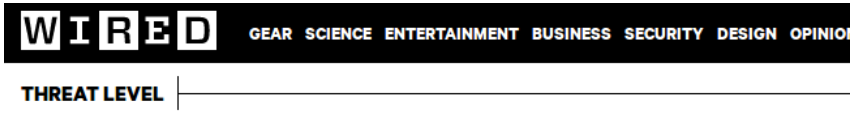
Rickrolling your Neighbors with Google Chromecast

Dan “AltF4” Petro

July 18, 2014

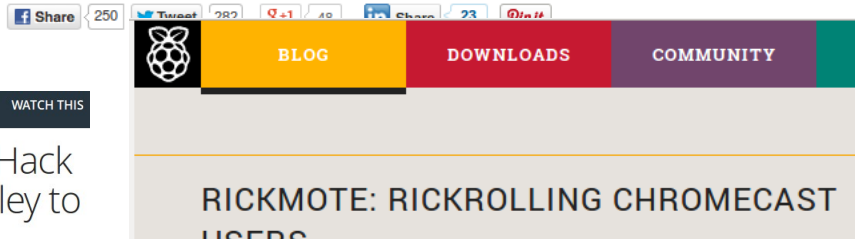
Media Blitz

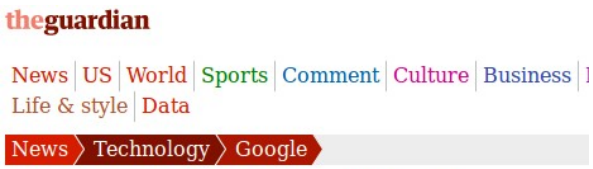
TEH INTERTUBES

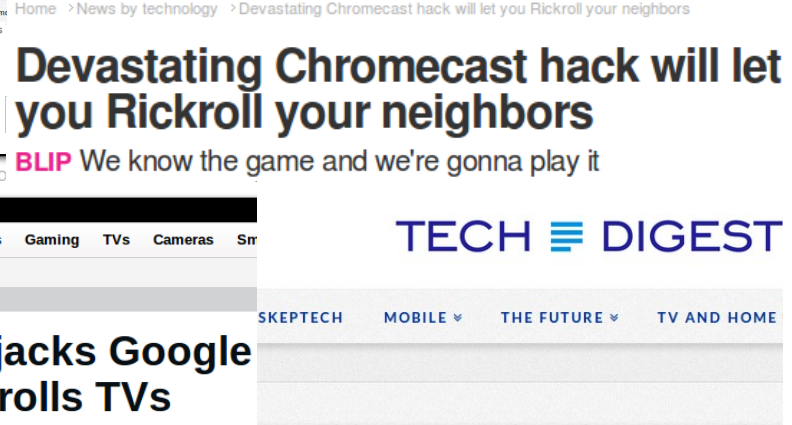


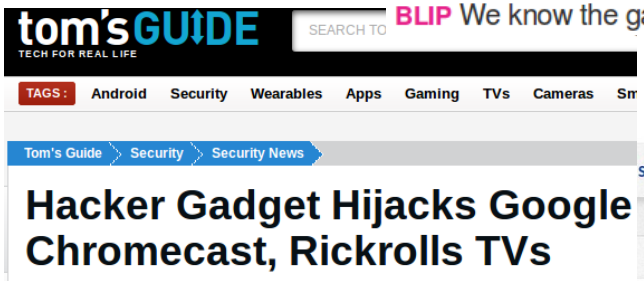
Rickroll Innocent Televisions With This Google Chromecast Hack

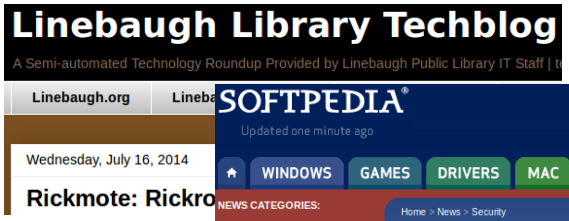
BY ANDY GREENBERG 07.16.14 | 6:30 AM | PERMALINK





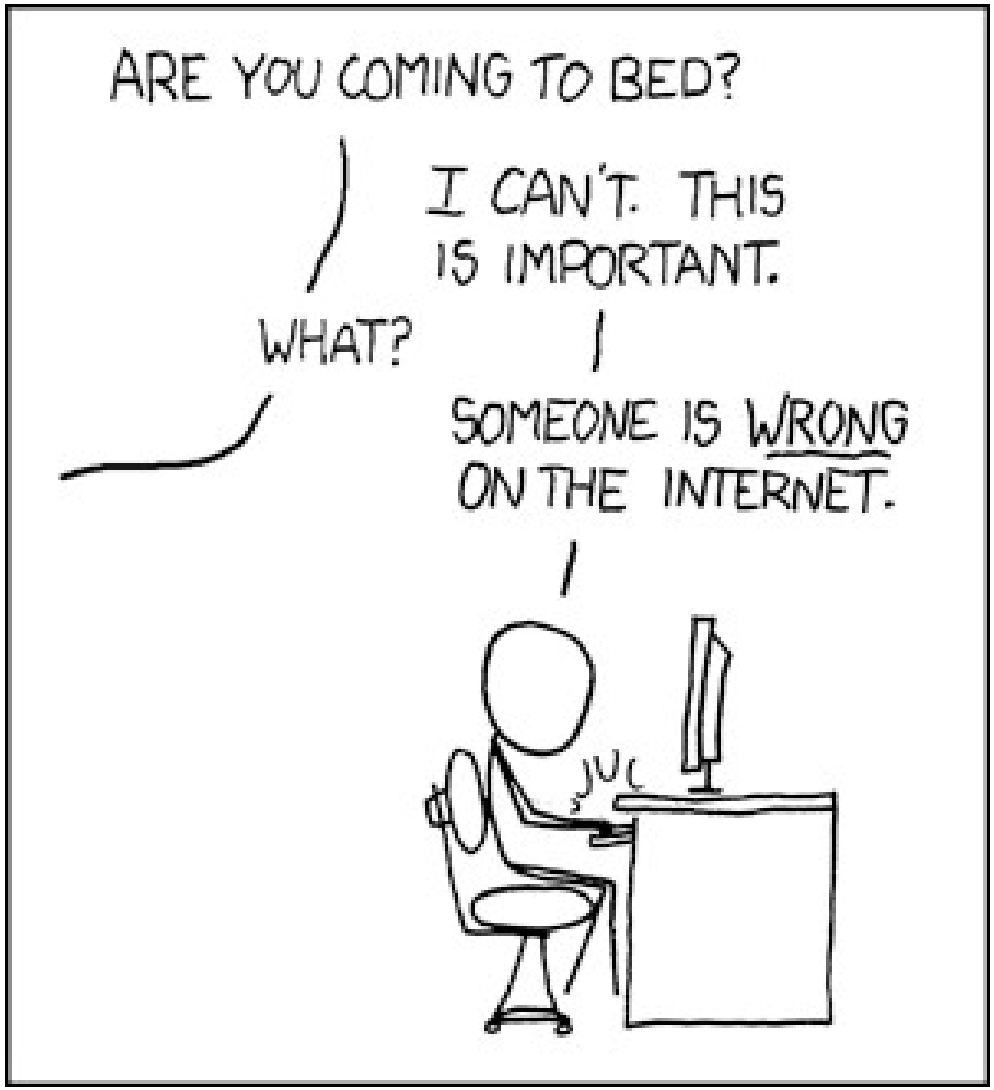






The Last 48 Hours

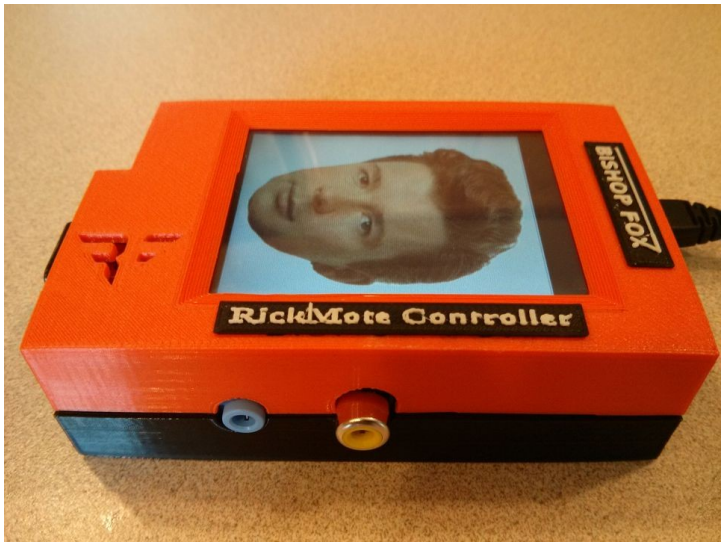
XKCD



Hijacking TVs

THE **RICK**MOTE CONT**ROLL**ER

- Classic Hack from the movies
- Take over someone's TV
- Raspberry Pi
  - Touchscreen
  - USB Wi-Fi NICs
  - 3D Printed Case
  - ~$100 parts



Hijacking TVs

HOLLYWOOD STYLE

Hijacking TVs

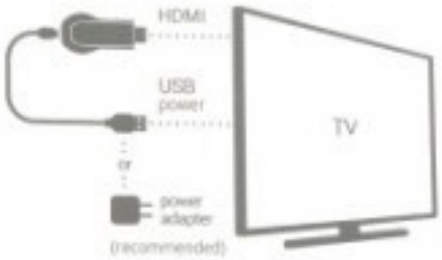
REAL WORLD

Google Chromecast

- Internet TV Gadget
- Plugs into TV
  - HDMI
- Connects to Wi-Fi
- Streams video
  - Netflix, YouTube, etc...

getting started

1. plug it in



2. switch input

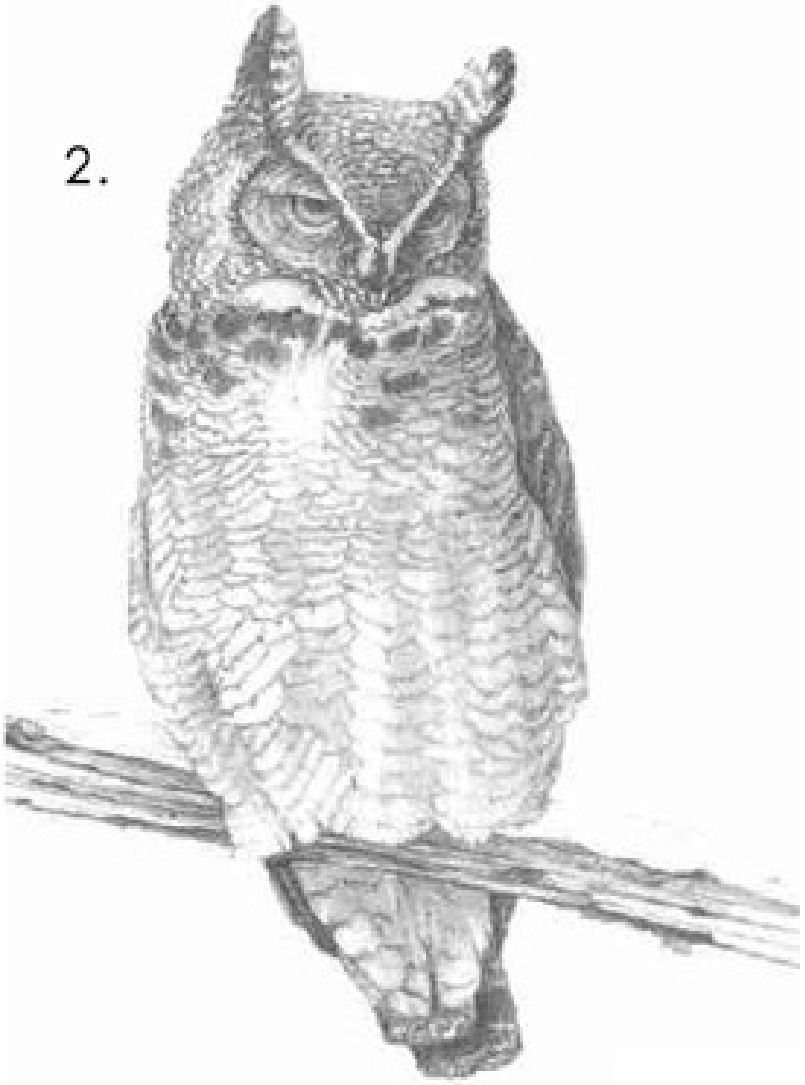
switch tv input/source until you see this

3. set it up **google.com/chromecast/setup**

How to draw an owl

1.

2.



1. Draw some circles

2. Draw the rest of the fucking owl

Simple Device

A LITTLE TOO SIMPLE...

- HDMI Port
  - Plugs into TV, duh
- USB Port
  - Power only, do data
- Single Button
  - Factory reset

Chromecast Setup

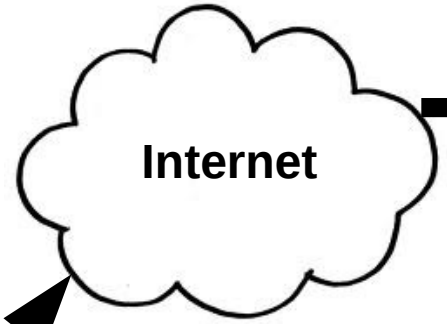
User

Internet

Key = Unbr34k4bl3

Chromecast Setup

User



SSID: Chromecast

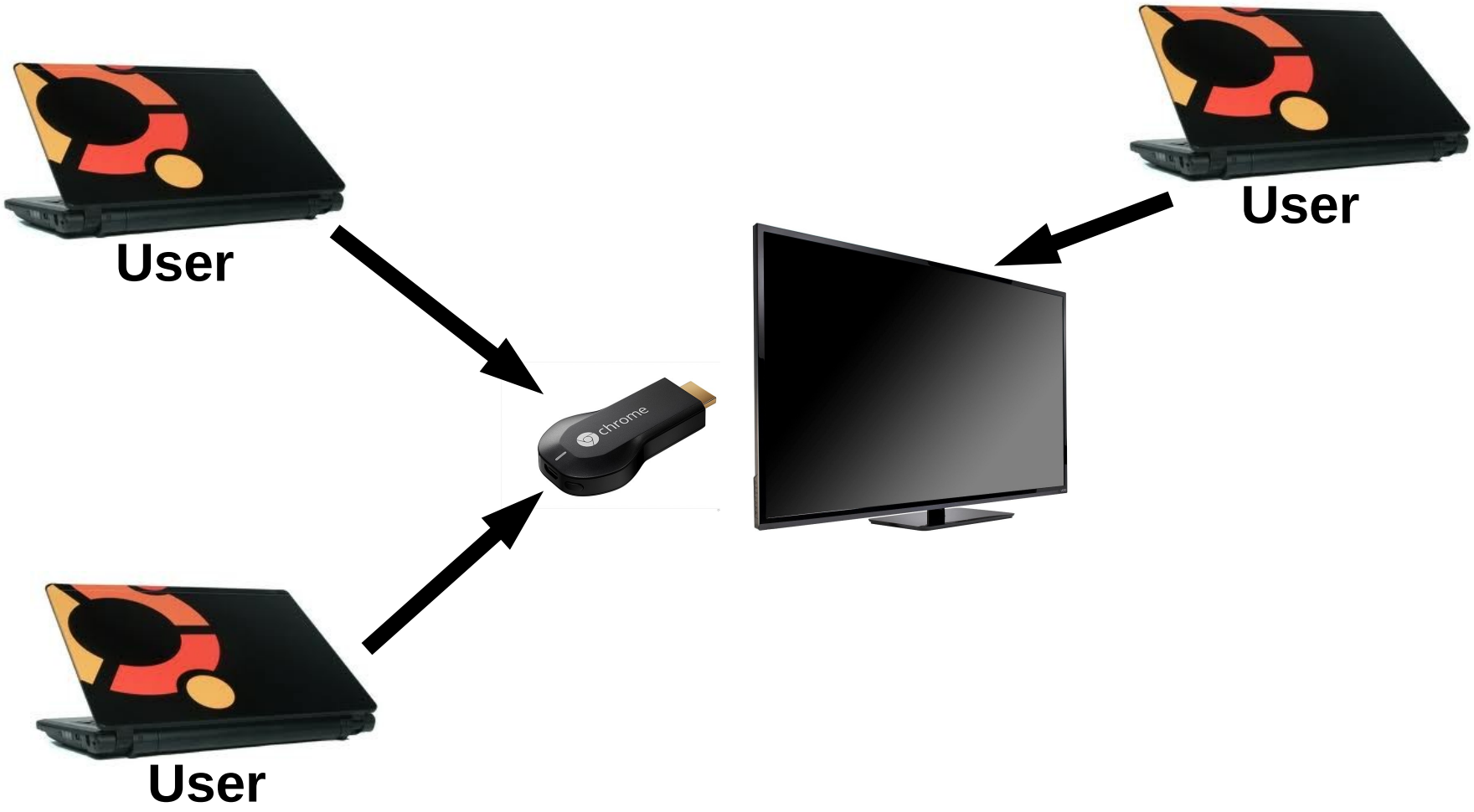
Key = Unbr34k4bl3

Chromecast Security Model

CANDY SECURITY

- Crunchy outer shell
- Gooey Inside
- One-time insecure setup

Open Interior



Secure Perimeter

User

Key = Unbr34k4bl3

Race Condition

Victim / User

LAME

SSID: Chromecast

Not Bad

SECURE?

- SSH-Like Security Model
- One-Time Insecure Setup
- Secure future operation

Hold on a sec...

IT DOES WHAT NOW?!

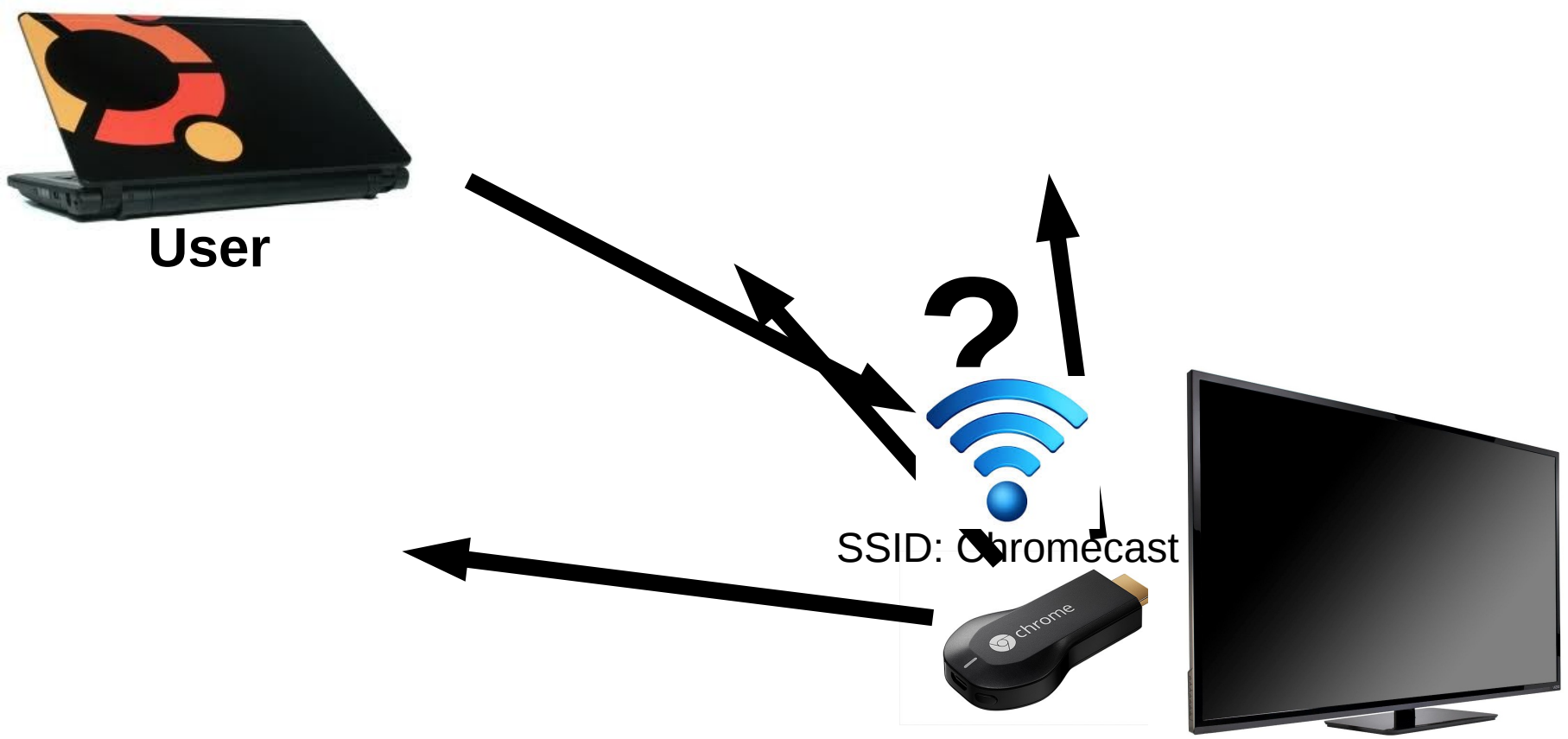
- Official Chromecast FAQ:
  - **Question**: Can I take Chromecast with me to use when I travel?
  - **Answer**: **Yes, Chromecast was built with portability in mind**. You can bring it with you when you travel, but keep in mind that **you will need Wi-Fi access to set up and use Chromecast**.

On Vacation

1. Trying to connect to your hotel's Wi-Fi...
2. How does Chromecast know that you're on travel?
3. **When it can't connect to your home Wi-Fi**

Vacation

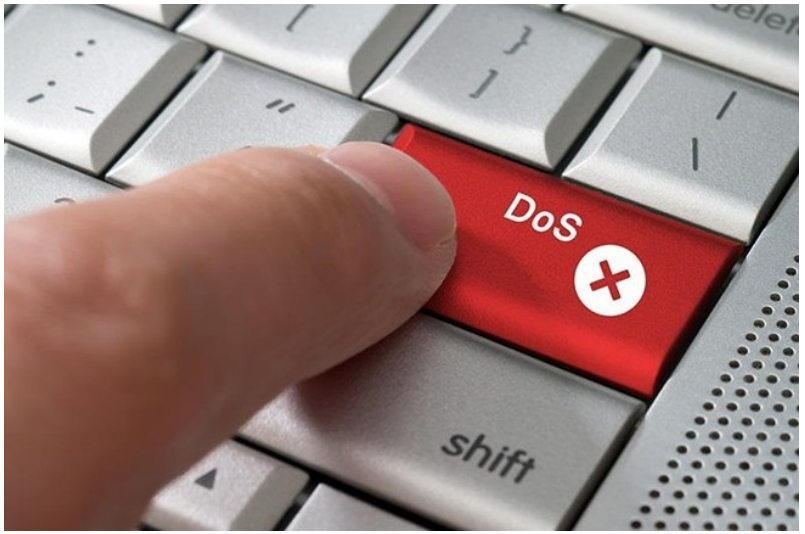
WHERE DID YOU GO?



Forced Vacation

ANYTIME I WANT

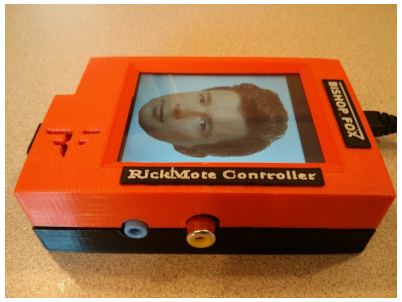
- Wi-Fi De-Authentication
  - Tells clients to disconnect
- Unencrypted
  - Clients may not be authenticated!
- Anyone can spoof
- Clients will disconnect!



The Attack

User

Internet



De-Authenticate

Key = Unbr34k4bl3

D: Chromecast

Automation

FUMBLING WITH WIRES IS NO FUN

- Popping the Chromecast AP is not enough
  - Need to also push video!
  - How does that happen?
- Little details available
  - Reverse Engineering!

Chromecast AP

INFO DUMP

- Open Wi-Fi
  - No authentication or encryption
- Chromecast at 192.168.255.249
- Web Server on TCP port 8008
- Some interesting services:
  - **/setup/eureka_info**
  - /setup/scan_wifi
  - /setup/scan_results
  - **/setup/connect_wifi**

Chromecast AP

EUREKA!

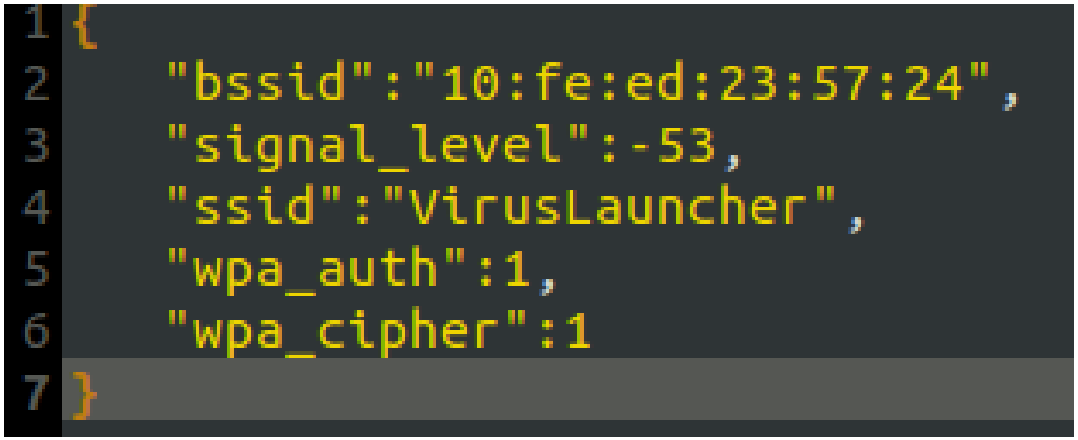
- **/setup/eureka_info**
- Friendly Name
- Public Key
- Current SSID
- Software Version
- Etc...


```
{
   "build_version":"17250",
   "connected":true,
   "has_update":false,
   "hdmi_control":true,
   "hotspot_bssid":"FA:8F:CA:3C:6E:B7",
   "ip_address":"192.168.43.32",
   "locale":"en-US",
   "location":{
      "country_code":"US",
      "latitude":255.0,
      "longitude":255.0
   },
   "mac_address":"D0:E7:82:BD:7D:22",
   "name":"Dancast",
   "noise_level":-87,
   "opt_in":{
      "crash":true,
      "device_id":false,
      "location":false,
      "stats":true
   },
   "public_key":"MIIBCgKCAQEAvjfUx1fGXlz+mw4LvO
+Mu9QvGqRG9RWNdsOrlljFRl3U2gs2bOcsgFclgASvQDFbPw5coYTU1XQZuXvyNthT520
+OWvSZsXzoh885f2MBZhQW2fYmBwt+64FJElLzwFjKWvhtZElWbx6gxoMN355PuouGbcw
+6SZWmGUyHed6YqtDuoJ00kt9kSs1zf4f0BEgoTQVa4KVzn0sATNU90QyOikJMJ0WviYw7
aPVngepzpPUj6CDxnGhigEzaapMkf3/2flBuvuM9EuNRqpQIDAQAB",
   "release_track":"stable-channel",
   "setup_state":61,
   "signal_level":-58,
   "ssdp_udn":"46d8f4b0-de65-edf3-5634-9cb347b57e14",
   "ssid":"VirusLauncher",
   "time_format":1,
   "timezone":"America/Phoenix",
   "uma_client_id":"E0177EE4-5CC2-E22C-D59E-7B63DB0FB546",
   "uptime":2741.51,
   "version":4,
   "wpa_configured":true,
   "wpa_id":12,
   "wpa_state":10
}
```

Swapping Connections

GET OVER HERE!

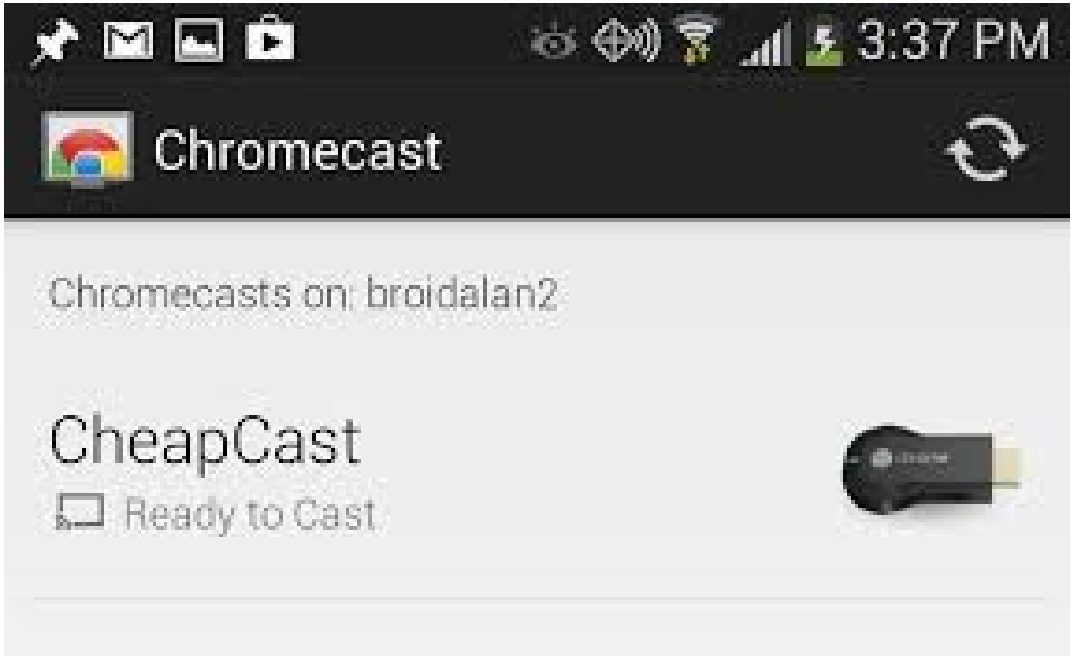
- **/setup/connect_wifi**
- JSON POST
- Wi-Fi keys are encrypted
  - With public key from eureka_info



Chromecast Discovery

SHOUT LOUDER

- Chromecast is on your network
  - Where?
- DIAL
  - SSDP
  - UDP
  - Port 1900
  - Multicast
- 239.255.255.250



Apps

- Two Halves: **Client** and **Server**
- **Server** apps run on the Chromecast
  - Submitted to Google
  - Code inspected (maybe)
  - Code signed
  - /apps/NAME_OF_APP
- **Client** apps run on your computer
  - Android / iOS / Web / Desktop

YouTube App

- /apps/YouTube
- Play YouTube video by POST
  - Content-Type: application/x-www-form-urlencoded

- **pairingCode**=2c726059-d6f5-4a64-803a-248f9059d1fb&**v**=**dQw4w9WgXcQ**&**t**=3

Persistence

THE LONG PLAY

- Advanced Persistent Neighbor
- Rather than a temp “Rickmote” Wi-Fi
  - Config Chromecast for your home Wi-Fi
  - Attacker network doesn't leave
  - CC'ast has a new home
- Non-technical user will have no way to undo!

Coming Soon

TO A TV NEAR YOU

- **Internet Connection**
  - Rickmote plays YouTube
  - From the Internet
  - Would be nice to cut the cord
- **Three Wi-Fi NICs**
  - Monitor mode (de-auth)
  - Managed mode (connect to CC'ast AP)
  - Master mode (CC'ast connect back to us)

Coming Soon

TO A TV NEAR YOU

- **General Rudeness**
  - Rickmote de-auth's everything in range
  - Everything
  - Over and over
  - There has to be a more targeted way
- **Identifying Chromecast networks**
  - The official Android app does it quick
  - Faster than the Rickmote does it
  - What is it doing?!

Remediation

MAYBE NOT POSSIBLE

- No good options
- **Screen Code**
  - Not used for security
  - Only accidental mistakes
- Suggestion
  - Re-purpose as security code
  - Require user to enter code on setup
- Cons:
  - Short code is brute force-able
  - Even a short code may be a pain to use

Remediation (cont'd)

MAYBE NOT POSSIBLE

- **Physical Device Interaction**
  - Require **button** to be **pressed**
  - Chromecast DOES have a button!
  - Setup will ask for user to press button
- Cons:
  - What if the user can't reach!
  - Some setups will be buried
  - Button malfunction (common problem)

Remediation (cont'd)

MAYBE NOT POSSIBLE

- **Config only on boot-up**
  - Chromecast only acts as AP on boot
  - Requires user to power cycle device
- Cons:
  - A huge pain
  - Unintuitive
  - Getting physical access may be hard

Remediation (cont'd)

MAYBE NOT POSSIBLE

- **Ignore De-Authenticate Packets**
  - Resistant to easy DoS attack
- Cons:
  - Breaks Wi-Fi spec
  - Doesn't really fix anything
  - Other DoS attacks exist
  - Flood the 2.4 Ghz spectrum

Thanks!

Questions