The Mood Altering Router

Presented by Philip Daian and Jack LaSota

CS563/ECE524 Advanced Computer Security University of Illinois

Premise

Confidentiality?
Integrity?
Availability?

Hardware

~$100, Wireless N
Long range, outdoor
Up to 1km OTB
FCC Maximum Wattage

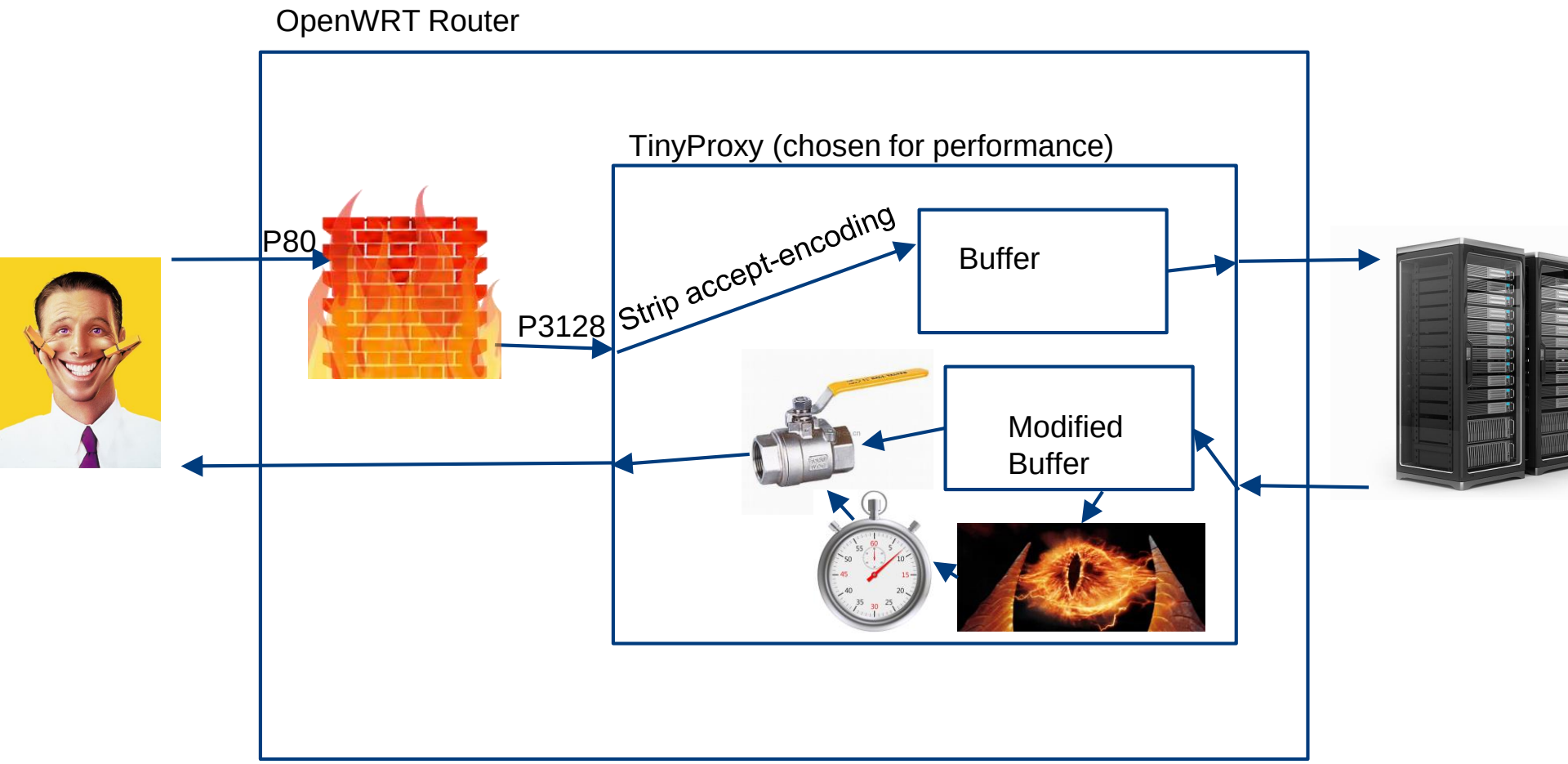
$150 next gen model :(

<<$20, Wireless G
~200 feet OTB

Generalizable? Kind of. Each router -> up to millions of identical. Each router model -> different chip, architecture, flash config, ...

openwrt-AGV2+W-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-AR-5381u-squashfs-cfe.bin	02-Oct-2014 07:28	838886
openwrt-AR-5387un-squashfs-cfe.bin	02-Oct-2014 07:28	838886
openwrt-AR1004G-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV2091_BTR-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV2091_ROI_WB-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV210_BTR-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV210_ROI_WB-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV2110-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV220V_MGCP_BTR-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-BTV2500V-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-CPA-ZNTE60T-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-CT536_CT5621-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-CT6373-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DG834GT_DG834PN-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DSL2640B-B2-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DSL2650U-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DSL274XB-C2-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DSL274XB-C3-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-DSL274XB-F1-AU-squashfs-cfe.bin	02-Oct-2014 07:28	419456
openwrt-DSL274XB-F1-EU-squashfs-cfe.bin	02-Oct-2014 07:28	419456
openwrt-DV201AMR-squashfs-cfe.bin	02-Oct-2014 07:28	340197
openwrt-DVAG3810BN-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-F5D7633-squashfs-cfe.bin	02-Oct-2014 07:28	340787
openwrt-F@ST2404-cfe-squashfs-cfe.bin	02-Oct-2014 07:28	340787

Solution for Bare HTTP



Sentiment Analysis

- LIWC = $$$, we couldn't obtain so we approximated

Prepositions	12.24	2.85	12.23	2.82	0.99
Negations	1.91	1.11	1.85	1.11	0.97
Numbers	2.52	2.15	2.51	2.15	1.00
Swear words	0.31	0.64	0.30	0.63	0.99
Social words	8.63	3.97	7.92	3.82	0.98
Family	0.53	0.85	0.51	0.84	0.99
Friends	0.33	0.46	0.32	0.46	0.99
Humans	0.73	0.66	0.67	0.61	0.95
Affect	5.12	2.25	4.04	1.91	0.93
Positive emotions	3.02	1.62	2.26	1.33	0.89
Negative emotions	2.04	1.43	1.76	1.31	0.97
Anxiety	0.39	0.46	0.28	0.39	0.91
Anger	0.69	0.86	0.59	0.79	0.97
Sadness	0.41	0.50	0.37	0.47	0.97
Cognitive mechanisms	16.34	4.02	6.41	2.50	0.75
Insight	2.20	1.26	1.86	1.05	0.86

Sentiment Analysis

```
static const char *bad_words[] = {
    "sad",
    "sore",
    "bullshit",
    "boring",
    "sucks",
    "worthless",
    "bad",
    "shitty",
    "lousy",
    "lost",
    "useless",
    "stupid",
    "cold",
    "dumb",
    "scare",
    "hate",
    "worse"
};
```

```
static const char *good_words[] = {
    "happy",
    "joy",
    "easy",
    "free",
    "kind",
    "great",
    "awesome",
    "glad",
    "blessed",
    "love",
    "warm",
    "hope"
};
```

<html

Handling SSL

- TLS: *confidentiality* of Internet data? Contagion?
- **PROBLEM**: We can't see traffic, how to classify web pages? How to know what to slow down?
- **PROBLEM**: We can't identify individual requests in a series of pages. Sockets often reused.

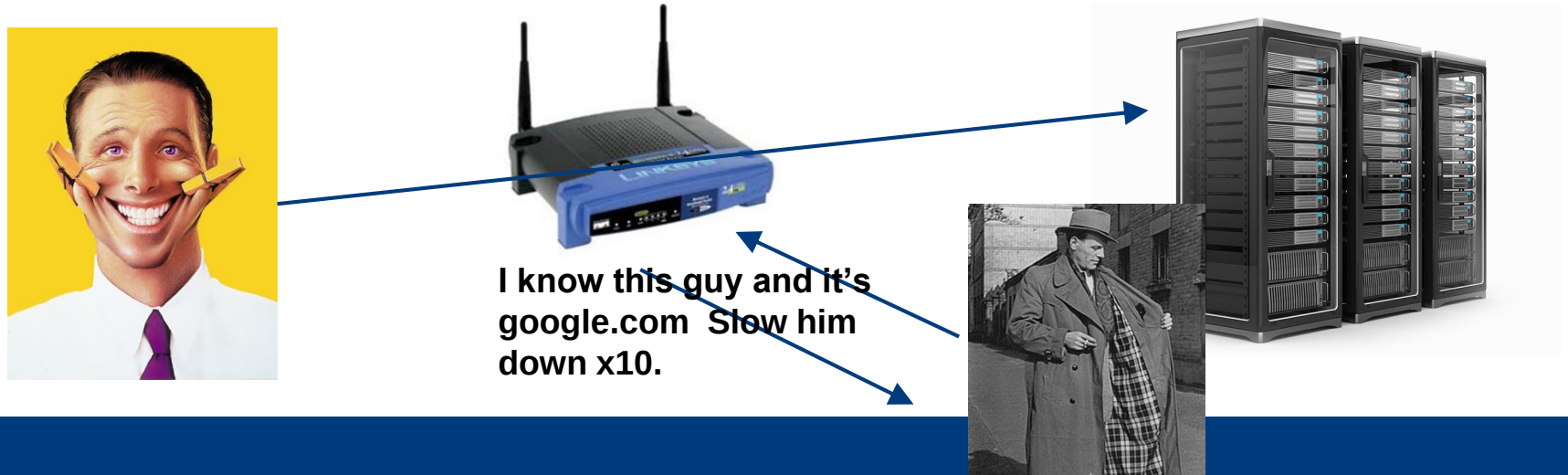
Preserve log | Disable cache

Name Path	Method	Status Text	Type	Initiator	Size Conter	Time Latency	Timeline
www.reddit.com	GET	200 OK	text/html	Other	19.6… 109 …	254 ms 144 ms	
templates.html gfdcmdcpehpkengmk…	GET	200 OK	text/html	browsers… Script	(fro…	4 ms 4 ms	
reddit.lSQn3qSpM_o…. www.redditstatic.com	GET	304 Not …	text/css	www.redd… Parser	547 B 213 …	336 ms 334 ms	
old-markdown.Lcx8l-…		304		www.redd…	547 B	380 ms	

50 requests | 66.5 KB transferred | 3.12 s (load: 3.24 s, DOMContentLoaded: 2.75 s)

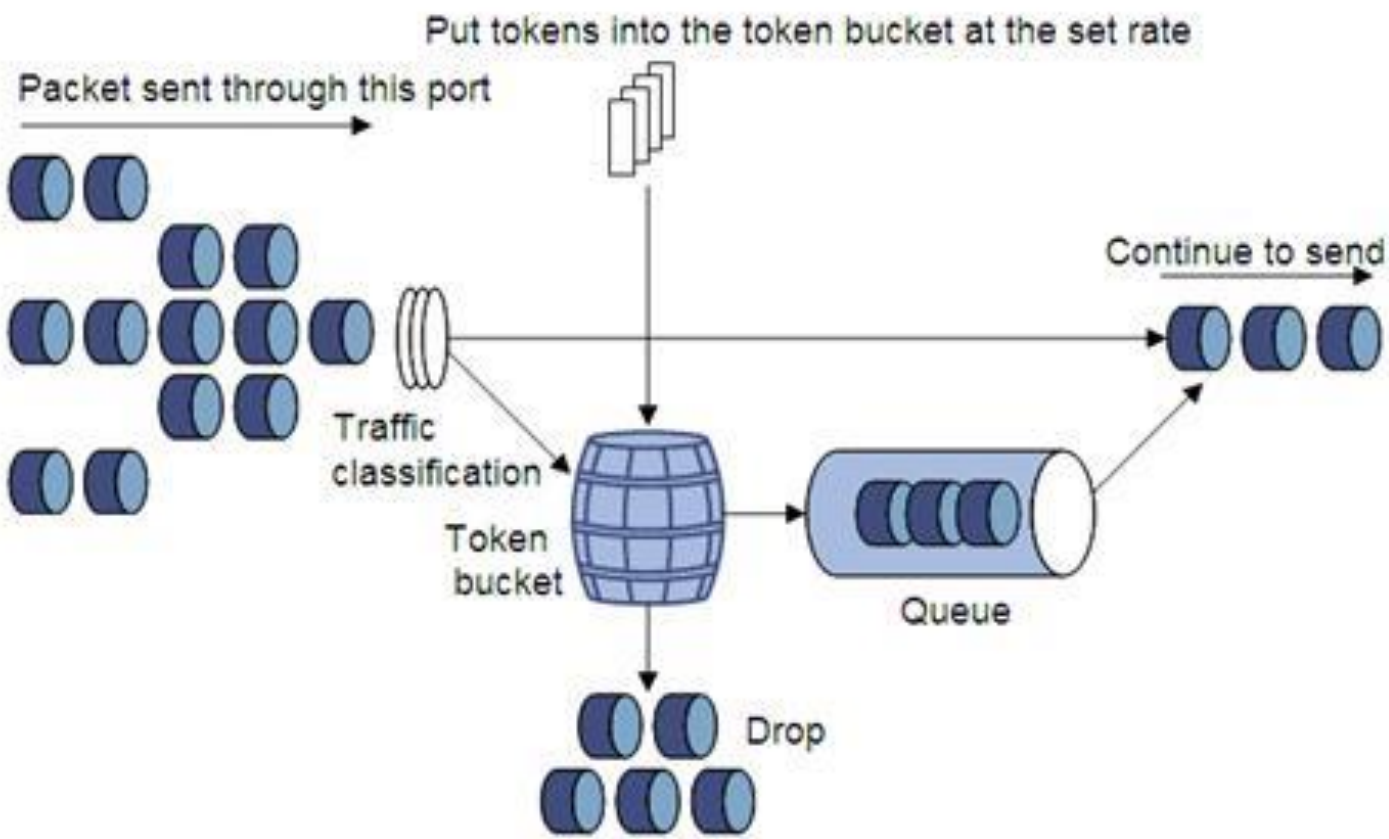
Really Handling SSL

- **sslstrip**: thoughtcrime.org/software/sslstrip/ BUT strict transport security, <0.4% of sites (now)
- **sslsniff**: Pull out certificate from connection.
- **Observation**: (IP, port) uniquely ID's cert
- **Solution**: Use OpenSSL to get cert, analysis online



Really *Really* Handling SSL

- Once traffic is ID'd, **traffic shaping** (token bucket)
- We use three buckets/traffic tiers (slow, med, fast`



Amateur Filtering

- We use **tc** (Linux tool) + **iptables** (stateful firewall) (together with **tcpdump** + **openssl** for traffic ID) (http://lartc.org/)

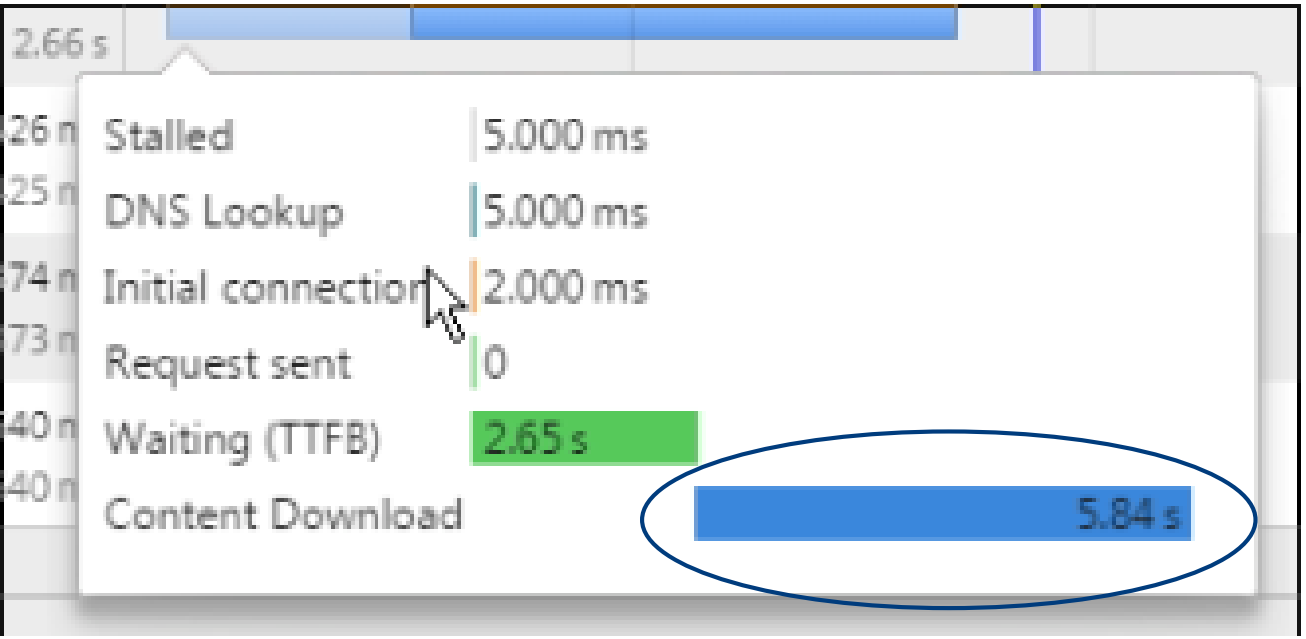
```
tc qdisc add dev br-lan root handle 1: htb default 30
tc class add dev br-lan parent 1: classid 1:1 htb rate 20mbit burst 15k
tc class add dev br-lan parent 1:1 classid 1:10 htb rate 19mbit burst 15k
tc class add dev br-lan parent 1:1 classid 1:20 htb rate 1mbit ceil 2mbit burst 15k
tc class add dev br-lan parent 1:1 classid 1:30 htb rate 1kbit ceil 20kbit burst 15k

tc qdisc add dev br-lan parent 1:10 handle 10: sfq perturb 10
tc qdisc add dev br-lan parent 1:20 handle 20: sfq perturb 10
tc qdisc add dev br-lan parent 1:30 handle 30: sfq perturb 30

iptables -t mangle -A POSTROUTING -j CLASSIFY --set-class 1:10
```

The ISP Level

- This filtering type is **legal** and **with precedent**
- http://arstechnica.com/gadgets/2007/07/deep-packet-inspection-meets-net-neutrality/
- http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works
- Infrastructure already exists, in use for **advertising, state censorship, copyright enforcement**
- Tools to use DPI + packet shaping, traffic control
- Attack feasible without significant new investment

Donning the Tinfoil Hat

Contagion attack is practical, legal, security violating



??

Detecting simple delays is easy.

Detecting traffic shaping, DPI is hard. Analytic tools?

Now for the **real** demo

Demo Videos

Download here: https://www.dropbox.com/s/c4y6jslr4gzfp7p/moodroutervideos.zip

Further Reading

- https://www.eff.org/deeplinks/2008/09/comcast-unveils-its-new-traffic-management-archite
- http://wiki.openwrt.org/doc/howto/packet.scheduler/packet.scheduler.theory
- http://broadband.mpi-sws.org/transparency/bttest.php
- (of course) http://www.pnas.org/content/111/24/8788.full
- http://ai.stanford.edu/~ronnyk/2009controlledExperimentsOnTheWebSurvey.pdf
- http://www.pnas.org/content/107/29/12804.abstract (emotions affecting voting, etc)