as simple as cloning one of the free pandorabots we make available to you. When you publish your pandorabot, it will be assigned a unique bot id. You can connect your app to your pandorabot through the XML-RPC connection using your unique bot id. You will provide this pandorabot to customers of your application or service.

If you are using the Free Community Server to host your pandorabot and it reaches its resource limit, the pandorabot's response will be changed to a message indicating that it is using too many resources on the Free Community Server. If your app begins to receive this message, please follow the above steps to create a bot on a Shared Hosting server.

10-26-2011

Pandorabots under heavy load from mobile apps

Apple introduced Siri recently, and many developers are developing and deploying phone apps based on Pandorabots. We are currently making some configuration changes to improve

performance. Meanwhile, if you are active in a chat bot forum, blog, or community, please help spread the word about the following:

If you are developing a phone-based app, please contact us at info@pandorabots so that we may explain our other service options. If you see your name near the top of this list (http://pandorabots.com/botmaster/en/mostactive), you should be contacting us. We have difficulty hosting very high traffic pandorabots on the Free Community Server. Wildly popular mobile apps using the Pandorabots free server (www.pandorabots.com) take resources away from many other botmasters and developers, who experience a service degradation.

Because of resource constraints on the Free Community Server we intend to move popular pandorabots onto our subscription services (see).http://bandore.pandorabots.com/subscription/ServiceComparison/index.html

One difficulty faced by the mobile developers is that their apps are “hard-wired” to specific bot ids on the Free Community Server. Because of the obstacles of the approval process required to push modified apps to the iPhone app store or Android Market, the transition to a different Pandorabots server takes time. A download app connected to a specific botid is quite likely to immediately fail, so the app developers must offer an upgrade to a new version when the transition is made.

We have real problems contacting some of our users. This is especially true for some of the pandorabots in the current “most popular list”. Pandorabots makes no attempt to verify the identities of people signing up for the free server. Unfortunately sometimes people use bogus email addresses for user ids, or in other cases botmasters lose access to their email addresses, and we are unable to contact them through the provided credentials. For this reason we are making this announcement to the broader community in the hopes that any botmasters we cannot reach will contact us.

9-19-2011

For some time we’ve been grappling with an issue involving the potential misuse of pandorabot content supplied by authors. And more recently, it has come to our attention that people developing chatbot-based phone apps are using other author’s chatbot’s content. Access to the content is achieved through accessing the pandorabot’s published XML-RPC connection (or in some cases by screen-scraping HTML pages--though we discourage this technique). In some cases these are unauthorized and unwelcome accesses.

When the Pandorabots Community Server was designed originally, we chose to create a Most Popular list containing links to the most active pandorabots on the Community Server. Our intention to was to foster good-natured competition among pandorabot authors while making it easy for clients to locate active and well-developed pandorabots on the free server. At that

time we failed to perceive the potential need for a secure XML-RPC connection. And today anyone can access any pandorabot by using its botid from the Most Popular list. Making a change to the interface runs the real risk of causing many existing applications to fail.

Previously we have recommended that people using XML-RPC establish their own account on Pandorabots and create their own pandorabot for their application, rather than connecting to someone else's existing bot through the API. Creating your own bot on Pandorabots is easy. An exception to this rule is the original ALICE bot (botid=f5d922d97e345aa1), which can be used in third-party apps that comply with our Terms of Service.

In the situation that third-party developers seek to connect to other people's pandorabots, a number of potential problems arise - including:

1. Clients (whether paying or not) may come to associate the phone app (or other application) with a third party unrelated to the actual pandorabot author.
2. Pandorabot authors may wish to obtain compensation for the use of their content.
3. The third-party app may consume significant resources (including exceeding the upper limit on daily interactions on the Community Server).
4. Some Pandorabots are designed to work specifically with web browsers, for example by playing sounds, showing images, providing links or including Javascript in their responses. These browser-dependent operations may not work through a third party app, thus degrading the quality of the bot's responses.
5. Potentially, a third party could create an app that re-brands your pandorabot in an offensive or abusive manner. In the worst case, a pandorabot author could be legally liable for a third party's bot (under some jurisdiction's laws).
6. Some developers take the position that they that they may interact with a publicly published bot, that everyone has equal rights to access public web pages and XML-RPC channels. They believe they can avoid seeking an author's permission (for publicly accessible pandorabots)

Some authors willingly allow nearly anyone to use their pandorabot content (e.g. the ALICE pandorabot). Other authors may wish to avoid anyone using their content. And this latter stance seems complicated to enforce for pandorabots publically hosted on the Community Server.

As another example, consider the recent publicity surrounding an application created by two Cornell University graduate students, which linked two instances of Cleverbot together for bot-to-bot communications. Although Cleverbot is not a pandorabot, the students' application raises some of the same concerns. Because their app was so popular, some people assumed that the bot itself was developed at Cornell. According to the bot's developer Rollo Carpenter, some of the "reporting often wrongly suggests or implies that Cleverbot comes from Cornell".

Before deciding how to proceed, we want to receive your comments and suggestions for addressing this issue. Do you think the solution would be a more secure XML-RPC style

interface (but then how do we prevent screen-scraping of public HTML pages?). Or an administrative solution such as a change in our Terms of Service? One possible solution would be to ask application developers to clearly attribute content obtained from pandorabots hosted on the Community Server. How might this best be accomplished? Do you have other ideas?

We've just established a beta program for pandorabot authors who wish to publish phone-based apps. Drop us a line at info@pandorabots.com if you would like to learn more details.

References:

http://www.hawkee.com/snippet/6306/

http://knytetrypper.proboards.com/index.cgi?action=display&board=Pandora&thread=2172&page=1

http://itunes.apple.com/us/app/chatbot/id449856276?mt=12

http://getsatisfaction.com/fliplevel/topics/unknown_error-1i8lmh

http://www.chatbots.org/ai_zone/viewthread/632/

Diary of Possible Solutions

9-22-2011
We've received some really interesting possible solutions from the community. Some of whom requested anonymity. We've extracted the essential ideas and presented them here so that we can receive further feedback from the community. We invite each of you to contribute ideas (and you may remain anonymous if you wish) in the comments. We will harvest the best ideas and add edited versions to this page (while preserving anonymity if you wish).

Suggestion from anonymous botmaster of one of the Top 10 Most Popular bots on the free server:

Could you add a new API feature called "secure XML-RPC", or "private XML-RPC" or "subscription XML-RPC" so that only the botmaster and those he authorizes know the credentials to access this API.

And at the same time, provide the option to disable existing XML-RPC.

This proposal would address these concerns:

- Botmasters who only want an HTML interface would be happy if they could just disable existing XML-RPC
- Botmasters who have their own custom apps, such as Flash, Second Life, etc., would be happy if they could use the new secure API and disable the existing XML-RPC
- Botmasters with legacy XML-RPC apps would be happy if they could do nothing and continue using existing XML-RPC.
- Developers of third-party apps who want to add the pandorabot would be happy because they could find botmasters who continue to use XML-RPC (perhaps you could add a clause in the in TOS allowing the public XML-RPC to be re-used without the botmaster's explicit permission unless they disable it); or alternatively, third-party developers could pay for subscription links to a private XML-RPC.

Here's one possible way to implement the "secure" XML-RPC: Duplicate the function of the existing Pandoabots subscription feature for XML-RPC. Then the botmaster can keep their own botid secret, and (optionally) give out a subid for instances of the secure XML-RPC.

Suppose botmaster Frank has a Flash app that connects to Pandorabots through the XML-RPC interface. The bot has botid 1234cde, and although this bot is published, Frank never gives out the URL (side note--Frank could modify the custom HTML files so that even if his bot id did get out, the HTML could be blank or for example say "no bot here"). Instead he creates a subscription instance of 1234cde with a new sub id 6789xyz, and his Flash app connects to XML-RPC port for subid 6789xyz.

Now, if an iPhone app developer George comes along and wants to pay Frank to use his bot, then Frank can create a new subid (for some number of months) and sell it to George. George can pay Frank through Paypal subscription.

(In any case, they might all like to receive some small money for uses of their bot).

Suggestions from anonymous botmaster of Top 10 bot on premium server:

AIML Responder ideas

My idea is similar to the old "Responder" class in early Java versions of ALICE. Make the output of AIML depend on the context or medium of the output. In some contexts the bot where the bot could be "stolen", or "non-authorized" the bot could "I am sleeping and need more resources" or some other message determined by the botmaster.

Show people how to create bots that are 'sleeping' when accessed through some unauthorized medium.

The basic idea behind an AIML Responder:

You should be able to set up a context for the response, for example a mobile app context, an HTML context (the default), a text-only context (such as the Loebner interface, or IM), and a TTS context for the avatar.

This is already partially implemented this in Pandorabots with the <template> context attribute for example we use this with our Sitepal avatar:

```
var response_1 = "<template context="tts"><response index="1"/></template>";
```

The <template context="tts"> does all the clever stuff like stripping out quotes and HTML markup before the javascript sees them.

At present <template context="tts"> works in custom HTML but not inside an AIML file.

If I train a bot with:

```
<category>
<pattern>TEST ONE</pattern>
<template>He said, "I am quoting "The Matrix"."</template>
</category>

<category>
<pattern>TEST TWO</pattern>
<template context="tts">He said, "I am quoting 'The Matrix'."</template>
</category>
```

Then I get:

Human: Test one
Bot: He said, I am quoting The Matrix..
Human: Test two
Bot: I have no answer for that.

I couldn't think of a way to put <template context="tts"> between the bot and the XML-RPC.

AIML Solution

With my Flash bot, I get it so that it says a secret word at the very start unknown to the user, similar to this

category:

```
<category>
<pattern>MUSTSAYTHIS</pattern>
<template>
<think><set name="validsite">YES</set></think>
</template>
</category>
```

I then have another category:

```
<category>
<pattern>TESTSITE</pattern>
<template>
<condition name="validsite">
<li value="YES"></li>
<li>This chatbot has been stolen by [name of developer], the app developer of [some app]. You should talk to [my bot] for free at [my web site].<br/>Please do not support this developer who has stolen this chatbot without the owner's permission and then sold it to you.<think><set name="topic">STOLEN</set></think></li>
</condition>
</template>
</category>
```

I then <srai> to this category in common categories like "hi", "hello" or the * category. If the chatbot is used via a phone app, people will just start talking and it won't say the secret word. I use a modified version of shutup.aiml to ban the user from talking to it.

I do the initial secret word in Flash but wondered if it is possible for Pandorabots to implement something similar?