

Rickrolling your Neighbors with Google Chromecast

Dan "AltF4" Petro

July 18, 2014



THREAT LEVEL | _____

Rickroll Innocent Televisions With This Google Chromecast Hack

BY ANDY GREENBERG 07.16.14 | 6:30 AM | PERMALINK

Share 250 Tweet 282 +1 40 +3 23 0/0

 **BLOG** **DOWNLOADS** **COMMUNITY**

RICKMOTE: RICKROLLING CHROMECAST

techradar TECHNOLOGY, TESTED

Home Reviews Phones TVs Cameras Laptops Tablets Car Tech Down

TRENDING Amazon Fire Phone Galaxy Tab S OnePlus One LG G3 HT

Home > News by technology > Devastating Chromecast hack will let you Rickroll your neighbors

Devastating Chromecast hack will let you Rickroll your neighbors

BLIP We know the game and we're gonna play it

TECH DIGEST

SKEPTECH MOBILE THE FUTURE TV AND HOME

Share US | 4 COMMENTS

Chromecast bug enables Rickrolling

 1

Media Blitz

TEH INTERTUBES

theguardian

News | US | World | Sports | Comment | Culture | Business | Life & style | Data

News > Technology > Google

How to Rickroll any TV using Chromecast flaw

Security researcher Dan Petro has developed the 'Rickmote', which uses a flaw in Chromecast's wireless to push any video to the streaming stick

GIZMODO UK UK NEWS GADGETS DESIGN WATCH THIS

"Rickmote" Chromecast Hack Brings Unauthorised Astley to Wired TVs

By Gary Cutlack on 17 Jul 2014 at 4:45AM

PCWorld Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES

Antivirus Privacy Encryption

SECURITY hardware, raspberry pi, chromecast, security

Rick-rolling 'Rickmote' shows no mercy when it finds

Linebaugh Library Techblog

A Semi-automated Technology Roundup Provided by Linebaugh Public Library IT Staff | t

Linebaugh.org Linebaugh

Wednesday, July 16, 2014

Rickmote: Rickro

NEWS CATEGORIES:

- Google I/O 2014
- NSA & Edward Snowden
- Latest News
- Oddiverse
- Laptops & Tablets
- NEW! 3D Printing

PC ADVISOR EXPERT ADVICE YOU

NEWS REVIEWS HOW-TO FORUMS ADVISORS VIDEOS DOW

Search News... You are here: > Homepage > News > The Rickmote 78,230 News Articles

The 'Rickmote' shows no mercy when it finds someone using Chromecast

A Raspberry-Pi powered tool tricks Google Chromecast into playing Rick Astley

By Jeremy Kalk | 17 July 14

tom'sGUIDE TECH FOR REAL LIFE

SEARCH TO

TAGS: Android Security Wearables Apps Gaming TVs Cameras Sr

Tom's Guide > Security > Security News

Hacker Gadget Hijacks Google Chromecast, Rickrolls TVs

Share US | 4 COMMENTS

Rickmote Controller Hijacks Nearby Chromecasts

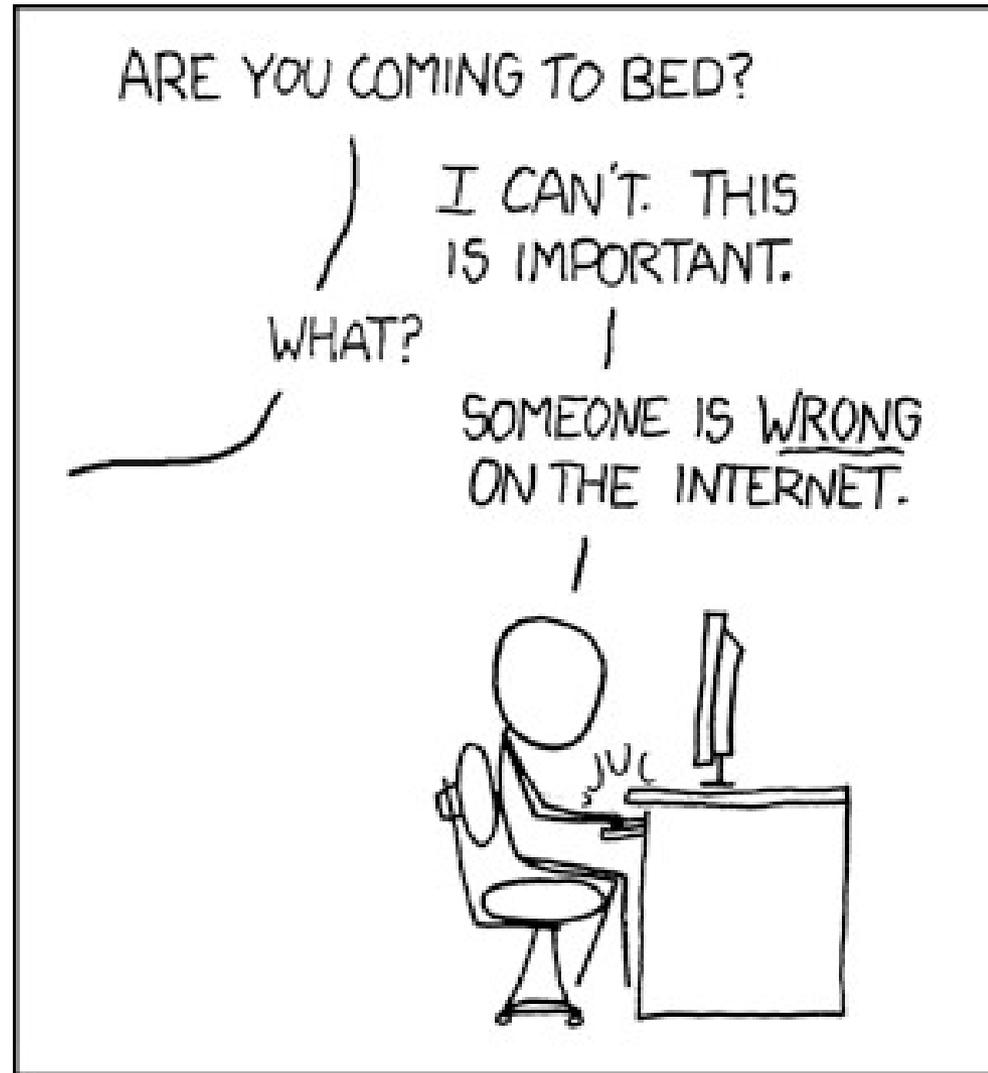
July 17th, 2014, 12:04 GMT - By Jonut Rescu

SHARE: 

Adjust text size: 

The Last 48 Hours

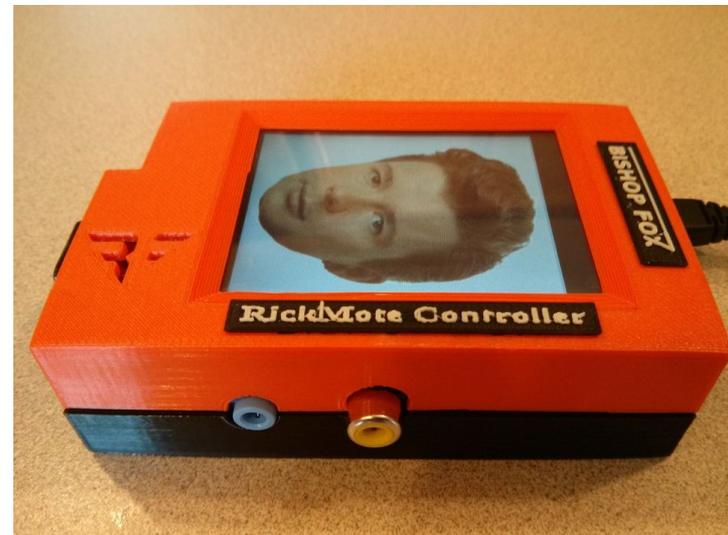
XKCD



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



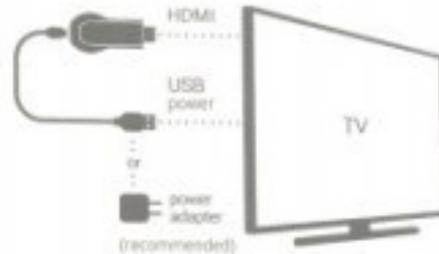
Google Chromecast

- 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

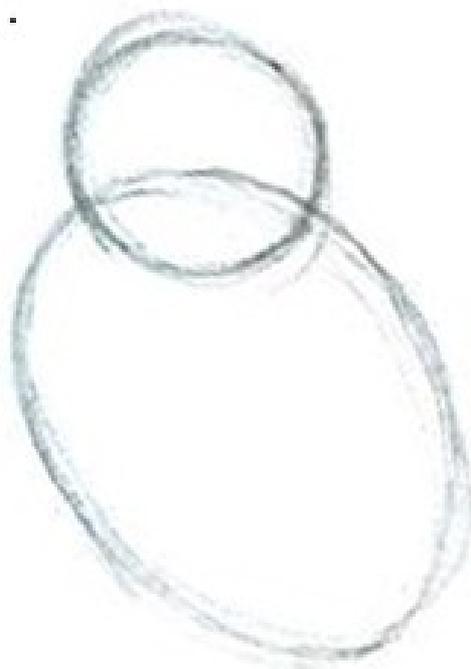


switch tv input/source until you see this

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

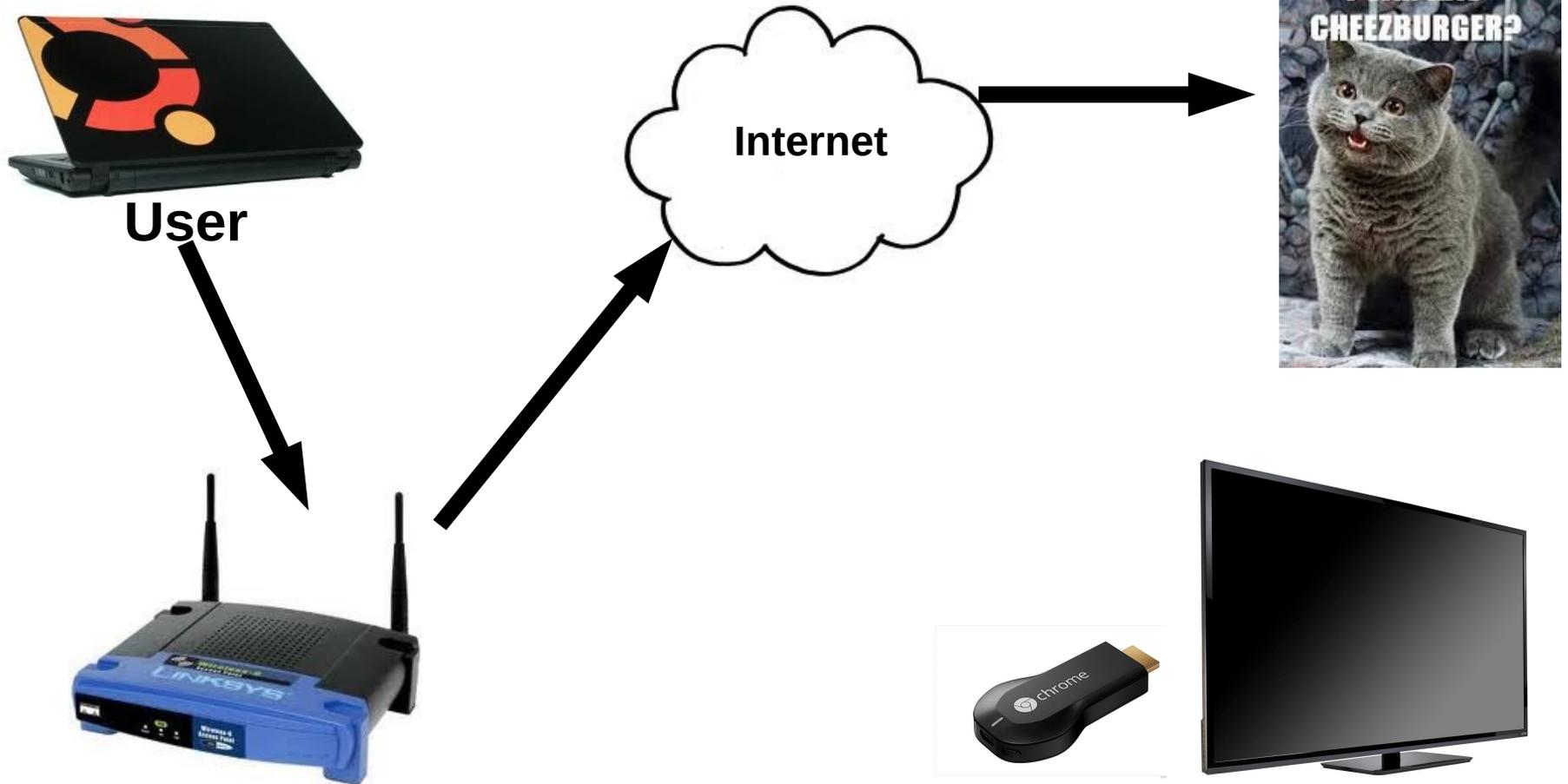
A LITTLE TOO SIMPLE...

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



COURTESY: GOOGLE

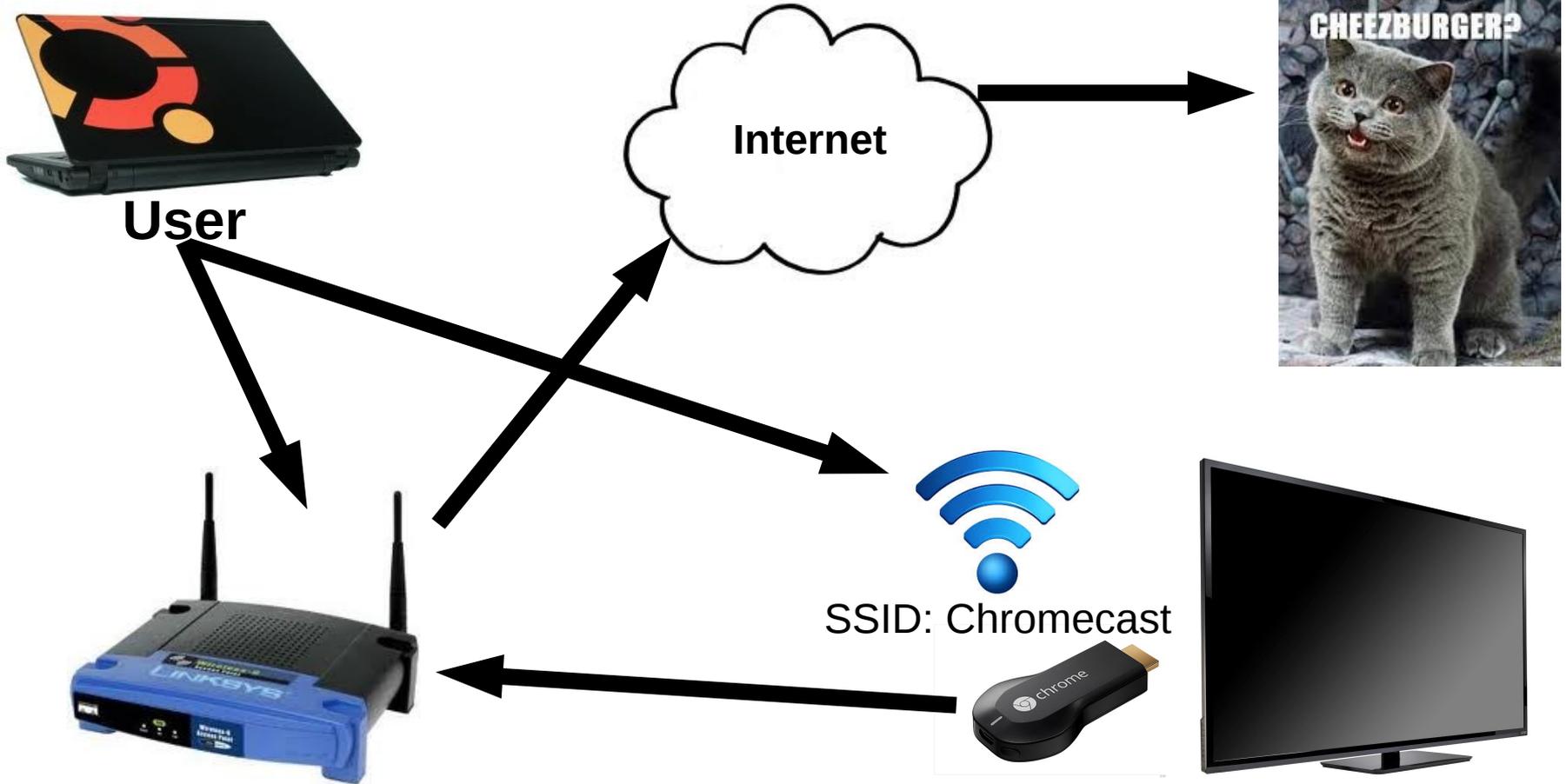
Chromecast Setup



Key = Unbr34k4bl3



Chromecast Setup



Key = Unbr34k4bl3



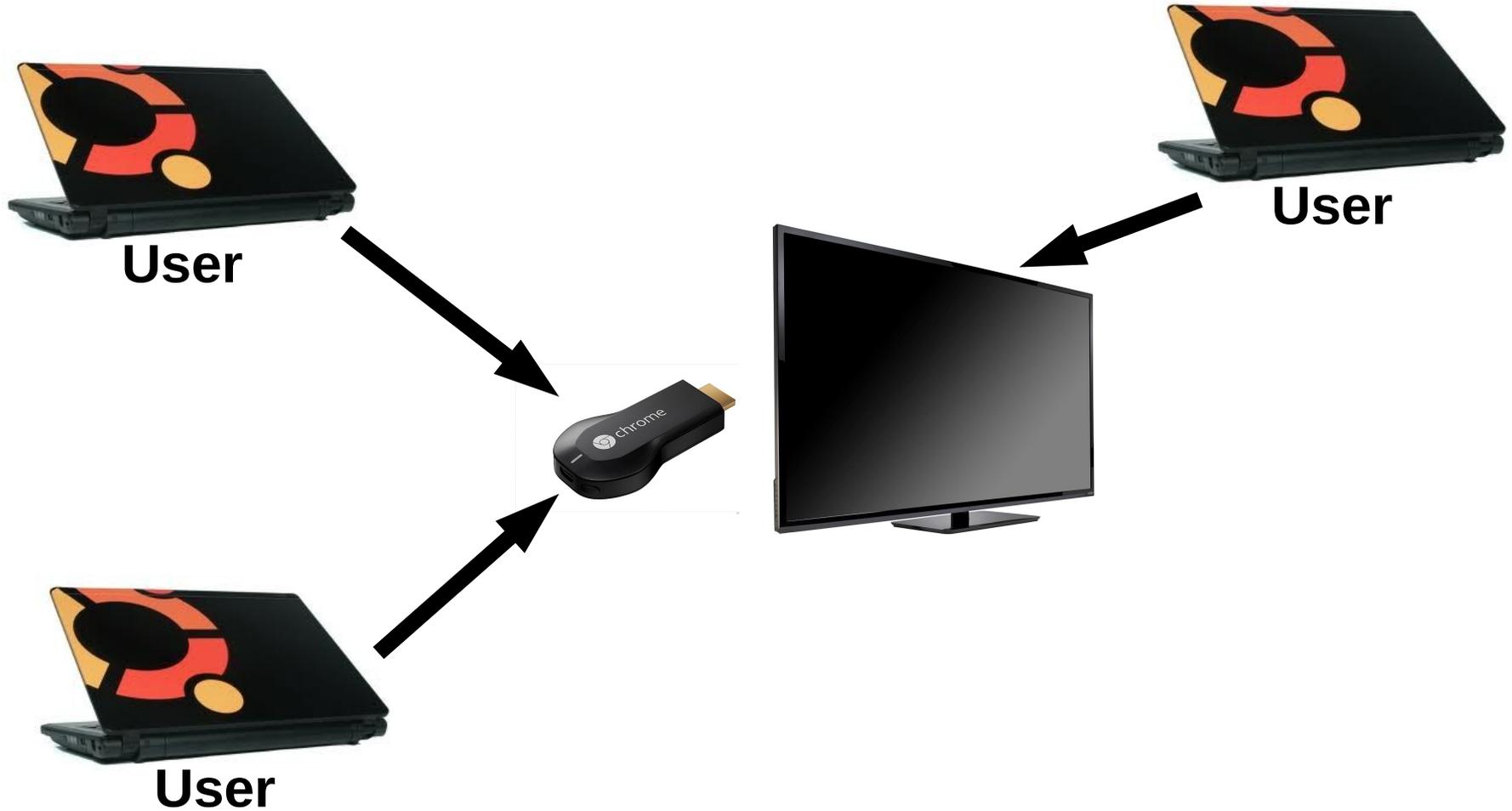
Chromecast Security Model

CANDY SECURITY

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



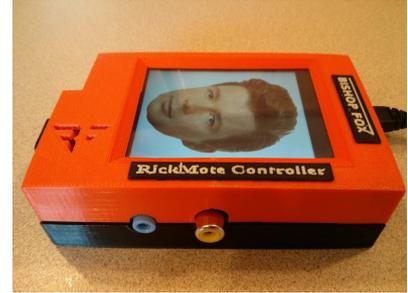
Open Interior



Secure Perimeter



User



Key = Unbr34k4bl3



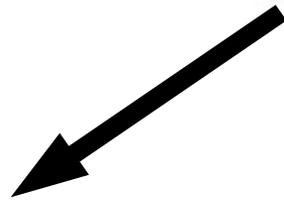
Race Condition



Victim / User



LAME



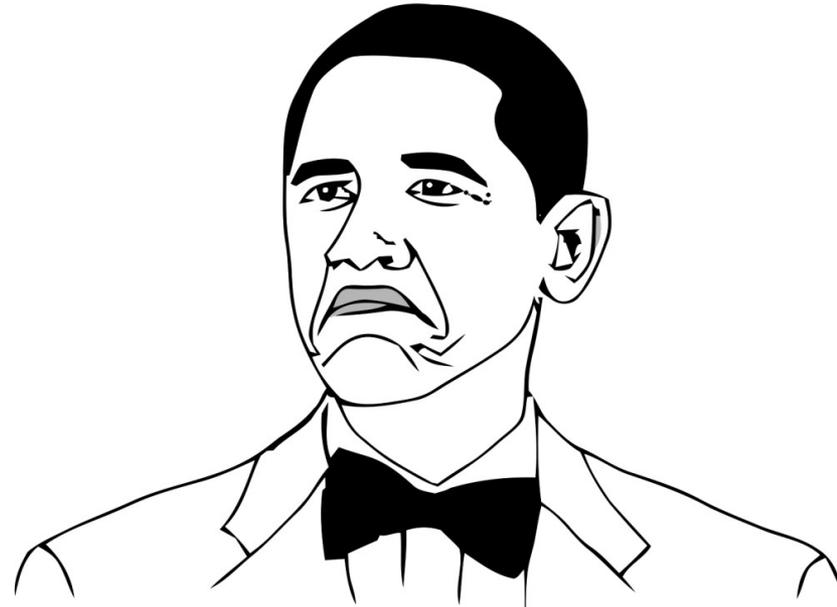
SSID: Chromecast



Not Bad

SECURE?

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



NOT BAD

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?



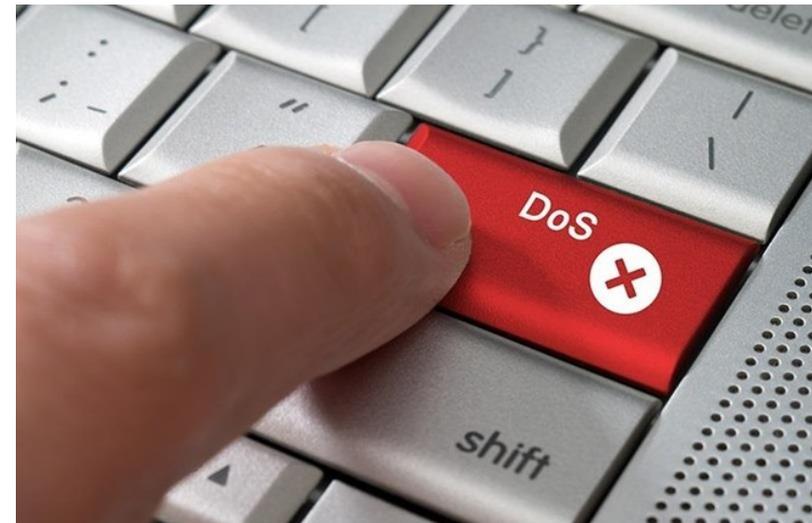
User



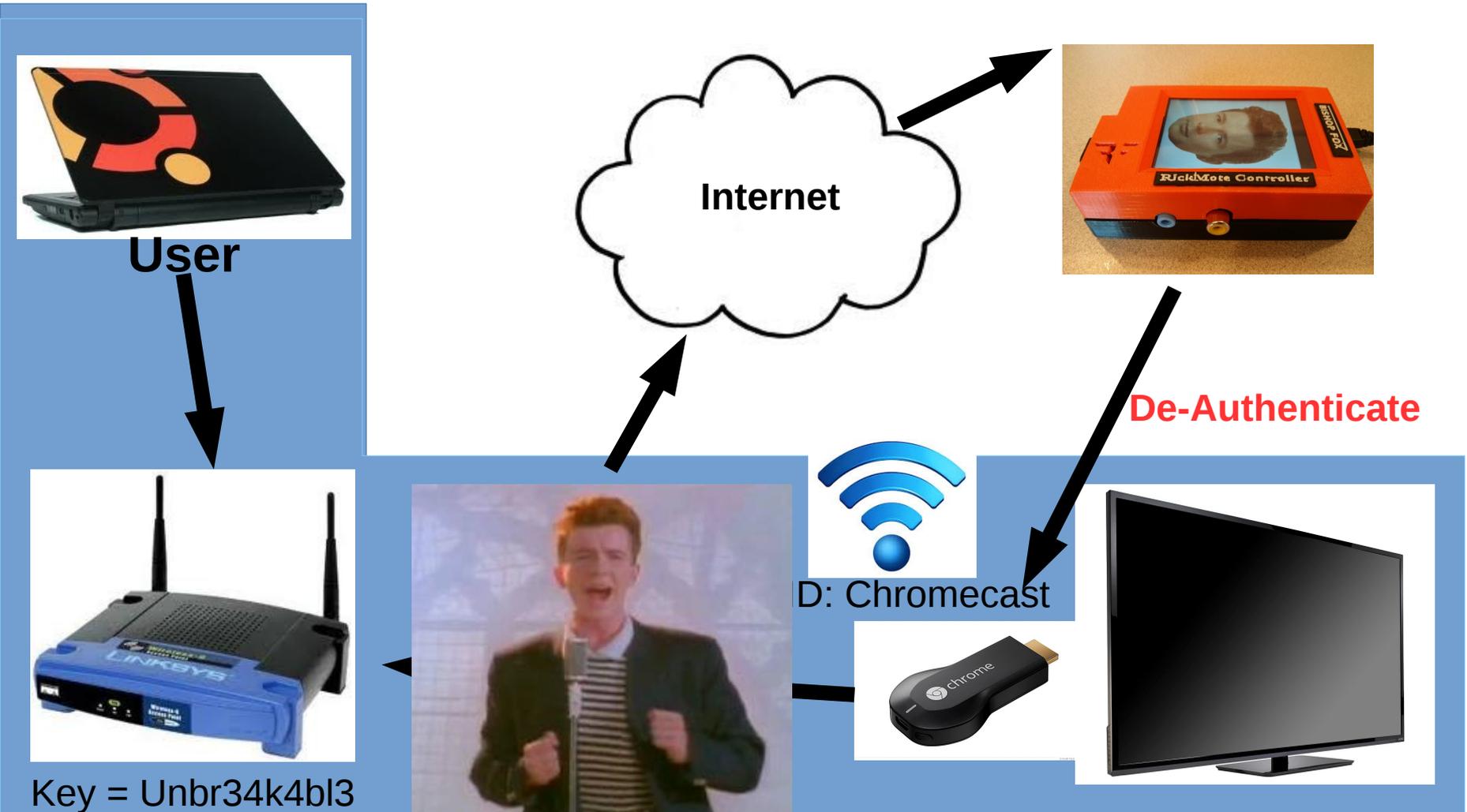
Forced Vacation

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



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...



```
1 {
2   "build_version": "17250",
3   "connected": true,
4   "has_update": false,
5   "hdm_i_control": true,
6   "hotspot_bssid": "FA:8F:CA:3C:6E:B7",
7   "ip_address": "192.168.43.32",
8   "locale": "en-US",
9   "location": {
10    "country_code": "US",
11    "latitude": 255.0,
12    "longitude": 255.0
13  },
14  "mac_address": "D0:E7:82:BD:7D:22",
15  "name": "Dancast",
16  "noise_level": -87,
17  "opt_in": {
18    "crash": true,
19    "device_id": false,
20    "location": false,
21    "stats": true
22  },
23  "public_key": "MIIBCgKCAQEAvjfUx1fGXlz+mw4Lv0
+Mu9QvGqRG9RWNdsOrllljFRl3U2gs2b0csgFcLgASvQDFbPw5coYTU1XQZuXvyNthT520
+0WvSZsXzoh885f2MBZhQW2fYmBwt+64FJELLzWfJkIwvhtZELWbx6gx0MN355PuouGbcw
+6SZWmGUyHed6YqtDuoJ00kt9kSs1zf4f0BEgotQVa4KVzn0sATNU90QyOikJMj0wviYw7
aPVNgepzpPUj6CDxnGhigEzaapMkf3/2flBuvuM9EuNRqpQIDAQAB",
24  "release_track": "stable-channel",
25  "setup_state": 61,
26  "signal_level": -58,
27  "ssdp_udn": "46d8f4b0-de65-edf3-5634-9cb347b57e14",
28  "ssid": "VirusLauncher",
29  "time_format": 1,
30  "timezone": "America/Phoenix",
31  "uma_client_id": "E0177EE4-SCC2-E22C-D59E-7B63DB0FB546",
32  "uptime": 2741.51,
33  "version": 4,
34  "wpa_configured": true,
35  "wpa_id": 12,
36  "wpa_state": 10
37 }
```

Swapping Connections

GET OVER HERE!

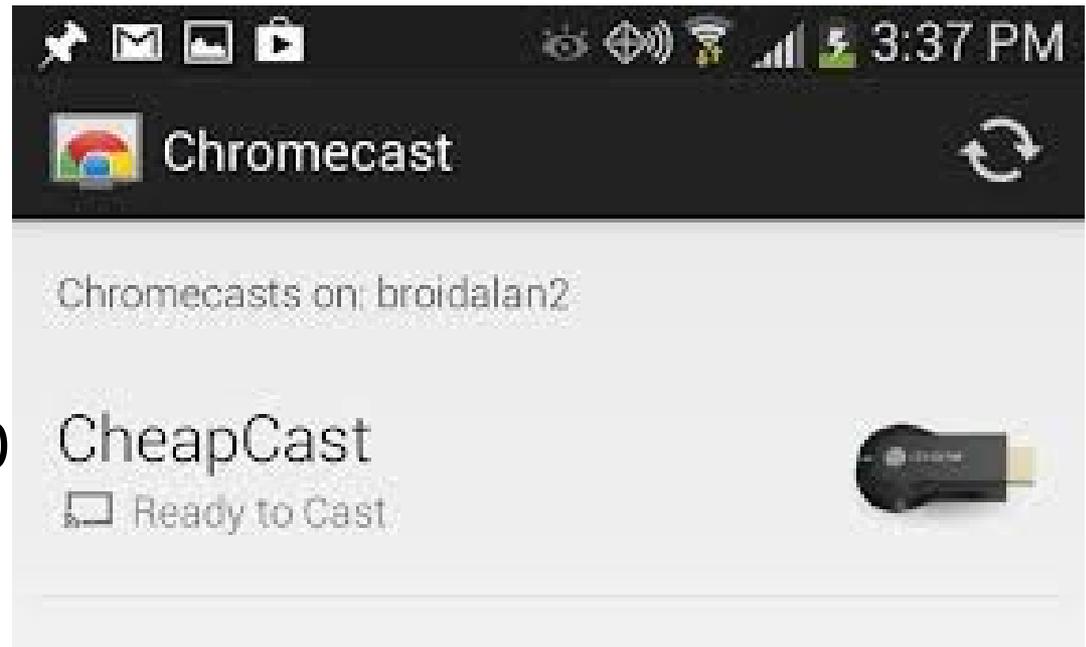
- **/setup/connect_wifi**
- JSON POST
- Wi-Fi keys are encrypted
 - With public key from eureka_info

```
1 {
2   "bssid": "10:fe:ed:23:57:24",
3   "signal_level": -53,
4   "ssid": "VirusLauncher",
5   "wpa_auth": 1,
6   "wpa_cipher": 1
7 }
```

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

