pCTF2011 Challenge 11 write-up

April 2011 © Daniel Kachakil @ int3pids

Summary

This document describes a solution to the challenge 11 (called "**Just being nosy**") of the first edition of the Plaid CTF, organized by the team Plaid Parliament of Pwning (PPP) held on April 22-24th, 2011.

Official description of the challenge

Category: *forensics*

One of our agents installed a packet sniffer on a router in the hallway a week ago to see if there's anything valuable that people have been sending behind locked doors.

Yesterday, it captured this file headed to a server owned by a different company. It seems AED's rivals haven't been lazy. Besides stealing their scientists, of course.

Find out what it's about.

Update:

We figured out these contain coordinates! However, we couldn't figure out what the 0's and 1's represent.

What could it be? It must be really important....

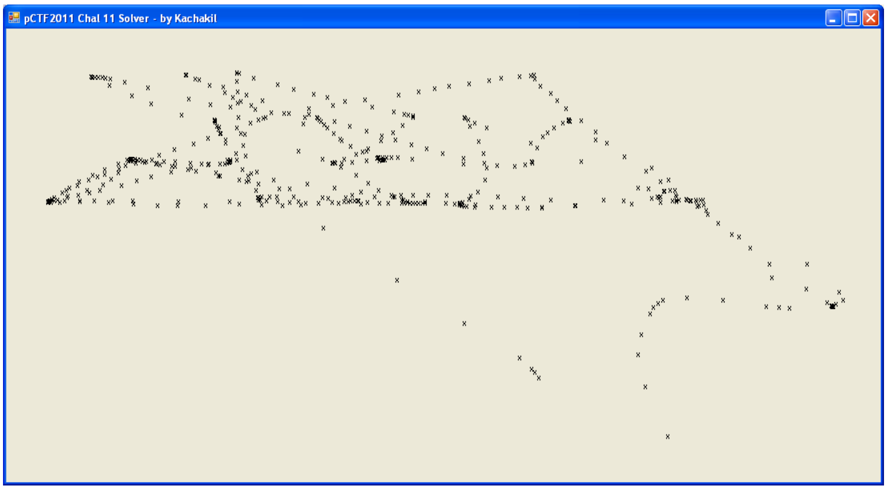
There was also a text file attached containing lines like these:

```
2011-4-23 17:8:39:046505  821  501  0
2011-4-23 17:8:39:980871  793  439  0
2011-4-23 17:8:40:084778  784  399  0
2011-4-23 17:8:40:195842  788  374  0
2011-4-23 17:8:40:300604  799  348  0
2011-4-23 17:8:40:404556  803  340  0
2011-4-23 17:8:40:507338  809  335  0
2011-4-23 17:8:40:612895  815  331  0
2011-4-23 17:8:40:717550  845  328  0
2011-4-23 17:8:40:821510  890  331  0
2011-4-23 17:8:40:925636  944  339  0
2011-4-23 17:8:41:029542  960  340  0
2011-4-23 17:8:41:133589  973  341  0
2011-4-23 17:8:41:237530  951  303  0
2011-4-23 17:8:41:344980  910  252  0
2011-4-23 17:8:41:453896  817  195  0
...
```

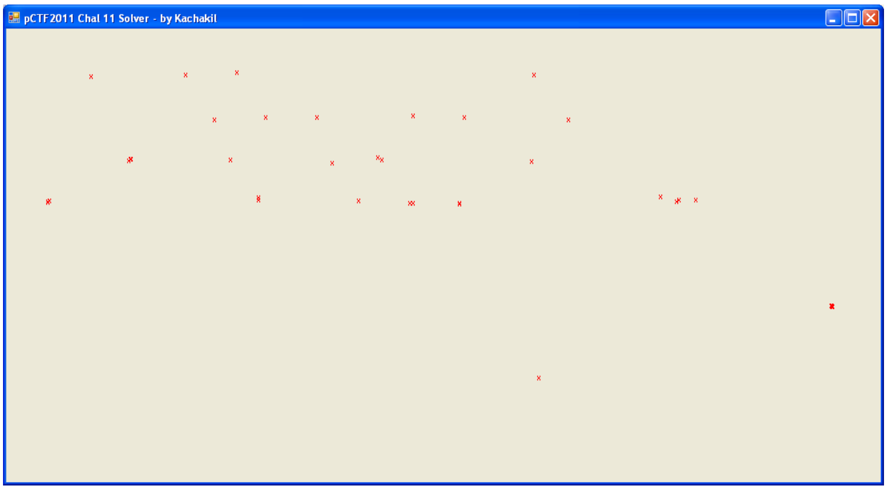
Analysis of the data

There are 5 columns in the file, so let's do some assumptions based on the data contained in each one. The first column must be a date and the second column must be a time in a high-precision format. Ok, so if the clue is talking about coordinates, they must be the ones in the next two columns (3rd and 4th). The remaining column only contains zeros and ones, so for now we will only assume that is some kind of boolean data.

Because the first two columns are in descending order and very close in time, we will strip them, so only 3 columns will remain in the file. Now let's do another logical assumption after analyzing the ranges of the data: the coordinates are paired (x, y) in a two-dimensional space (in a plane). And it seems the values fit in a common screen resolution (by chance?) ;-)



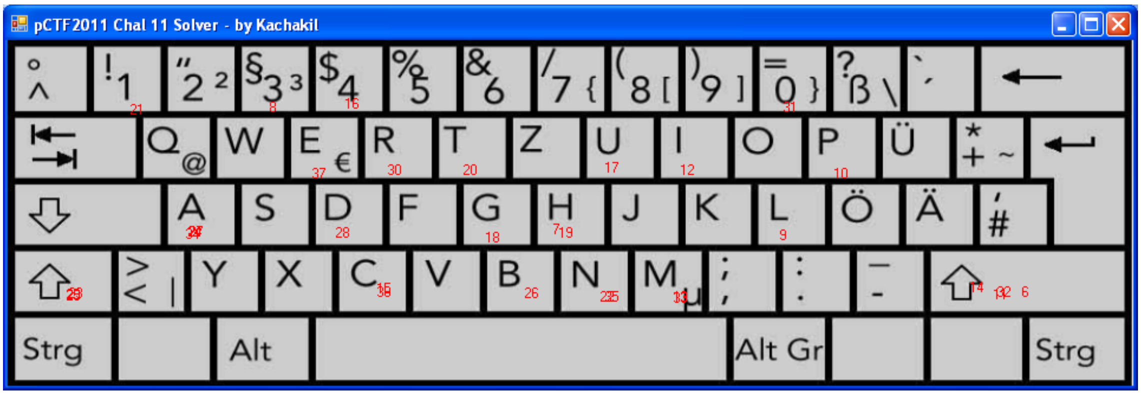
Wow! This plot seems to be very interesting, because the dots are clearly describing some kind of natural movement. We can assume that it's a mouse (or touchpad) moving across the screen, so the third column must be the state of the click button, right? Let's draw the dots which third column is 1 to see where these hypothetical clicks are.



I'm sure that I'm not the only one seeing a virtual keyboard behind these clicks… Ok, in the CTF I actually assumed this theory from the beginning and got to the solution quickly, without these drawings, but I'm describing here the analytical and logical path to the solution! :-)

Getting the solution

Well, if we are assuming that we're dealing with a virtual (on-screen) keyboard, then we only have to focus on the clicks, not on the movements. But the order is also very important, so let's draw a keyboard background numbering each click, to see what we will get.



pCTF2011 Chal 11 Solver - by Kachakil

The image is still a bit confusing, not only because of this awful keyboard layout, but because there are some numbers overlapped. Anyways, it seems that we're clearly on the right track, and it's trivial to animate the sequence pausing some seconds after each click to get a step-by-step solution.

The first key pressed is the "H" (click 7), the second is "3" (click 8), the third is "L" (9), the fourth "P" (10), and so on…

Flag of the challenge

h3lpimc4ught1nabadr0mance

Source code used

I know most of you hate this language (I don't understand why), but my code is in VB.NET… :-P

The file "keboard.jpg" used in this code was taken from here.

The file "data.txt" contains the last 3 columns of the original file (in my case, I stripped it with Excel). Notice that the final file of the challenge is not the one mirrored on shell-storm.

```
Private Sub Form_Load(...) Handles MyBase.Load
    Dim img As New Bitmap(1100, 600)
    Dim g = Graphics.FromImage(img)
    Me.Size = img.Size
    Me.BackgroundImage = img
    Me.Show()

    Dim keyboard As New Bitmap("keyboard.jpg")
```

```
        g.DrawImage(keyboard, 0, 0, 1100, 700)

        Dim n As Integer = 0
        Dim file = IO.File.ReadAllLines("data.txt")

        For Each line In file
            Dim data = line.Split(CChar(vbTab))
            Dim x = CInt(data(0))
            Dim y = CInt(data(1))
            Dim click = CBool(data(2))

            If click Then
                n += 1
                g.DrawString(n.ToString, Me.Font, Brushes.Red, x, y)

                Me.Refresh()
                Threading.Thread.Sleep(5000)
            End If
        Next
    End Sub
```

Acknowledgments

Thanks to the **PPP** team for this awesome CTF! Almost every single challenge was very original and funny the whole CTF was one of the best I've ever played. We're waiting for the next one!

And of course, thanks to all my **int3pids** teammates, because they're also really awesome!

Regards,
Daniel Kachakil
dani@kachakil.com