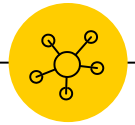
# Стандартни алгоритми за WiFi пароли + PoC




Александър Станев

@RealEnderSec
alex@stanev.org
https://github.com/RealEnder
https://wpa-sec.stanev.org

## Въведение

Често WiFi рутерите идват с предварително зададена парола за безжичната мрежа:

- Нови off-the-shelf WiFi рутери
- Устройства, предоставени от ISP

Това включва не само WPA-PSK, но и WPS PINs, достъп до административния интерфейс на устройството

## Как се създават тези пароли?

В много от случаите:

- Използване на налични в устройството уникални параметри като seed:
  - BSSID / WAN MAC
  - Serial Number
- Обфускиращ алгоритъм, който генерира SSID, WPA-PSK паролата, WPS PIN...

## Алгоритмите

- Стрингови операции/математически операции
- Заместващи таблици
- Hash функции
- Алгоритми за генериране на псевдо случайни числа (PRNGs)
- Споделени речници

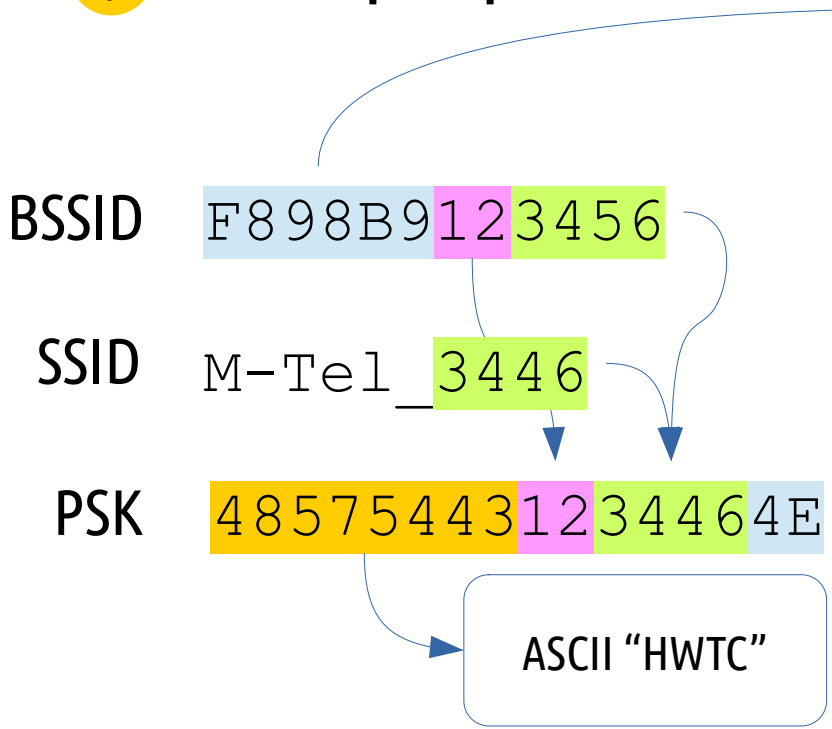
## Как се откриват

- Наблюдение на вече известни пароли
  - Снимки в сайтове за продажба
  - “Счупени” пароли във wpa-sec.stanev.org
- Техническа документация и патенти
- Модифициране на сходни алгоритми от същия производител
- Reverse engineering на firmware

# PoC – Huawei routers

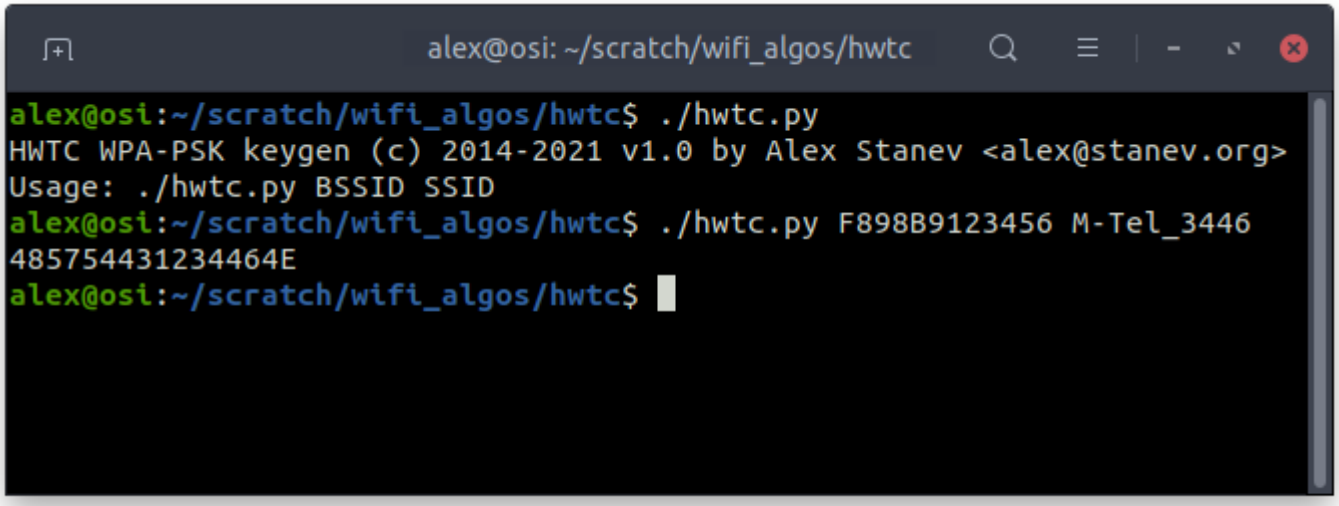
- Известен от 2013 г.
- Използва се в мрежи със следните SSID маски:
  - A1-XXXX
  - A1_XXXX
  - M-Tel_XXXX
  - CLAROXXXXX
  - HUAWEI-XXXX
- Някои устройства използват вариация на алгоритъма
- Първи прихванат handshake във wpa-sec: 2012 г.

# PoC – Пример




| OUI | Last |
|---|---|
| 049FCA | 7C |
| 08C021 | 73 |
| 104780 | 13 |
| 203DB2 | 81 |
| 48435A | 79 |
| ... | ... |
| E09796 | 31 |
| F02FA7 | 88 |
| F09838 | 89 |
| F898B9 | 4E |

# PoC – hwtc.py




https://github.com/RealEnder

## Още алгоритми

- RouterKeygenPC
  https://github.com/routerkeygen/routerkeygenPC
- hcxtools / hcxpsktool
  https://github.com/ZerBea/hcxtools
- wpa-sec
  https://wpa-sec.stanev.org

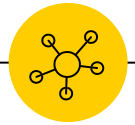
Имате идеи? Обичате математически пъзели? Пишете!

## Мерки

- Винаги променяйте фабричните пароли
- Сменяйте паролата за мрежата си поне веднъж годишно
- Използвайте WPA3-SAE aka Wi-Fi 6
- Избягвайте ISP, които предоставят “заключени” устройства
- WIDS / WIPS / WPA-Enterprise

# Стандартни алгоритми за WiFi пароли + PoC

# Благодаря за вниманието!




Александър Станев

@RealEnderSec
alex@stanev.org
https://github.com/RealEnder
https://wpa-sec.stanev.org