From: Vincenzo Iozzo <[redacted]>
Sent: Monday, November 10, 2014 9:39 AM
To: jeffrey E.
Cc: Joichi Ito
Subject: Bitcoin over Tor considered unsafe

This is a very interesting paper: http://arxiv.org/pdf/1410.6079v1.pdf

It gets technical but the TL;DR is that mobile devices & privacy seeking =itcoin users (mobile devices because they can't hold the whole ledger =ot for privacy reasons) route their bitcoin activities through Tor.
These guys showed that you can with roughly 5k a month hijack all the =itcoin clients inside tor and allow both the de-anonymization of the =sers and also potentially to double spending attacks assuming that you =ontrol something like 10% of the network.

The two main issues are that 1) Bitcoin has an anti-DoS protection that =s very strict and 2) Bitcoin connections are not =uthenticated/encrypted.

It's funny because it's another instance of where Postel's law is right =http://en.wikipedia.org/wiki/Robustness_principle), in the sense that =ere Bitcoin clients less restrictive then the attack would not be =easible. On the other hand if they were less restrictive the network might get DoSed..

The remediations section is also very interesting because essentially =ne of the solutions proposed is to centralize Bitcoin more..

Again, nothing earth shaking but by now you should start to see a trend =ith Bitcoin and security :-)


```
V=?xml version=.0" encoding=TF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version=.0">
<dict>
        <key>conversation-id</key>
        <integer>306602</integer>
        <key>date-last-viewed</key>
        <integer>0</integer>
        <key>date-received</key>
        <integer>1415612324</integer>
        <key>flags</key>
        <integer>8590195713</integer>
        <key>gmail-label-ids</key>
        <array>
                <integer>2</integer>
        </array>
        <key>remote-id</key>
        <string>455026</string>
</dict>
</plist>
```