From the Aether to the Ethernet—Attacking the Internet using Broadcast Digital Television

Yossef Oren and Angelos D. Keromytis, Columbia University

23rd USENIX Security Symposium, August 2014

ented by Ren-Jay Wang

CS598 - COMPUTER SECURITY IN THE PHYSICA

V – Past

Multiple data streams (MPEG-2 Elementary Streams)

Information tables group these streams into an individual TV channel

TV Broadcasters

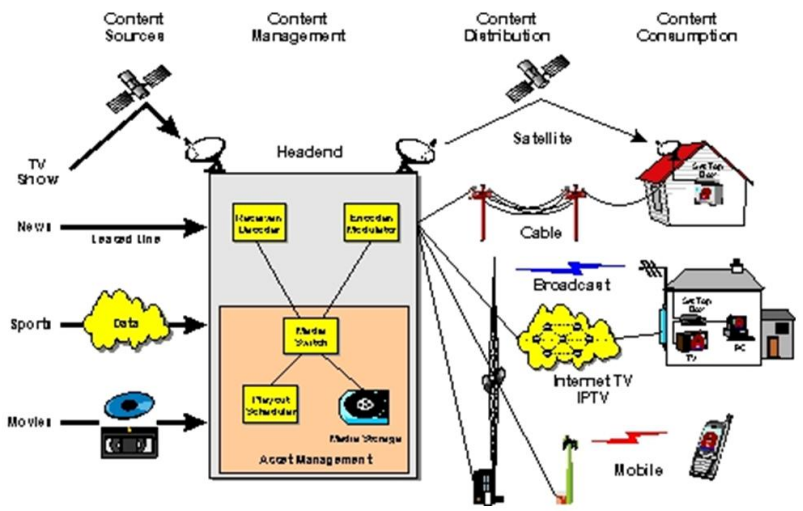
Content Sources

Subscription Services

Ad Sources

Broadcast Systems

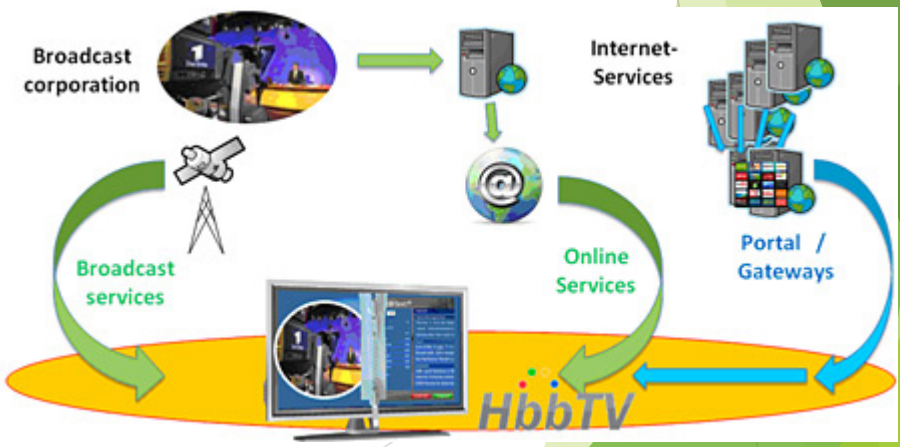
- Cable TV
- Satellite TV
- Broadcast TV
- Mobile TV
- IPTV
- Internet TV



V – Present(HbbTV)

Additional **application information table (AIT)** describing broadband-based application

AIT can hold URL to web content, or an additional data stream can hold the relevant HTML files (<-vulnerable!)



elated work

2013 – Tews et al. showed that it is possible to tell what someone is watching by sniffing encrypted HbbTV traffic packets

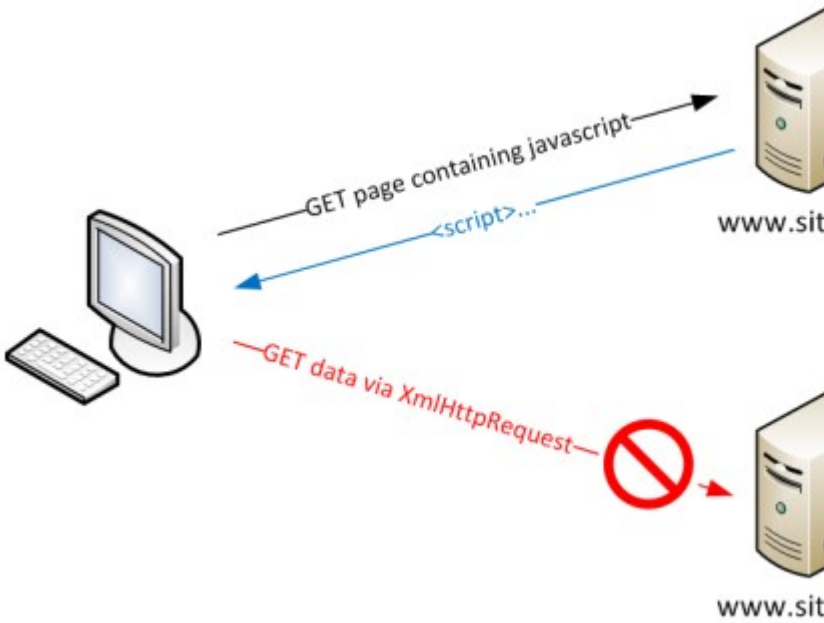
2013 – Herfurt discovered that many German HbbTV providers abused the HbbTV capabilities by having them “phone home” periodically when the channel was on

bbTV Security Weaknesses

Same-Origin Policy is flawed because broadcast streams can define THEIR OWN web origins to ANY desired domain name

uting, the **same-origin policy** is an important concept in the web application model. Under the **policy**, a web browser permits scripts contained in a first e to access data in a second web page, but only if both web pages have the **igin**.

rigin policy - Wikipedia, the free encyclopedia
wikipedia.org/wiki/**Same-origin_policy** Wikipedia



bbTV Security Weaknesses (cont.)

- Untraceable attacks
- Invisible and unstoppable attacks

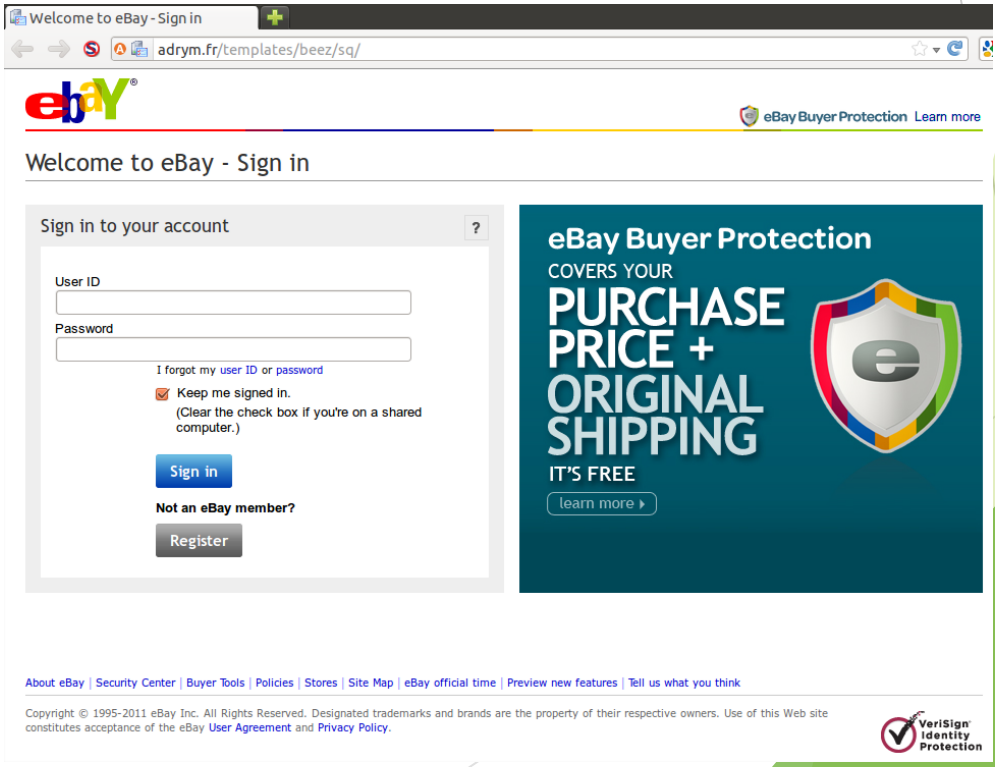
hreat Model – Who are we defending gainst?

- Man in the middle attack
- Attacker has a physical device with an omnidirectional antenna
- Device is level with targeted devices
- Attacker is using an amplifier
- Co-Channel interference – is this a reasonable assumption?
- Densely populated urban area with low power TV stations

ossible attacks

- Distributed Denial of Service
- Unauthenticated Request Forgery
- Authenticated Request Forgery

- Intranet Request Forgery
- Phishing/Social Engineering
- Exploit Distribution



emonstration of Attacks

2012 Smart TV

No power amplifier or transmitter antenna – DVB modulator directly connected to TV's antenna input

Created applications that ran in background & took over TV screen

isk Assessment Analysis

$450 to setup, additional $50/hour per attack

Can affect 10,000 hosts using a modest amplifier

Attack Type	Complexity	Damage Potential	Overall Risk
Denial of Service	Low	Low	Medium
Unauthenticated Request Forgery	Low	Medium	High
Authenticated Request Forgery	Medium	High	High
Intranet Request Forgery	Medium	High	High
Phishing/Social Engineering	High	High	Medium
Exploit Distribution	Medium	High	High

ountermeasures

Crowdsource detection of RF attacks

Indicate to users when HTML content is being displayed … however this may be resisted by broadcasters

Prevent broadcast-delivered HTML content from accessing the internet – applications that required Internet access would have to submit a URL

Encryption and proxies ineffective

Content signing would prevent same-origin abuse, but would still not be sufficient due to “blind” CSRF/PuppetNet attacks

iscussion Points

Are the criticisms leveled against the paper valid? That is, can these attacks feasibly reach a large number of systems? Are they cost-effective?

What are limitations to these attacks?

What are the main contributions of this paper?

What could be done to prevent these attacks?