darknet.org.uk
Don't Learn to HACK - Hack to LEARN

crackle – Crack Bluetooth Smart Encryption (BLE)

February 20, 2017 | 724 views 0

crackle is a tool to crack Bluetooth Smart Encryption (BLE), it exploits a flaw in the pairing mechanism that leaves all communications vulnerable to decryption by passive eavesdroppers.

crackle can guess or very quickly brute force the TK (temporary key) used in the pairing modes supported by most devices (Just Works and 6-digit PIN). With this TK, crackle can derive all further keys used during the encrypted session that immediately follows pairing.

The LTK (long-term key) is typically exchanged in this encrypted session, and it is the key used to encrypt all future communications between the master and slave. The net result: a passive eavesdropper can decrypt everything. Bluetooth Smart encryption is worthless.

Modes of Operation

Crack TK

This is the default mode used when providing crackle with an input file using `-i`.

In Crack TK mode, crackle brute forces the TK used during a BLE pairing event. crackle exploits the fact that the TK in Just Works(tm) and 6-digit PIN is a value in the range [0,999999] padded to 128 bits.

Decrypt with LTK

In Decrypt with LTK mode, crackle uses a user-supplied LTK to decrypt communications between a master and slave. This mode is identical to the decryption portion of Crack TK mode.

Usage

```
# crack TK mode
$ crackle -i <file.pcap> -o <decrypted.pcap>
TK found: 412741
LTK found: 26db138f0cc63a12dd596228577c4730
Done, processed 306 total packets, decrypted 17

# decrypting future communications with the above LTK
$ crackle -i <file.pcap> -o <decrypted.pcap> -l 26db138f0cc63a12dd596228577c4730
Done, processed 373 total packets, decrypted 15
```

You can download crackle here:

crackle-0.1.zip

Or read more here.

Posted in: Exploits/Vulnerabilities, Hacking Tools, Network Hacking

ble, **ble encryption**, **bluetooth**, **bluetooth low energy**, **bluetooth security**, **bluetooth smart**, **crack ble**, **crack bluetooth smart**, **crackle**, **decrypt ble encryption**

Recent in Exploits/Vulnerabilities:
- 160,000 Network Printers Hacked
- OWASP VBScan – vBulletin Vulnerability Scanner
- p0wnedShell – PowerShell Runspace Post Exploitation Toolkit

Related Posts:
- BlueMaho Project – Bluetooth Security Testing Suite
- Haraldscan – BlueTooth Discovery Scanner
- BlueScan – A Bluetooth Device Scanner

Most Read in Exploits/Vulnerabilities:
- Learn to use Metasploit – Tutorials, Docs & Videos - 237,152 views
- AJAX: Is your application secure enough? - 120,479 views
- eEye Launches 0-Day Exploit Tracker - 86,002 views

‹ ONIOFF – Onion URL Inspector

No comments yet.

Leave a Reply

B | I | LINK | B-QUOTE | DEL | INS | IMG | UL | OL | LI | CODE | MORE | CLOSE TAGS | CRAYON

Name (required)

Email (will not be published) (required)

Website

SUBMIT COMMENT

Search Darknet

Search...

Subscribe

Subscribe via e-mail for updates!

Enter your e-mail

SUBSCRIBE ME!

7932 readers BY FEEDBURNER 5427 email readers BY FEEDBLITZ

Follow 34,793

Like Zih-Ling Chen and 12K others like this.

Follow @THEdarknet 16.5K followers

TRENDING LATEST POSTS TAGS

Stitch – Python Remote Administration Tool AKA RAT
FEBRUARY 10, 2017 - 137 LIKES

160,000 Network Printers Hacked
FEBRUARY 9, 2017 - 117 LIKES

OWASP VBScan – vBulletin Vulnerability Scanner
JANUARY 28, 2017 - 107 LIKES

dns2proxy – Offensive DNS server
JANUARY 24, 2017 - 78 LIKES

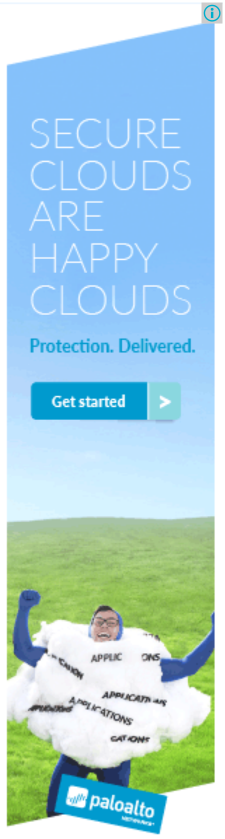
ONIOFF – Onion URL Inspector
FEBRUARY 17, 2017 - 67 LIKES

Why Are Hackers Winning The Security Game?
FEBRUARY 15, 2017 - 54 LIKES

Navigation

- About Darknet
- Popular Posts
- Darknet Archives
- Darknet Tags
- Hack Tools/Exploits
- Contact Darknet

Advertisements



Who is protecting your website?
Sucuri's Website Security Stack solution provides your website complete end-to-end security.
LEARN MORE
sucuri
Real People. Real Security.

Users Online

25 Users Online

Recent Articles

- crackle – Crack Bluetooth Smart Encryption (BLE)
- ONIOFF – Onion URL Inspector
- Why Are Hackers Winning The Security Game?
- hashID – Identify Different Types of Hashes
- Stitch – Python Remote Administration Tool AKA RAT
- 160,000 Network Printers Hacked
- Abbrase – Abbreviated Passphrase Password Generator
- Webbies Toolkit – Web Recon & Enumeration Tools
- Dark Web Paying Corporate Workers To Leak Info
- Barnyard2 – Dedicated Spooler for Snort Output

Topics

- Advertorial (38)
- Apple (46)
- Countermeasures (212)
- Cryptography (68)
- Database Hacking (86)
- Events/Cons (7)
- Exploits/Vulnerabilities (411)
- Forensics (66)
- General Hacking (180)
- General News (124)
- Hacking Tools (612)
- Hardware Hacking (74)
- Legal Issues (170)
- Linux Hacking (75)
- Malware (230)
- Network Hacking (355)
- Old Skool Philes (7)
- Password Cracking (102)
- Phishing (40)
- Privacy (212)
- Programming (115)
- Retards (6)
- Security Software (212)
- Site News (50)
  - Authors (6)
- Social Engineering (35)
- Spammers & Scammers (76)
- Telecomms Hacking (6)
- UNIX Hacking (6)
- Virology (6)
- Web Hacking (404)
- Windows Hacking (174)
- Wireless Hacking (39)

Security Blogs

- Dancho Danchev
- F-Secure Weblog
- Google Online Security
- Internet Storm Center
- Krebs on Security
- Mckeay
- PaulDotCom
- Schneier on Security
- SecuriTeam Blog
- TaoSecurity
- Tech Republic Security

Security Links

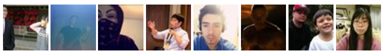
- Exploits Database
- Linux Security
- NetworkWorld – Security
- Register – Security
- SANS
- Sec Lists
- Security Focus
- US CERT

Facebook

Darknet.org.uk

Like Page 12K likes

4 friends like this



Darknet.org.uk
14 hrs

crackle is a Bluetooth hacking tool aimed at Bluetooth Smart or BLE encryption, it can brute force the TK used during pairing and also decrypt with LTK - Darknet.org.uk

crackle - Crack Bluetooth Smar...

crackle is a tool to crack Bluetooth Smart Encr

Twitter Updates

Tweets by @THEdarknet

Darknet.org.uk
@THEdarknet

New Post: crackle – Crack Bluetooth Smart Encryption (BLE) ift.tt/2m0pgcR

14h

Darknet.org.uk
@THEdarknet

New Post: ONIOFF – Onion URL Inspector ift.tt/2lezrYi

```
root@kali:~/onioff# python onioff.py -f ~/onions.txt -o ~/report.txt
```

Embed View on Twitter

Privacy Policy