The New Age of Community Driven Distributed Computing

Dean Pierce :: ToorCon 14 :: 2012

Who am I?

- Infosec Professional
- Security Researcher
- Portland Native, Resident
- Bitcoin Hipster

- I love writing tools to arm children
- I wrote pickupline :-O
- Why are wireless talks so popular?

What am I Doing Here?

- (re)Launching hashbounty.net
  - aka : cracking WPA2 for bitcoins
  - appengine + python, bitcoind backend

- Some bitcoin stuff
- Some distributed computing stuff

The Bitcoin Slide

- Crypto currency
- Transactions are signed over with PKI
- Transactions cannot be reversed
- Transactions are globally distributed

- 50 coins distributed every ~10 minutes
- Pain in the ass to purchase
- Not for investment purposes

Ermegerd, Burtcern

The Process (sniffer)

prerequisites:

- Some spare bitcoins
- Proximity to a WPA2 network

The Process (sniffer)

Step 1 : Grabbing the handshake

- airmon-ng start wlan0 # creates mon0
- airodump-ng -w hax -t wpa2 mon0
- cap2hccap hax-01.cap crackme.hccap

The Process (sniffer)

Step 2 : Uploading the handshake

The Process (sniffer)

Step 3 : Funding the bounty

You have submitted a handshake for the network 'linksys'.

To fund the bounty, please send any number of bitcoins to 1QHiAUH9egh2RsmPaTw6gS8kuG9o4HaE87

The bounty will not appear until the transaction is verified, which can take around 30 minutes.

The bounty for 'linksys' has been funded.

Bounty is 0.234btc.

The Process (sniffer)

Step 4 : ???

The Process (sniffer)

Step 5 : PROFIT

The PSK is sent to you by email.

The bounty for 'linksys' has been solved.
The passphrase is 'dictionary'

The Process (cracker)

prerequisites:

- some fatty GPUs / rainbow tables / etc
- a bitcoin address to receive coins

The Process (cracker)

Step 1 : Find a good looking handshake

The Process (cracker)

Step 2 : Crack it

- oclHashcat-plus is good

The Process (cracker)

Step 3 : Submit solution to the service

- Coins are immediately sent to the cracker's bitcoin address

Why have I done this?

- To incentivize research in password cracking
- Capitalizing on the coming GPU surplus
- To PoC distributed bounty systems

The Future of Hashbounty?

- re-enabling md5, sha1
- adding MS-CHAPv2, a5/1 ?
- rss / xmpp feeds of new bounties
- end to end automation?
- expanding the bitcoin market
- establish a global network of bounty services
  - crypto, data, code, poetry, gifs
  - anyone remember webrings?

The Future of Computing?

- seti@home was nice
- BOINC took it to the next level
- Look what mining has done for sha256
- Bitcoins cure cancer

- Everyone has extra resources
- Anyone can figure out how to squeeze more performance from existing resources
- Cold silicon is a sin

* SLOW CLAP *

- hashbounty.net
- github.com/pierce403/hashbounty (old)

- Special Thanks
  - h1kari, jure, satoshi, hashcrack devs everywhere

* ROARING APPLAUSE *

- hashbounty.net
- github.com/pierce403/hashbounty (old)

- Special Thanks
  - h1kari, jure, satoshi, hashcrack devs everywhere

Questions Maybe?

- hashbounty.net
- github.com/pierce403/hashbounty (old)

- Special Thanks
  - h1kari, jure, satoshi, hashcrack devs everywhere