

Idea

Unfortunately there are far more iPod users than there are Rockbox users. If we want to provide an easy transition for these users, then we need to provide a way for them to use their existing software with Rockbox. Additionally a significant portion of the Rockbox user base is requesting that they be able to use iTunes with their iPod.

Some benefits of integrating Rockbox with iTunes include the fact that users will not be required to rebuild their collections/playlists when they want to upload songs from their existing collections to Rockbox. Additionally for users that use both an iPod and Rockbox, they will be able to use a single piece of software.

Implementation

The implementation should be transparent, so that the users do not need to know how the songs are being transferred to their Rockbox, it just works. In effect, the Rockbox will act as if it is an iPod while connected to the computer.

Game Plan

In order to complete this task, I will use usb sniffing tools, such as UsbSnoop in order to capture traffic between the iPod and iTunes. The specific traffic that will be watched is the handshake protocol when the iPod is inserted and when it is removed. This traffic will be the easiest to sniff because we know the difference between a typical mass storage device and the iPod. Since the iPod identifies itself as both a mass storage device and transmits data to iTunes, we can just subtract the mass storage protocol from the stream in order to isolate the handshake data used to determine that the device is indeed an iPod.

The next step will be to watch the transfer of files between the iPod and the computer. Using a "blank" audio file will make this process fairly easy because you will be able to distinguish the "blank" audio file from the rest of the protocol. Additionally, work may be done inside iTunes itself in order to discourage monitoring of the data stream. This will require a debugger, such as ollydbg. Since we are the ones that determine what data goes into iTunes, it will be easy to determine the process that iTunes goes through in "iPodifying" the content.

Once the protocol has been discovered, it will be relatively simple to emulate this in Rockbox players. The first step will be to recreate the handshake protocol used by the iPod in order to determine who's iPod is plugged in, what firmware it is running, etc. The next step will be to recreate the protocol iTunes uses to transfer and encode the files and metadata. Once this is done, steps must be taken to ensure that each Rockbox is given it's own unique id in order to be distinguished from other iPods/Rockboxes.

Finally the protocol must be able to work in the reverse direction, so iTunes will be able to recognize, what songs are already on the Rockbox. This task will be the most challenging because iTunes most likely directly reads the database from the iPod rather than indexing individual files. As noted by many sources, the database is secured. In order to replicate this security in a Rockbox database, we must first understand how exactly it is secured.

This will require some major reversing of iTunes. However the process is systematic, you add the same file to the library over and over and note the changes in the database. Then you make small changes to the file and repeat the process, noticing the difference. This should provide a general idea of how the database is encrypted. The specific details can be discovered through debugging iTunes in ollydbg.

About Me

I am a hacker, I take *everything* apart, you name it, hardware, software, even concepts. I have a lot of experience programming (9+ years) and have worked with a number of open source organizations, like ikiwiki (GSoC 2007), XMMS2, the Linux kernel, and ProjectXI (a self started project).

My experience in creating ProjectXI is most relevant to this project. ProjectXI was designed to be a game server for the commercial game Final Fantasy XI. The original server was run solely by Square Enix and not even the binary server was distributed. I decided to create my own server for the game from scratch. To do this I used Wireshark to monitor the Ethernet connection between the game's client and server. However the protocol was encrypted. In order to decrypt the protocol I had to sift through megabytes of assembly code in order to find out that it was encrypted using a modified version of the Blowfish algorithm. Since the key used by the Blowfish algorithm was never transmitted through the network, I had to determine how it was generated in parallel between the client and server, this required further disassembly.

Once all of the decryption was through, I then had to analyze the protocol itself since it is not human readable. The results for hundreds of decrypted packet types can be found on a wiki that I used located at <http://wiki.projectxi.org/>. Specifically look at the section marked "Command."

I have also reversed hardware protocols such as a ps/2 keyboard. To do this I used an oscilloscope to monitor the voltages across the data lines and the clock lines. After several days, I had a firm grasp on the protocol and began designing schematics for my own keyboard. I then implemented my own keyboard using only 74LS chips (simple logic gates such as AND, OR, NAND, XOR, etc.). Sure I could have used schematics found floating around the net, but what fun would that be? Besides, I doubt that there are "schematics" floating around the web for iTunes or the iPod.

Time Line

| | |
|-------------------|---|
| Now - May 26 | Research the structure of the iPod database |
| May 26 - June 1 | Reverse Engineer the handshake protocol |
| June 1 - June 14 | Reverse the file transfer protocol |
| June 14 - July 1 | Write initial code to emulate iPod for iTunes After this is complete, a Rockbox with no initial songs should be able to sync with iTunes |
| July 1 - July 15 | Research database creation in iPod |
| July 15 - July 29 | Create an emulated iPod database |
| July 29 - Aug 5 | Generate unique id's recognizable by iTunes |
| Aug 5 - Aug 11 | Test Rockbox-iTunes interaction on multiple devices |
| Aug 11 - Aug 18 | Develop a method to add songs to iTunes database |

without iTunes (used for preexisting songs on
Rockbox)