



# From the Aether to the Ethernet: Attacking the Internet using Broadcast Digital Television

Usenix Security Symposium, 21/Aug/2014

Yossi Oren, [yos@cs.columbia.edu](mailto:yos@cs.columbia.edu)

Joint work with Angelos D. Keromytis

# Related Work

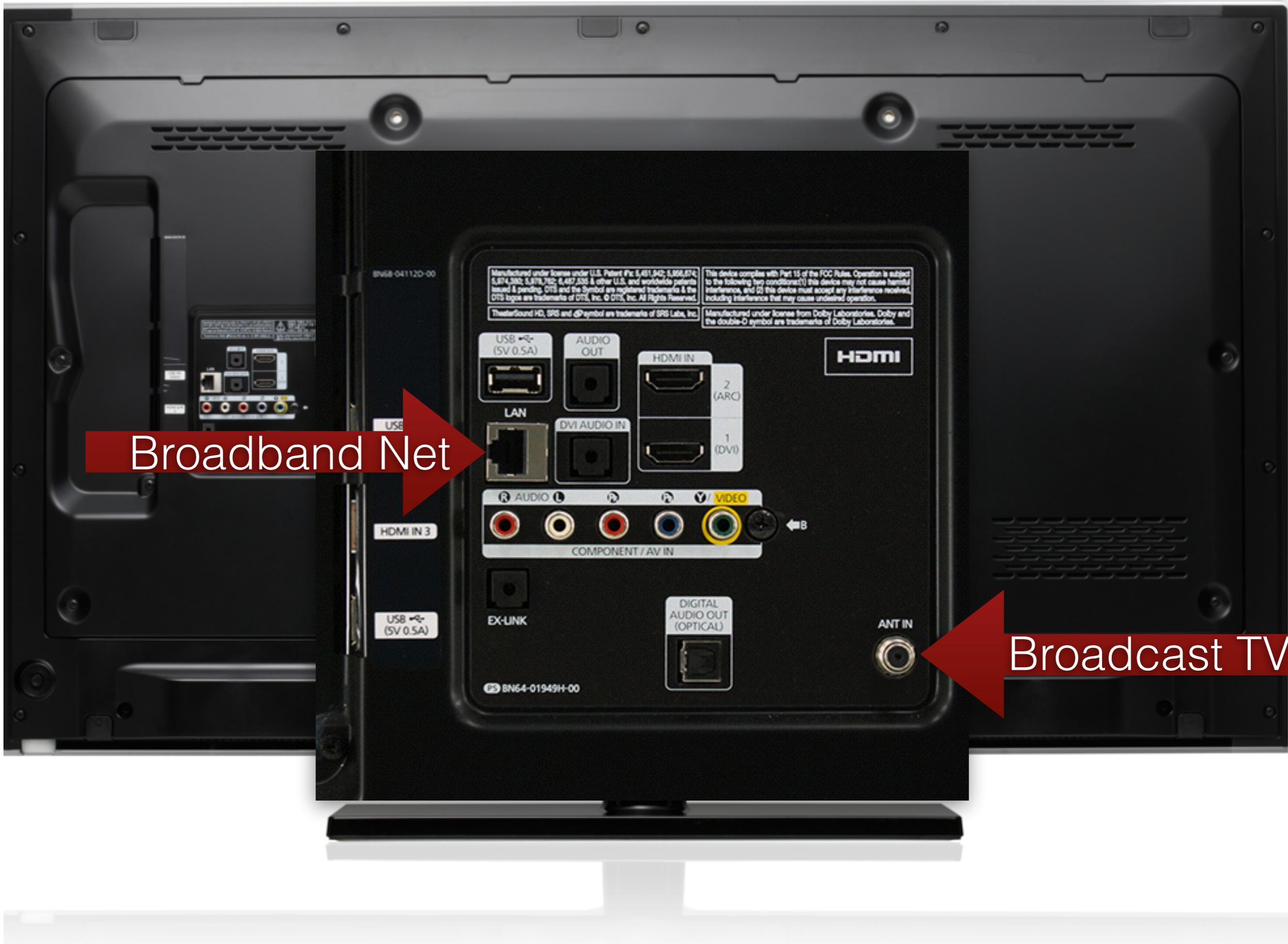
- Grattafiori and Yavor, Lee and Kim: Security issues in Smart TVs
- Herfurt, Tews et al.: Privacy-related problems (and possible solutions) in HbbTV advertising
- Nighswander et al., Checkoway et al.: RF-based attacks on embedded computers





Broadband Net

Broadcast TV



Smart TV!



NOS

Live

12 09

1x rood 2x geel

Overtredingen

55% 45%

Balbezit

1 4 12 9

Buitenspel

Hoekschoppen

10

Sch

< WK 2014

0 Nu 1 Gemist 2 Straks 3 Radio 8 WK Voetbal 9 Help

Aan/Uit Favorieten

Source: <http://www.broadbandtvnews.com/2014/05/31/dutch-pubcasters-step-up-hbbtv-efforts/>

# Security Problems in the HbbTV Specification



# Security Problems in the HbbTV Specification

- No user control over app life cycle
- Web Origin manually specified by app
- RF-based entry point into the Internet

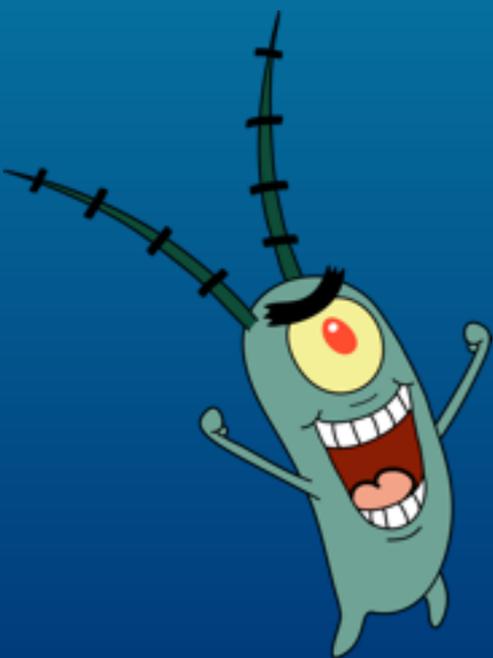
An elephant is standing on a small wooden stool. The elephant's trunk is raised and pointing towards the right. The elephant's body is mostly obscured by the text 'See Only a Part of the Picture' which is written in white on a black background. The stool is a simple wooden stool with three legs and a flat top. The elephant's front legs are resting on the stool.

# See Only a Part of the Picture Problems in the App Specification

- No user control over app life cycle
- Web Origin manually specified by app
- RF-based entry point into the Internet

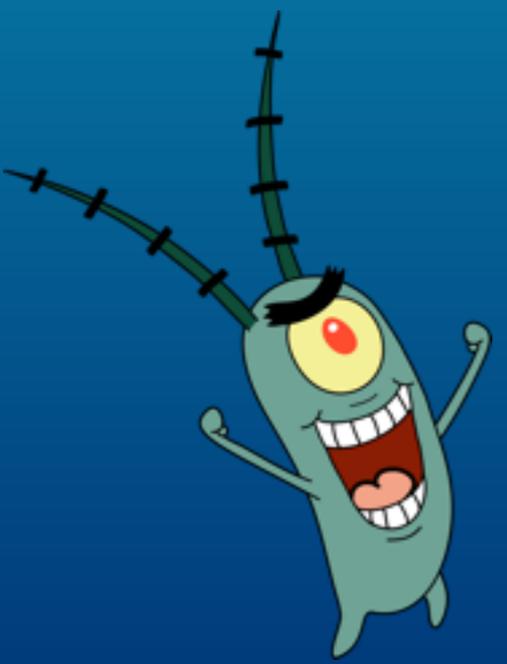








# Kelp

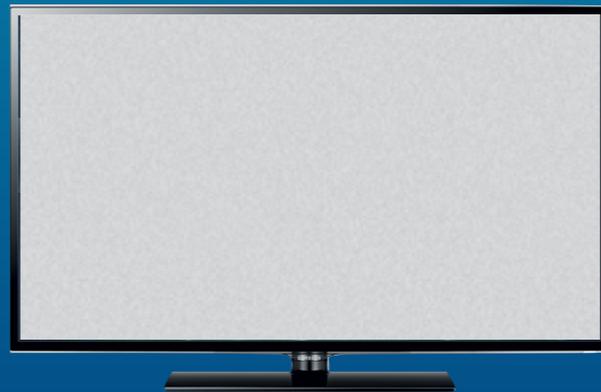
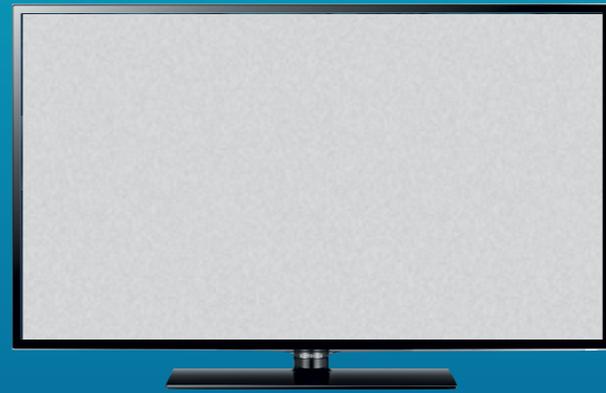
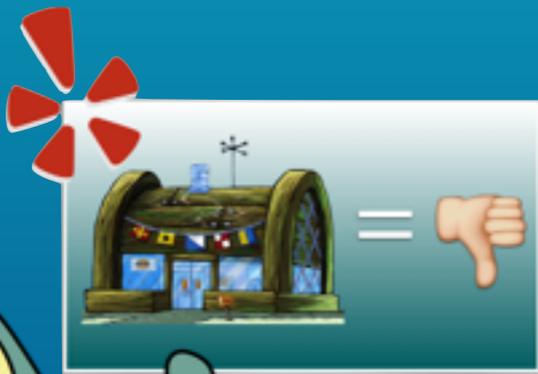


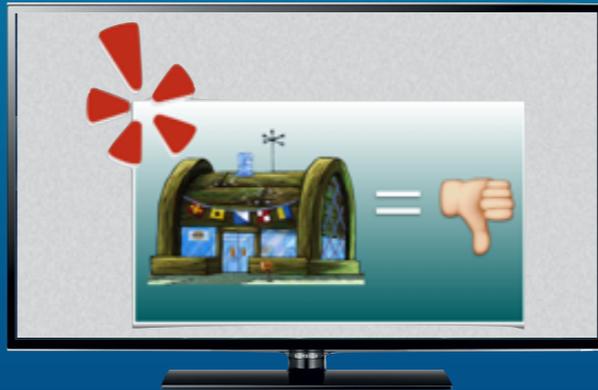
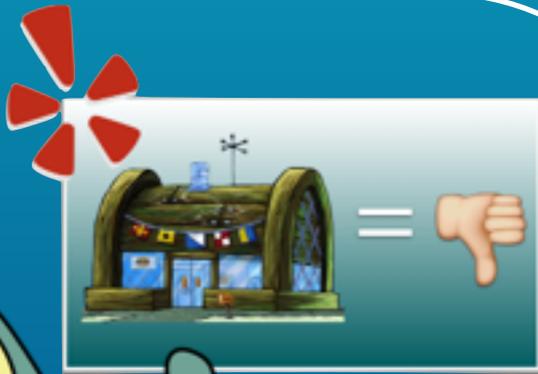


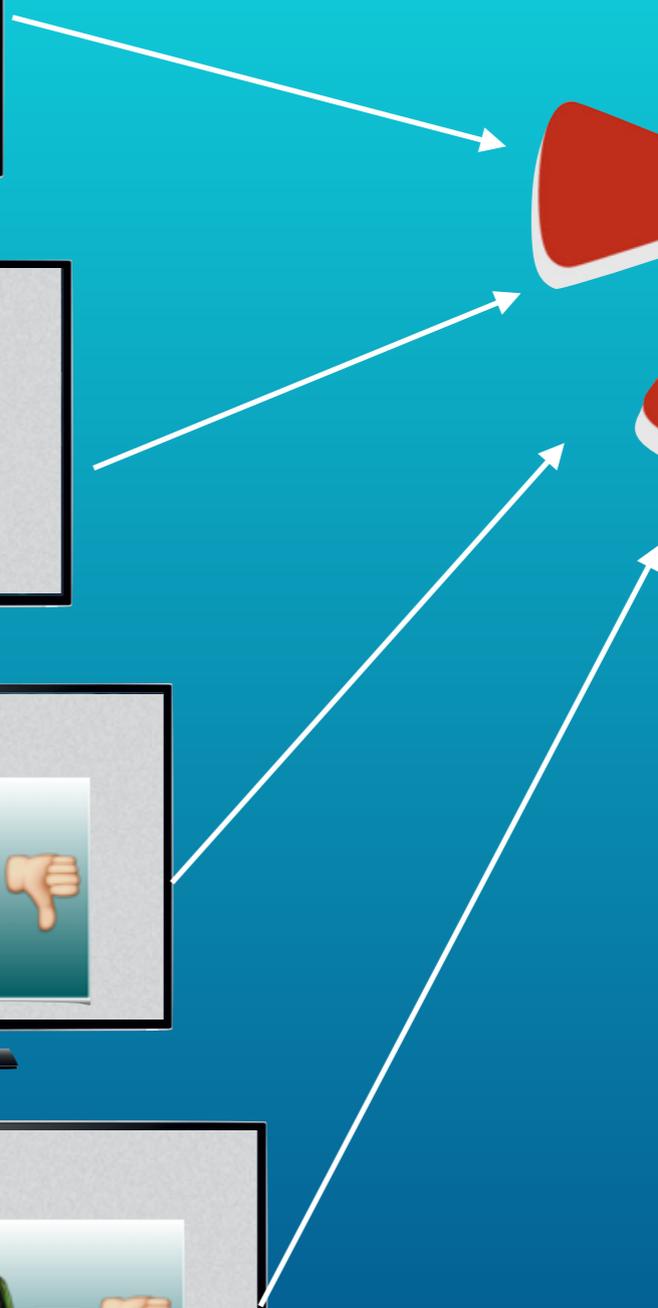
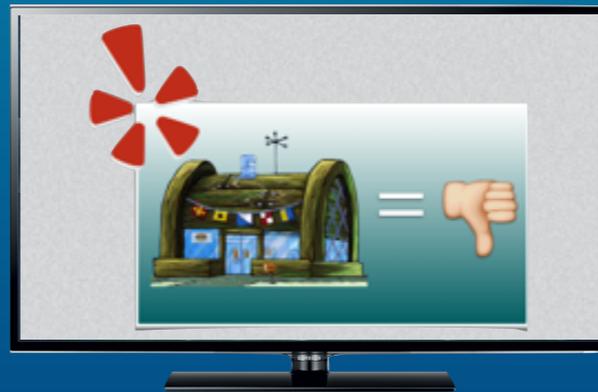
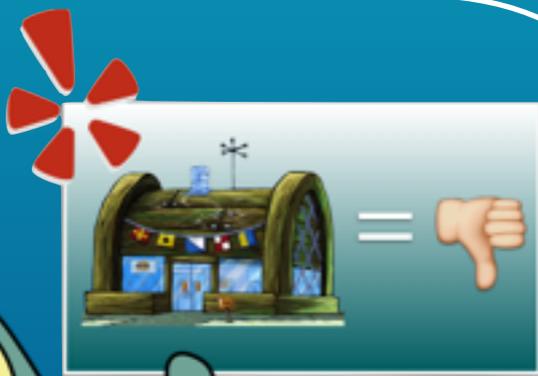


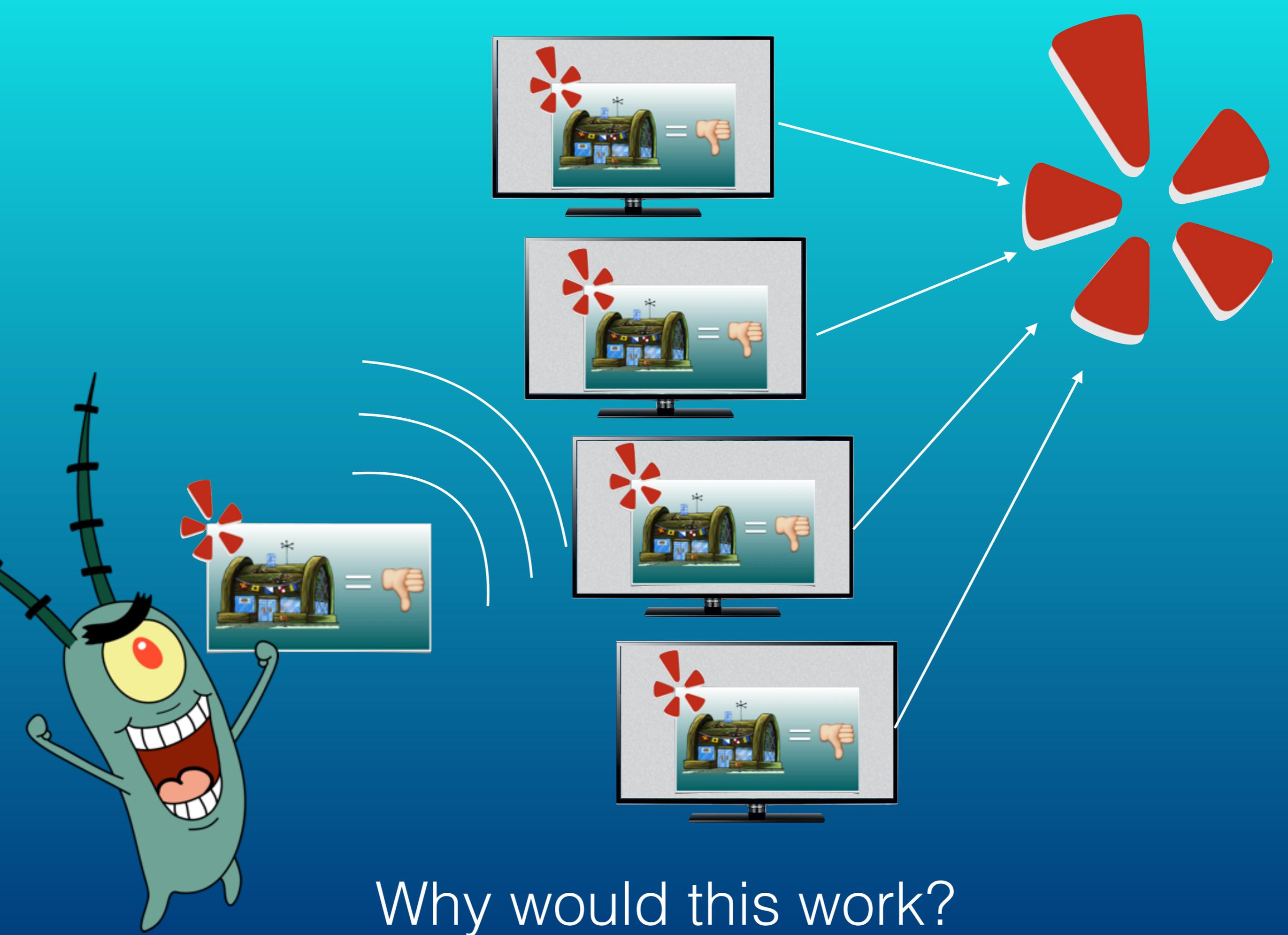
=





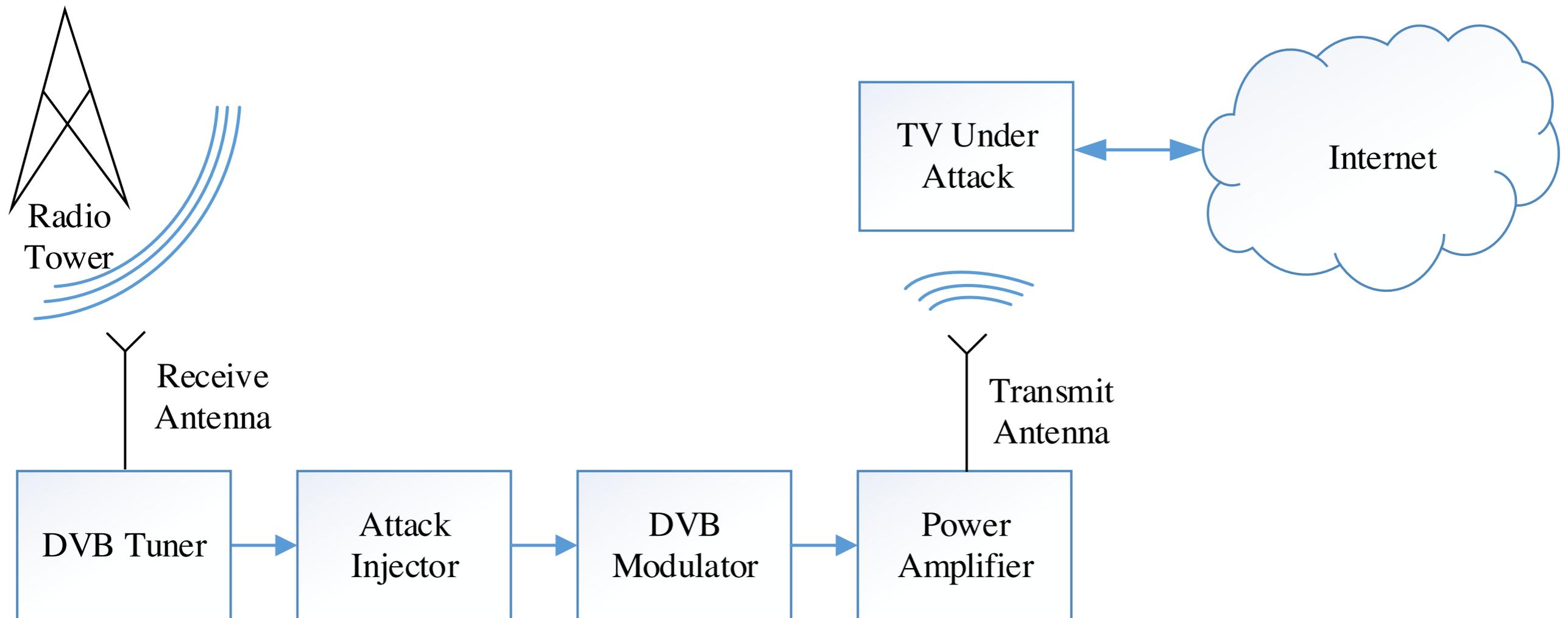




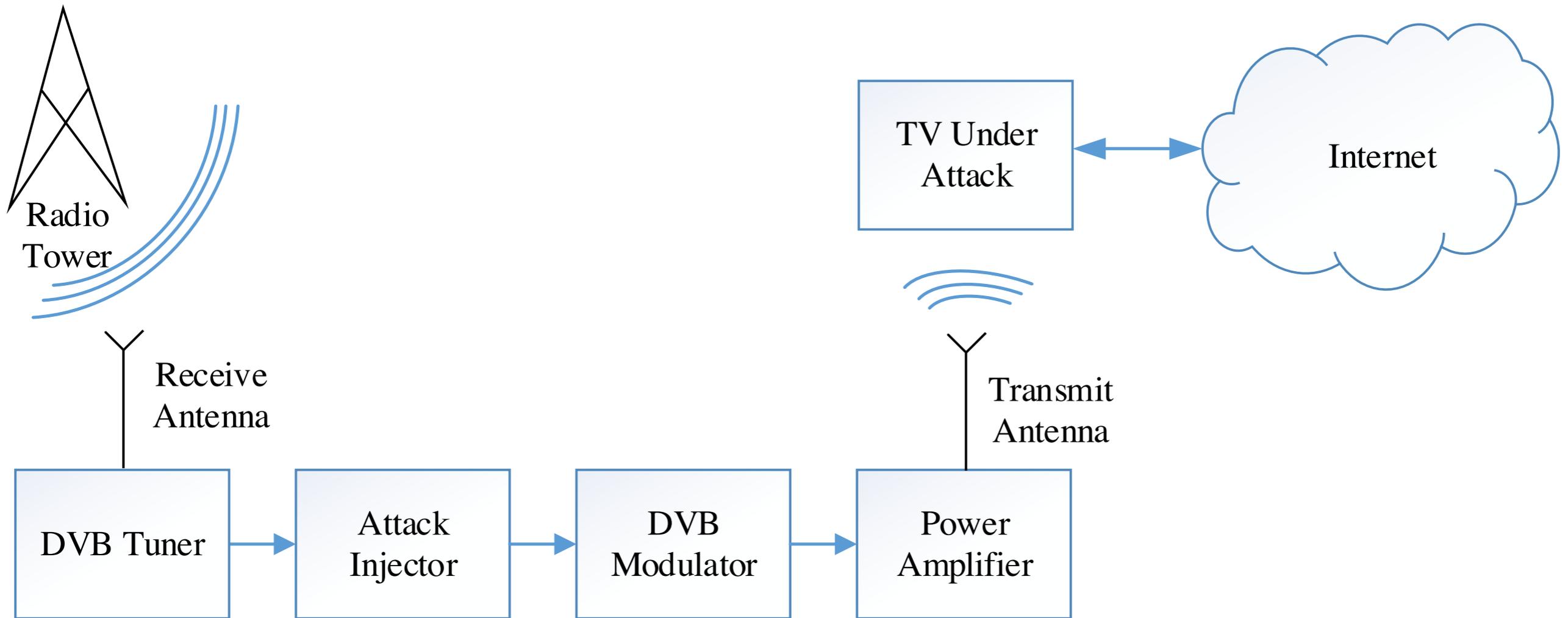


Why would this work?

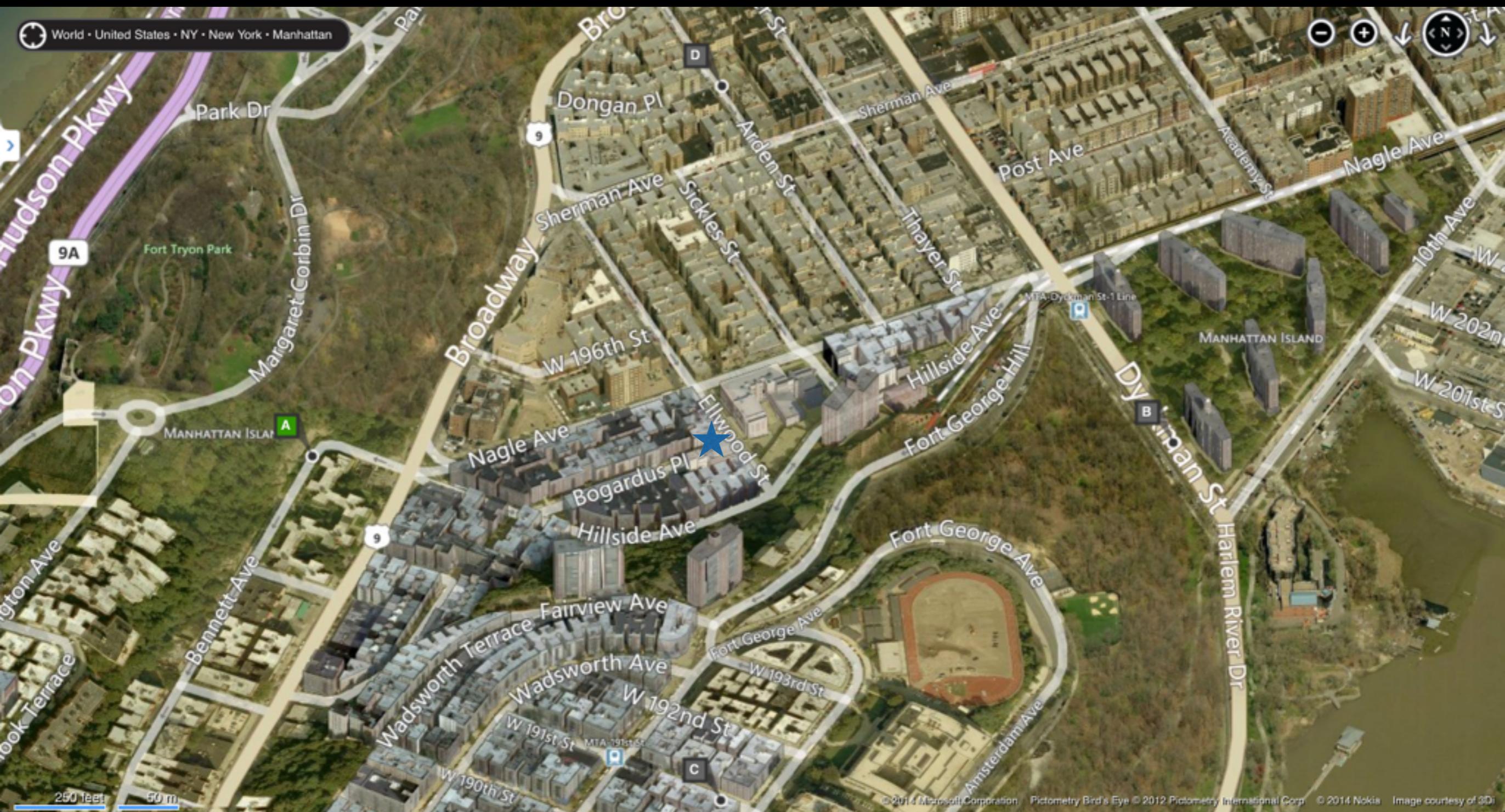
# Attack Setup



# Attack Setup



Total cost: \$450



Total cost: \$450



Total cost: \$450

# Countermeasures

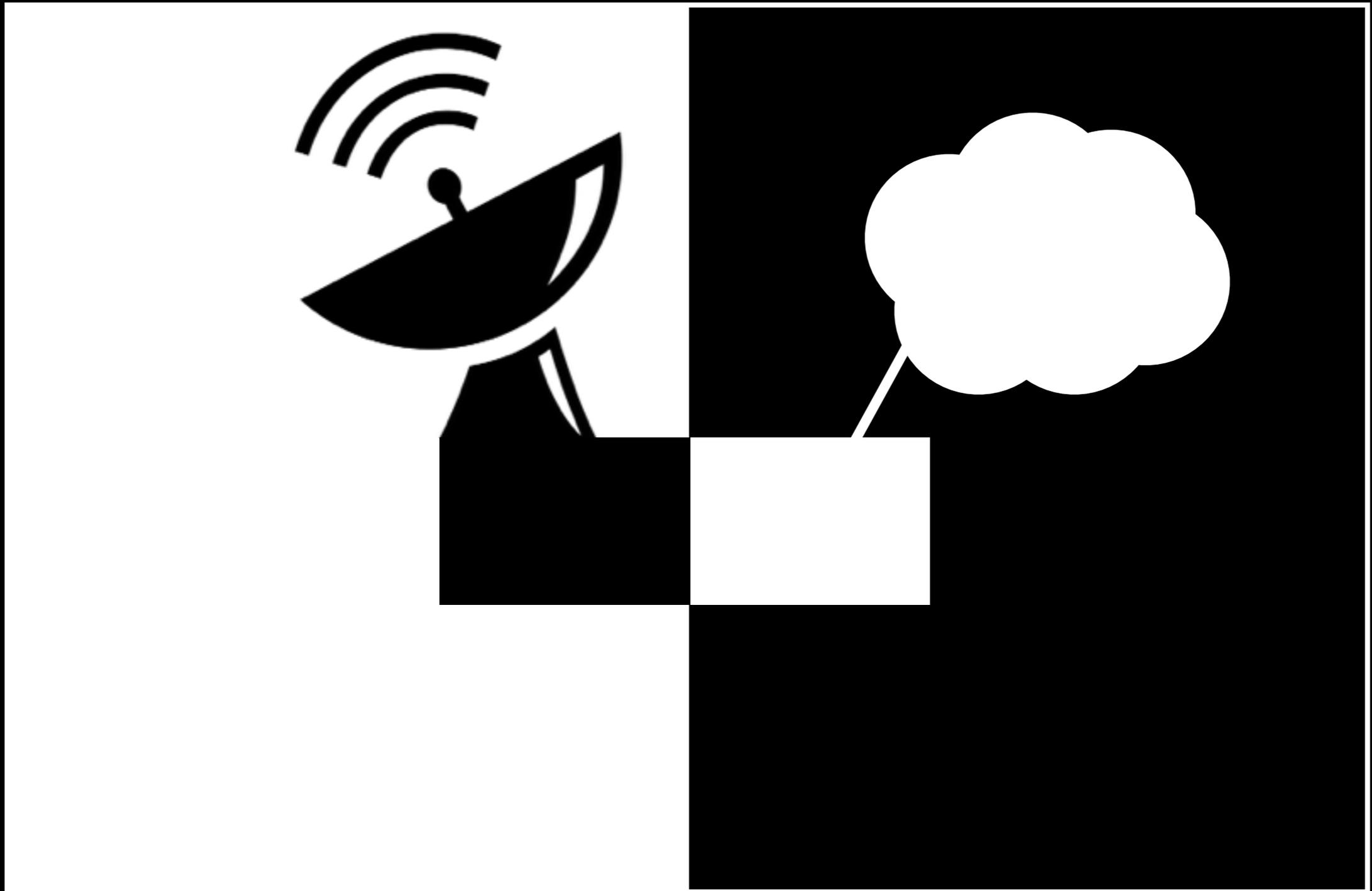
- Give user **explicit control** over life cycle
- **Fix implementation** of Web Origin
- **Isolate RF-sourced programs** from the Internet

# Countermeasures

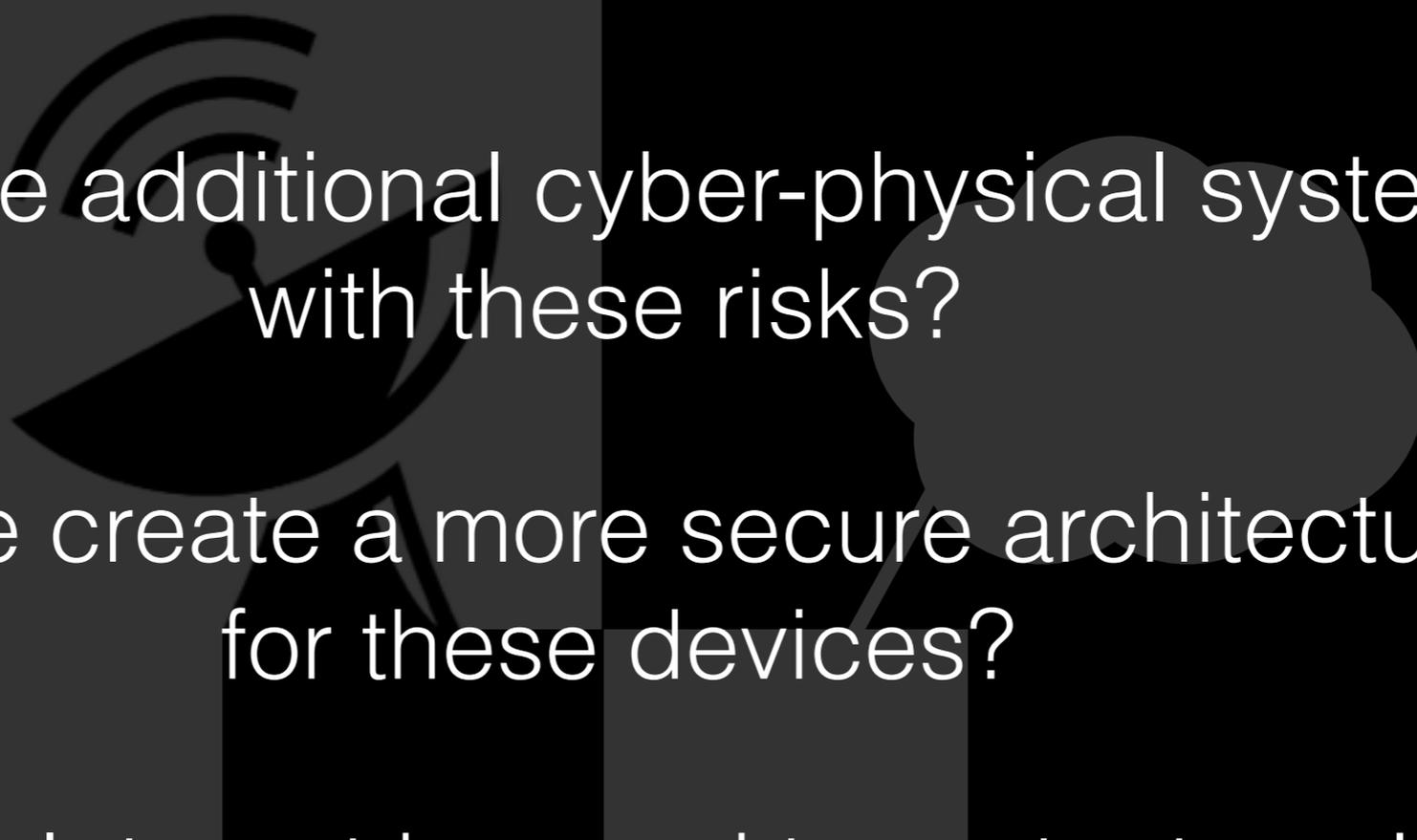
- Give user **explicit control** over life cycle
- **Fix implementation** of Web Origin
- **Isolate RF-sourced programs** from the Internet
- Problem: countermeasures are bad for business

The big picture

# The big picture



# The big picture



Are there additional cyber-physical systems with these risks?

Can we create a more secure architecture for these devices?

Can the Internet be used to protect against sensor-side attacks?

# Thank You!

For more information:

<http://iss.oy.ne.ro/Aether#Usenix>