An Empirical Study of

Vulnerability Rewards Programs

Matthew Finifter, Devdatta Akhawe, David Wagner
UC Berkeley

security development lifecycle

A vulnerability remediation strategy is any systematic approach whose goal is to reduce the number of software vulnerabilities.

CERT

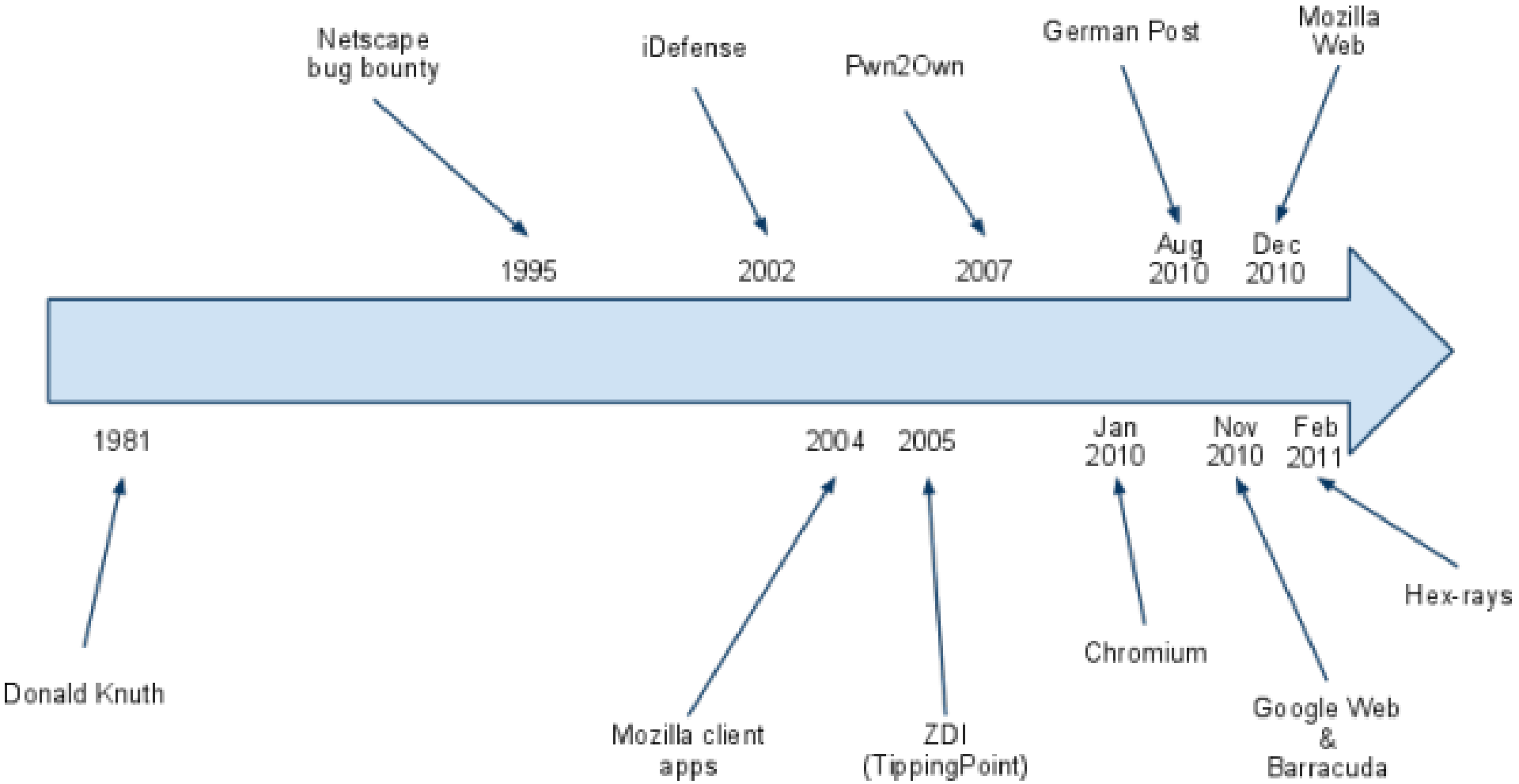
Code Reviews

Penetration Testing

Dynamic/Static Analysis Tools

Bug Bounties?


WHAT IS A BUG BOUNTY?
WE PAY PEOPLE FOR PWNING US



There is an active debate over the value and effectiveness of VRPs. A number of vendors, notably Microsoft, Adobe, and Oracle, do not maintain a VRP, with Microsoft arguing that VRPs do not represent the best return on investment on a per-bug basis

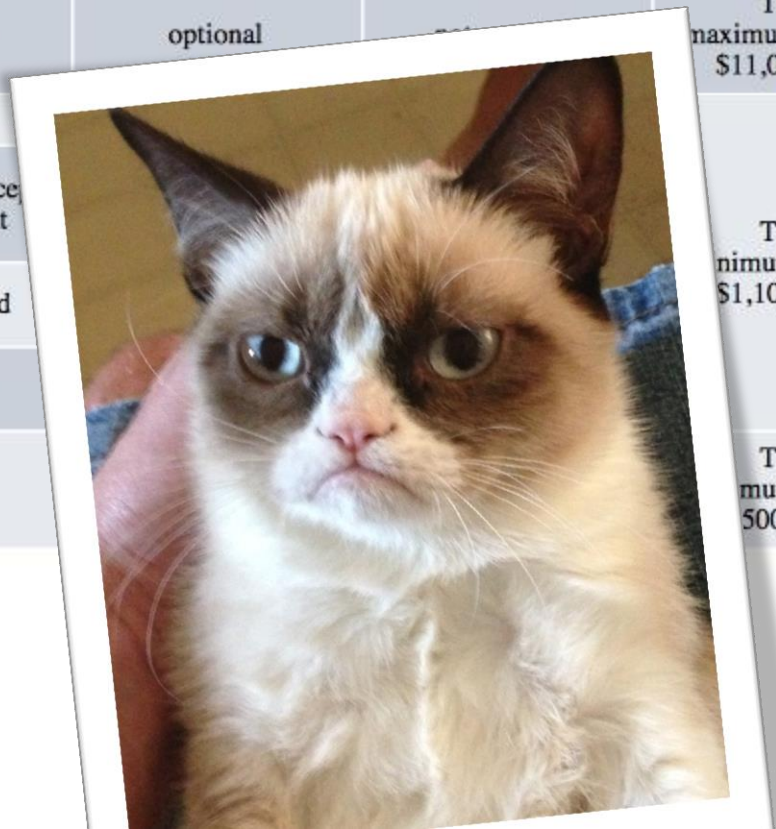
-- Our paper

IE11 Preview Bug Bounty

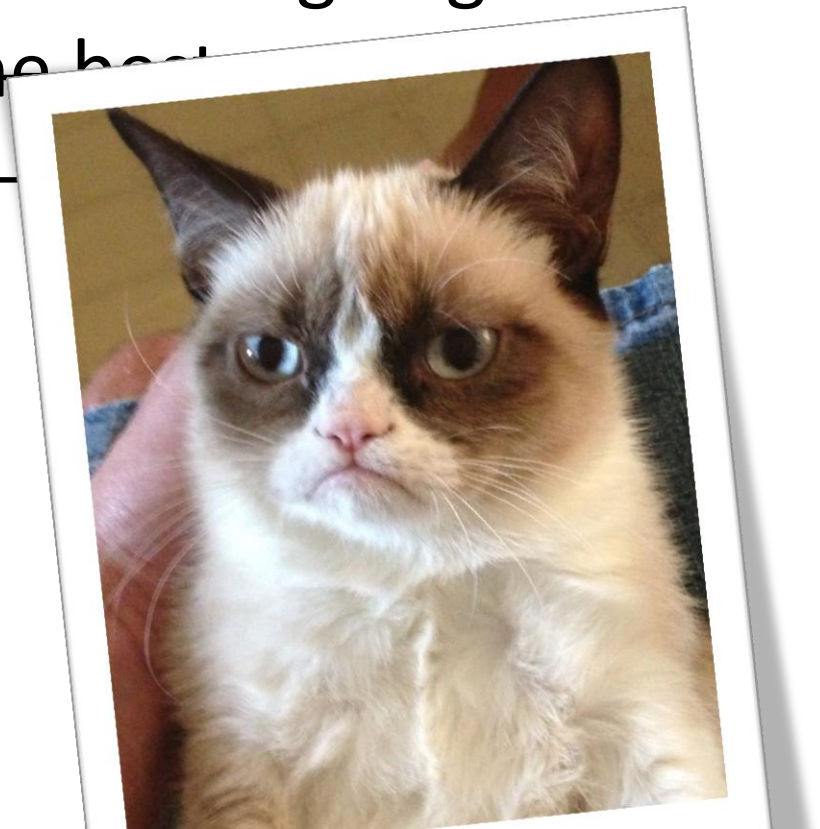
Payouts & Tiers

Vulnerability Type	Crash dump	Proof of concept	Functioning exploit	Whitepaper	Sandbox escape	Base Payout Tier
RCE vulnerability	not required	required	required	required	required	Tier 0 Could exceed $11,000 USD*
	not required	required	required	required	not required	
	not required	required	required	optional		Tier 1 naximum payment $11,000 USD
	not required	required	n/a			
Important or higher severity design-level vulnerability	not required	required	Proof of Conce is sufficient			Tier 2 nimum payment $1,100 USD*
Security bug with Privacy Implications	not required	required	not required			
Sandbox Escape Vulnerability	not required	required	optional			
ASLR Info Disclosure Vulnerability	not required	required	n/a			Tier 3 mum payment 500 USD*

* Higher payouts possible at Microsoft's discretion based on level of quality and complexity.

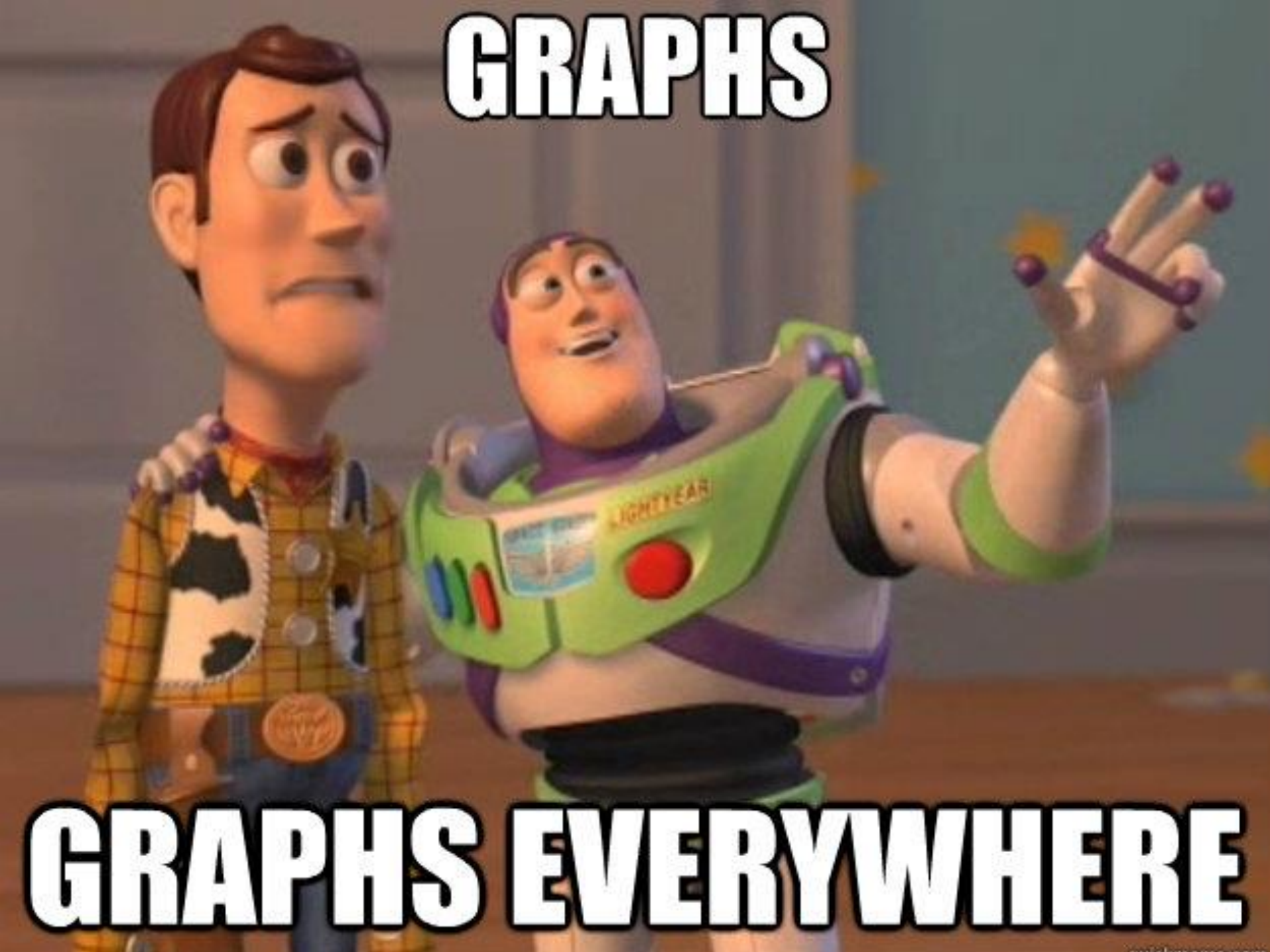


There is an active debate over the value and effectiveness of VRPs. A number of vendors, notably ~~Microsoft~~, Adobe, and Oracle, do not maintain a VRP, ~~with Microsoft arguing that VRPs do not represent the best~~ ~~investment on a per-bug~~



- Analysis of Chrome & Firefox VRPs
- From 2 viewpoints
  - Software Vendor
  - Security Researchers
- Other analysis of the data
- Lots of hypotheses
  - We can't do experiments!

today


GRAPHS
GRAPHS EVERYWHERE

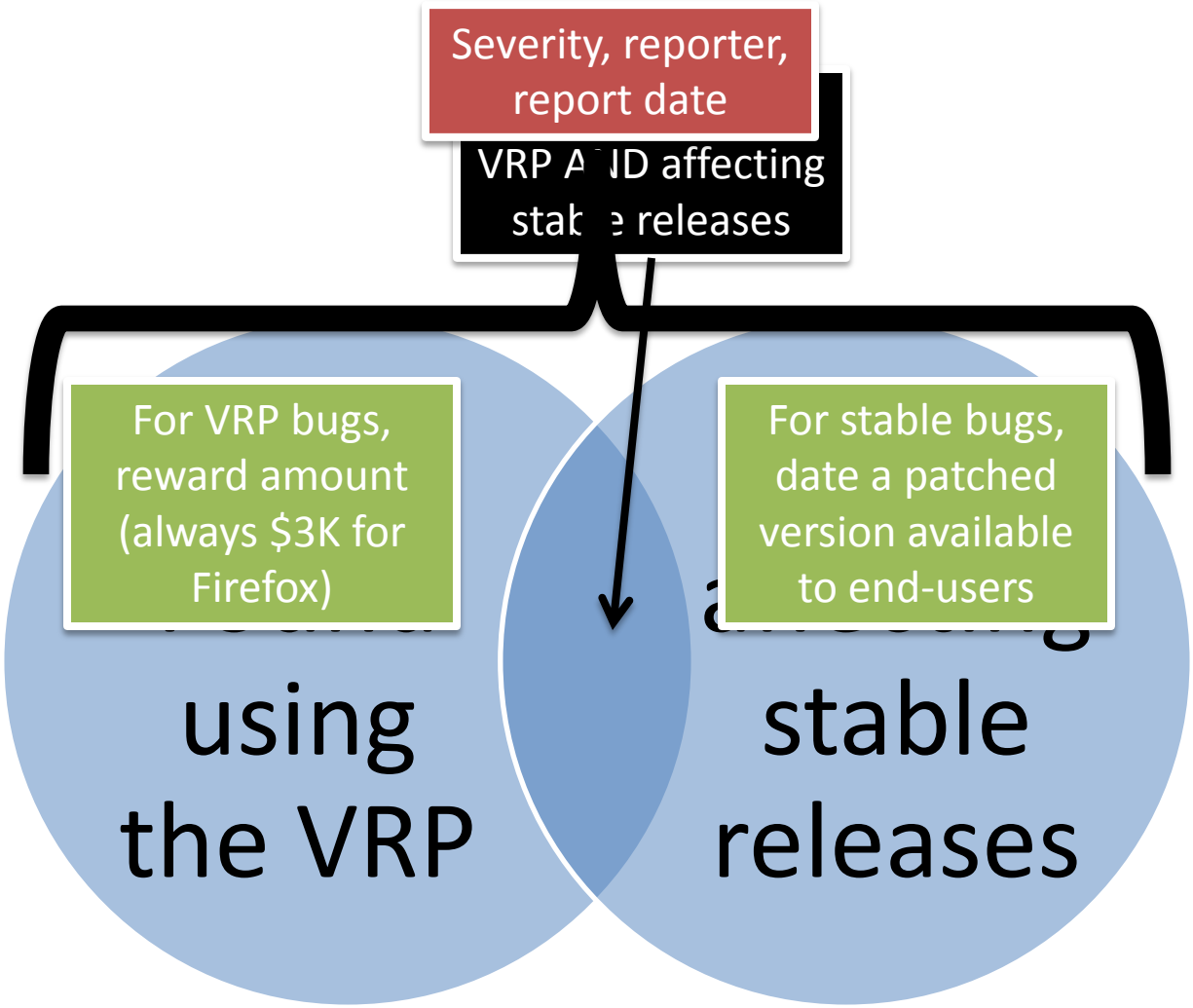
Chrome VRP

- Started in Jan 2010
- Rewards ranging from $500 to $1337
- Amounts increased over time to $1000--$3133.7
  - $31,336 for exceptional reports with patches

Firefox VRP

- Started in 1995 by Netscape
- Rewards increased to $3000 on July 1, 2010
- *All* high/critical vulns get $3000!

data


Severity, reporter, report date
VRP A JD affecting stab e releases
For VRP bugs, reward amount (always $3K for Firefox)
For stable bugs, date a patched version available to end-users
using the VRP
stable releases

Severity

- An ordinal measure of “badness” of a security bug
- Arbitrary code execution with user’s privilege on the OS considered critical severity by both browsers
  - Chrome has a privilege separated design and a memory corruption vulnerability in the “renderer” process is only high severity (same origin bypass)
  - Nearly all memory corruption vulnerabilities in Firefox are critical severity

Severity	Chrome Stable	Chrome Bounty	Firefox Stable	Firefox Bounty
Low	226	1	16	1
Medium	288	72	66	9
High	793	395	79	38
Critical	32	20	393	142
Unknown	8	13	59	0
Total	**1347**	**501**	**613**	**190**

software vendor perspective

1

Finding Bugs

Bugs found

- 27.5% of bugs affecting Chrome releases originate from VRP contributions (371 of 1347), and 24.1% of bugs affecting Firefox releases (148 of 613) result from VRP contributions.
  - **Effective!**
- Note that we are only looking at bugs affecting release versions!
  - 140 high/crit Jan-May ’13 in Chrome, only 40 found by VRP

Bugs found

- 27.5% of bugs affecting Chrome releases originate from VRP contributions (371 of 1347), and 24.1% of bugs affecting Firefox releases (148 of 613) result from VRP contributions.
  - **Effective!**

Bugs found

- 27.5% of bugs affecting Chrome releases originate from VRP contributions (371 of 1347), and 24.1% of bugs affecting Firefox releases (148 of 613) result from VRP contributions.
  - Effective!
- Total bugs found by Chrome VRP: 371
  - Max found by best internal researcher: 263
- 148 found by Firefox VRP (vs 48 by best internal)

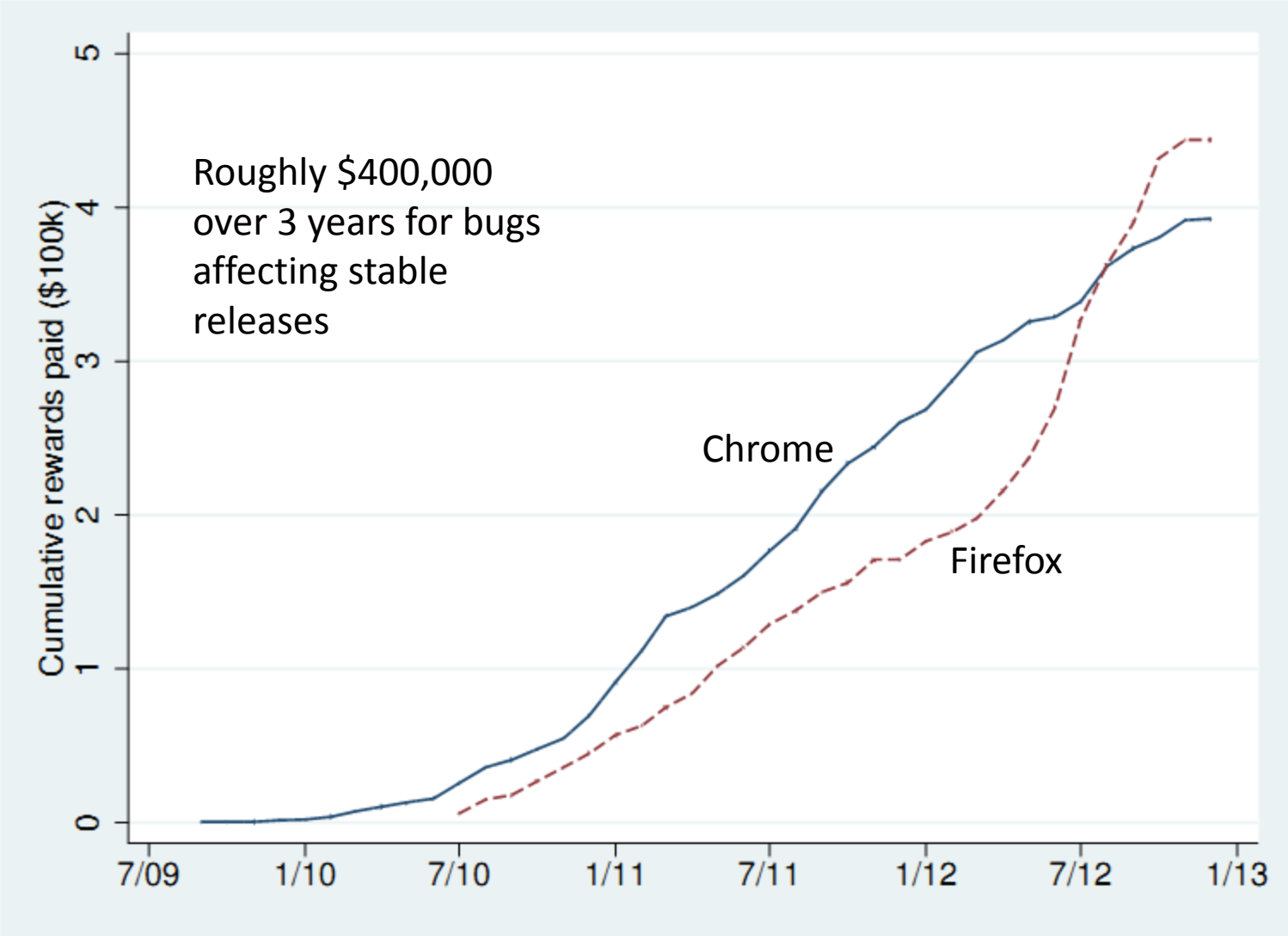
Bugs found

- 27.5% of bugs affecting Chrome releases originate from VRP contributions (371 of 1347), and 24.1% of bugs affecting Firefox releases (148 of 613) result from VRP contributions.
  - Effective!
- But is it cost-effective?

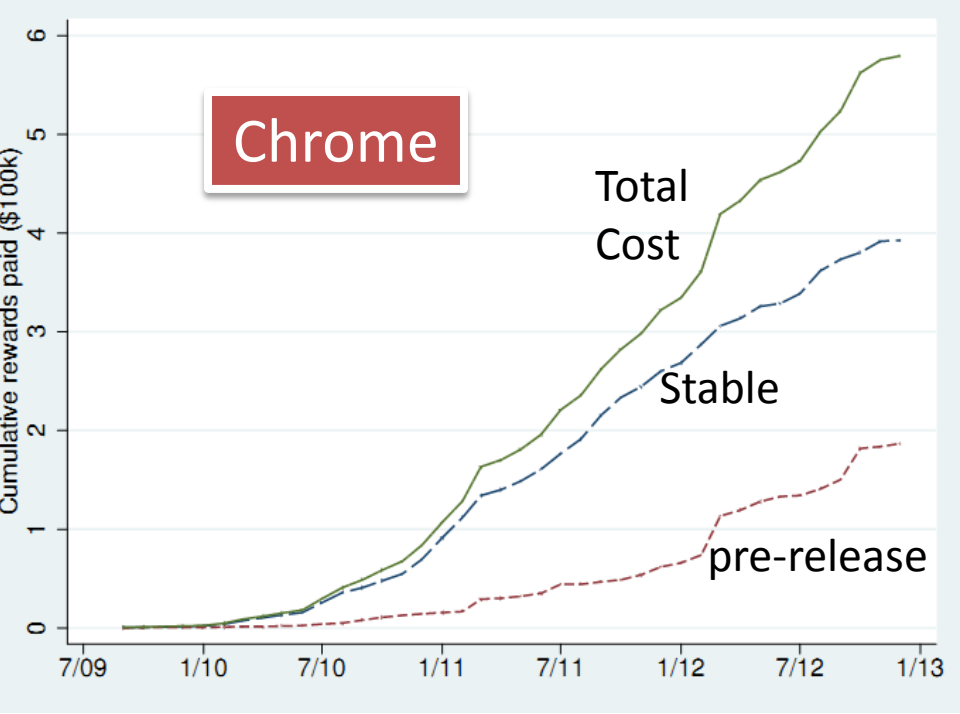
2

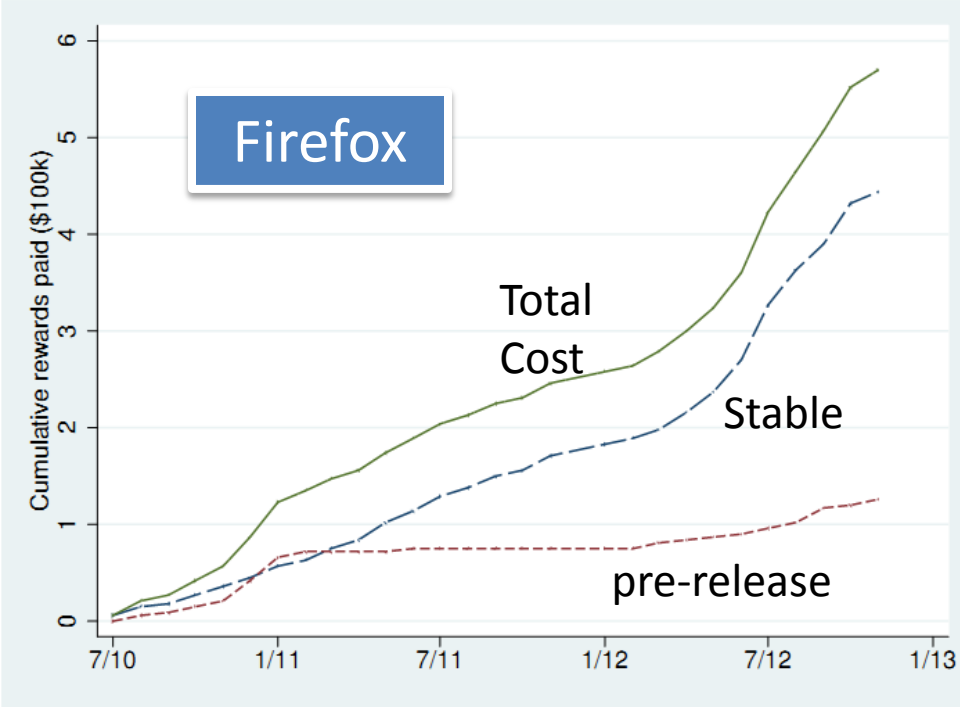
Cost

Cost of VRP


Roughly $400,000
over 3 years for bugs
affecting stable
releases
Chrome
Firefox
Cumulative rewards paid ($100k)
0
1
2
3
4
5
7/09
1/10
7/10
1/11
7/11
1/12
7/12
1/13

Cost of VRP


Chrome
Total
Cost
Stable
pre-release
Cumulative rewards paid ($100k)
0
1
2
3
4
5
6
7/09
1/10
7/10
1/11
7/11
1/12
7/12
1/13


Firefox
Total
Cost
Stable
pre-release
Cumulative rewards paid ($100k)
0
1
2
3
4
5
6
7/10
1/11
7/11
1/12
7/12
1/13

Cost of VRP

- Chrome total cost: $579,605 ($485/day)
  - $186,839 (32%) for non-release bugs
- Firefox total cost: $570,000 ($658/day)
  - $126,000 (22%) for non-release bugs
- Roughly, $190,000/year
  - Comparable to total cost of **ONE** security engineer
  - $100,000 + 50% overhead = $500/day
- But is it cost-effective? YES

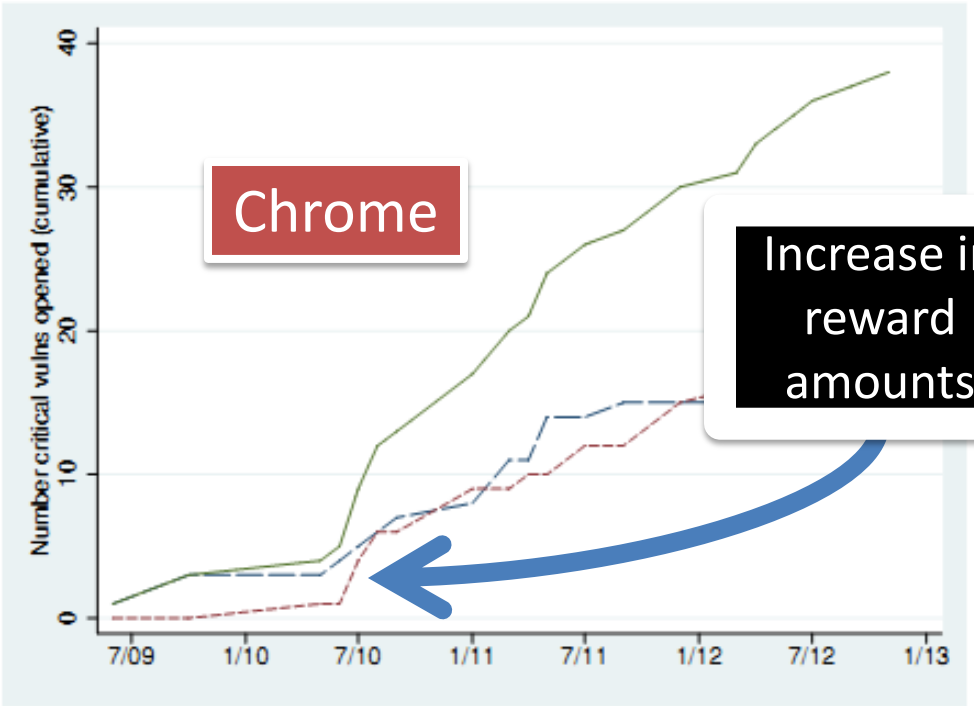
3

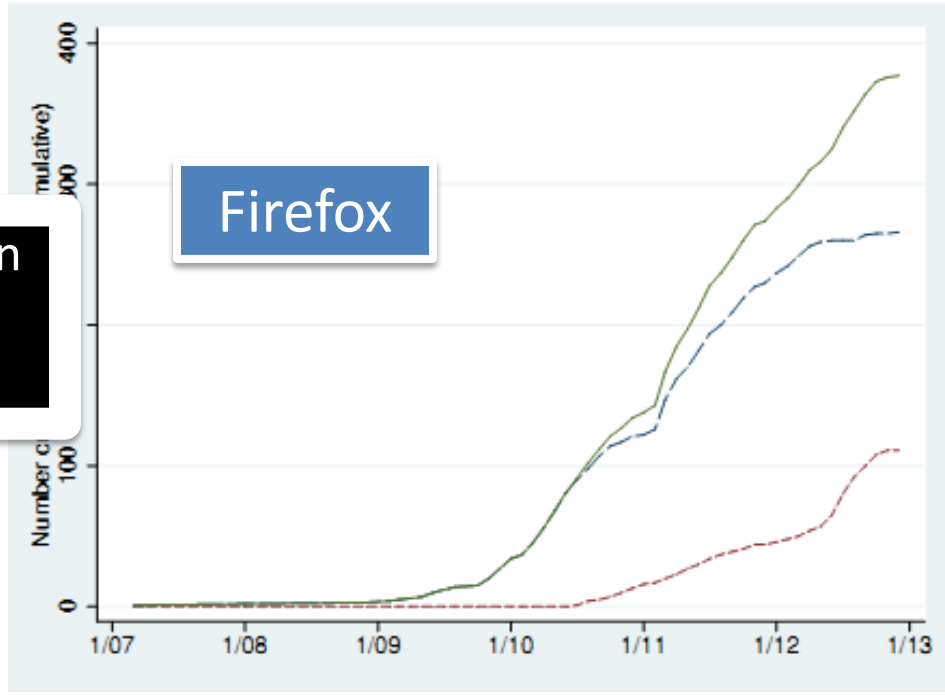
Community Engagement

Community Engagement

- Get more security bugs from the community

Community Engagement: Critical Bugs





internal (blue) vs external (red)

Community Engagement

- Get more security bugs from the community
  - VRP found more critical bugs in Chrome (release) than Internal researchers
  - For Firefox, internal researchers find the lion's share of critical vulnerabilities
    - Although, VRP impact is improving

Given enough eyeballs, all bugs are shallow

Linus’ Law

# Bugs	Freq.
1	45
3	2
4	1
6	1
10	1
12	2
13	3
16	1
17	1
22	1
24	1
27	1
35	1
48	1
92	1
Total	63

(a) Chrome

45/46 people only reported 1 high/critical bug

# Bugs	Freq.
1	46
2	9
3	4
5	1
6	1
9	1
10	1
12	1
14	1
47	1
Total	66

(b) Firefox

Dino A. Dai Zovi
@dinodaizovi

Follow

Linus' Law ("given enough eyeballs, all bugs are shallow") is oblivious of Bystander Effect. Everyone assumes someone else audited the code.

Reply Retweeted Favorite More

136 RETWEETS

45 FAVORITES

Maybe if we offer money?

Community Engagement

- Get more security bugs from the community
- Get more eyeballs on code
- Get more diverse bugs from the community
  - Chrome awards amounts ending with 337 for particularly smart/novel vulnerabilities
  - 31 such awards in our dataset
- Anecdotal evidence that it can lead to more bugs!
  - PinkiePie's exploit => full review of kernel API
  - a large number of similar issues found

software vendor perspective

From the Software Vendor's view

- Effective: ~25% of bugs affecting release
- Cost effective: comparable to ONE developer
- Community Engagement
  - More bugs from community
  - More eyeballs
  - Diverse bugs leading to finding more issues

security researcher perspective

1

Reward Amount

Chrome Reward Amounts

Amount ($)	Frequency (%)
500	24.75
1,000	60.08
1,337	3.59
1,500	2.99
2,000	2.99
2,337	0.60
2,500	0.60
3,000	0.20
3,133	1.80
3,500	0.20
4,000	0.20
4,500	0.20
[illegible]	[illegible]
7,331	0.20
10,000	1.40

95.8% of awards ≤ $3000 (Firefox)

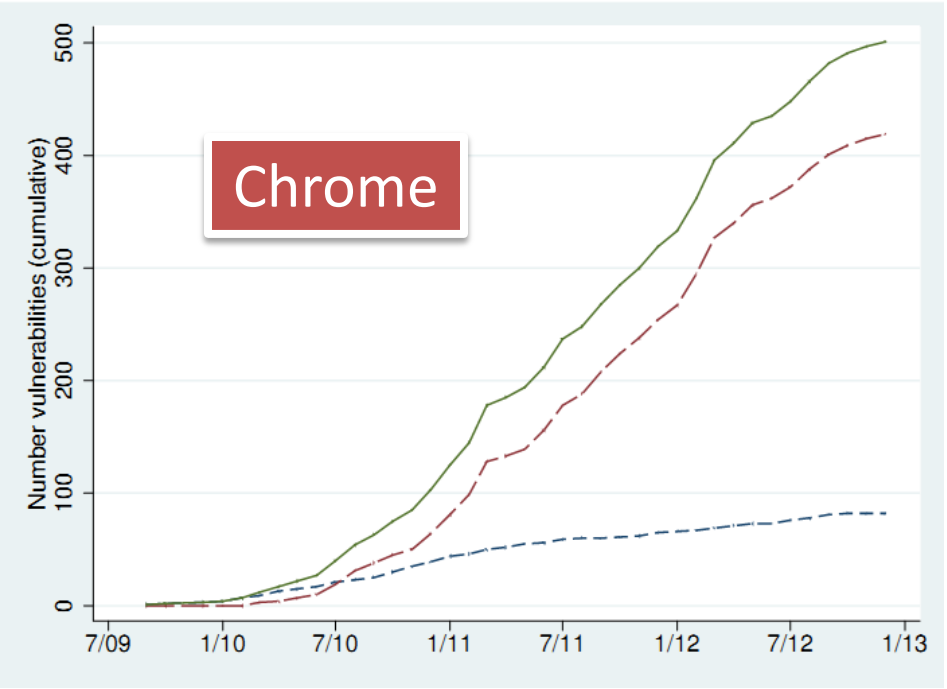
Reward Amounts

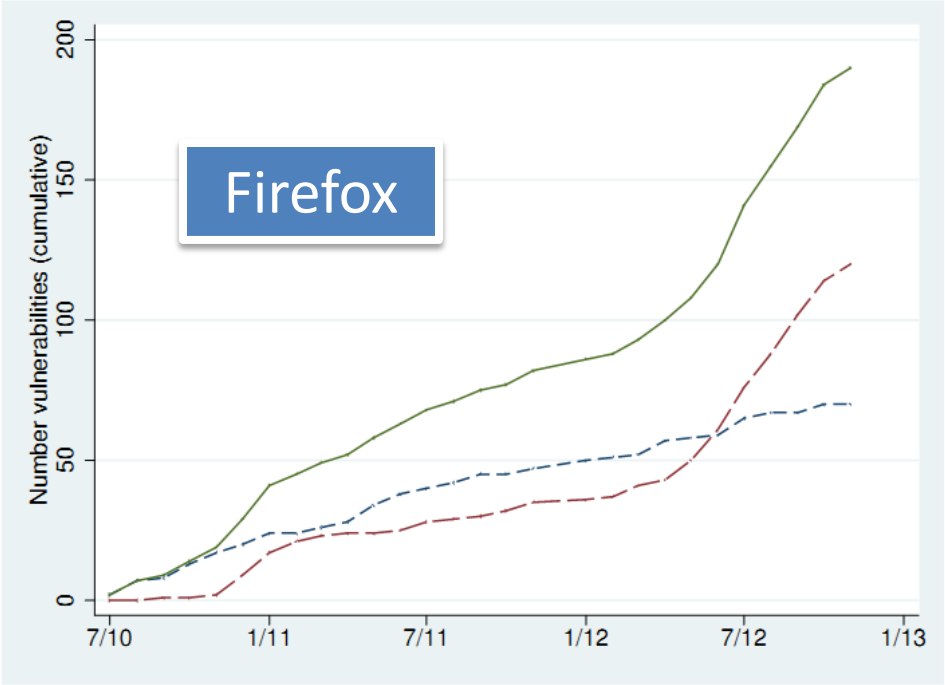
- Vast majority of rewards for Chrome under $1000 (median: $1000, mean $1156.9)
- Firefox award is $3000 (high/critical) or $0
- Lottery?
  - Low (or possibly negative) expected return on investment of finding bugs
  - But possibility of very large rewards!

2

Repeat Participation

First time vs. Repeat Contribution





First-time (blue) vs repeat (red)

3

VRP as Employment

Total Income

$ earned	Freq.
500	26
1,000	25
1,337	6
1,500	2
2,000	1
3,000	2
3,133	1
3,500	2
4,000	1
5,000	1
7,500	1
11,000	1
11,500	1
11,837	1
15,000	1
17,133	1
18,337	1
20,633	1
24,133	1
28,500	1
28,633	1
37,470	1
80,679	1
85,992	1
105,103	1
Total	82

(a) Chrome

$ earned	Freq.
3,000	46
6,000	12
9,000	4
12,000	1
15,000	1
21,000	1
27,000	1
30,000	1
36,000	1
42,000	1
141,000	1
Total	70

(b) Firefox

VRP as Employment

- The very best earn at the most $47,000 per year
  - Such a person likely to make much more working for Firefox and Chrome
- Both Google and Mozilla hired researchers found via VRPs
  - Hypothesis: The best security researchers bubble to the top, where a full-time job awaits.

security researcher perspective

From the Researcher's view

- Participation in a single VRP program likely not comparable to full-time employment
  - Although, good performance might lead to a job
  - Multiple programs could provide significant income
- Repeat participation is increasing
  - Suggests that researchers have a good experience with the programs
- Expected reward in Firefox higher than in Chrome
  - Although, possibility of much higher payoff in Chrome

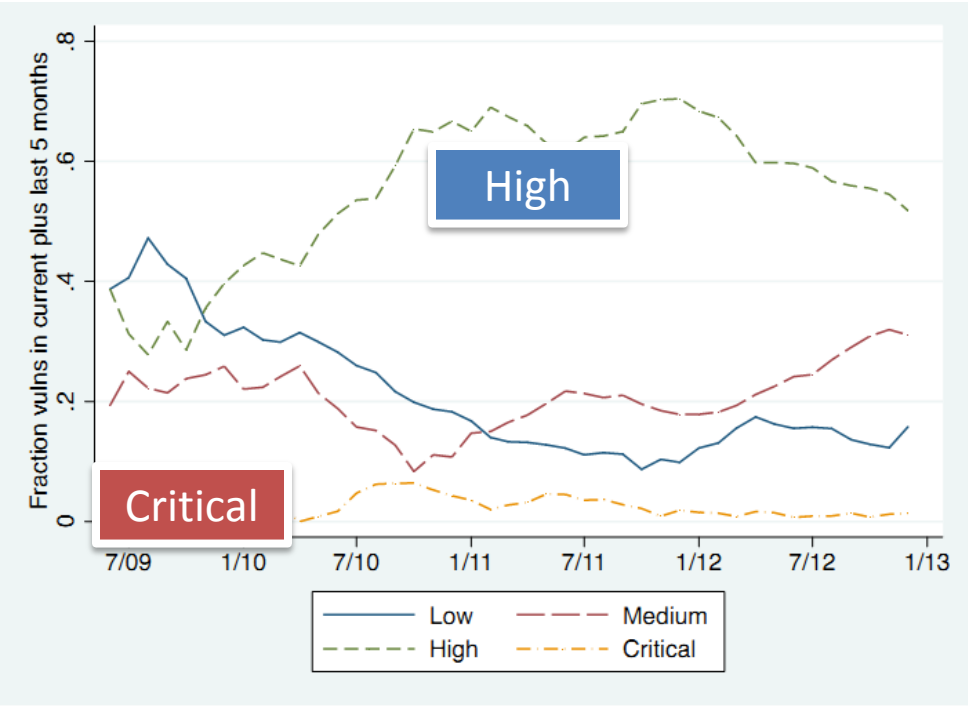
other analysis

Severity

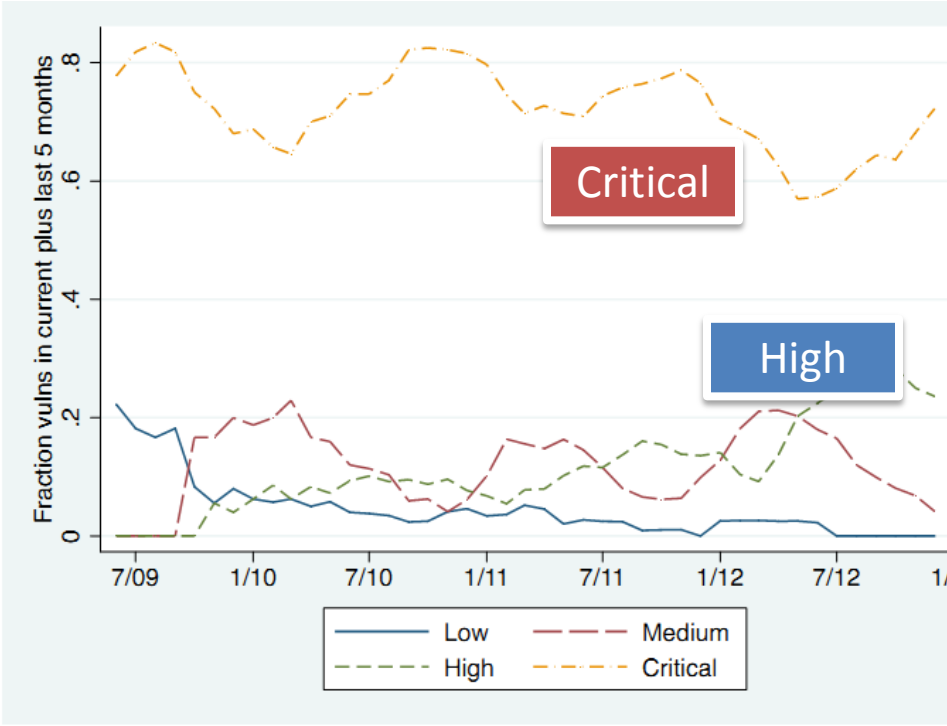
1

Severity	Chrome Stable	Chrome Bounty	Firefox Stable	Firefox Bounty
Low	226	1	16	1
Medium	288	72	66	9
High	793	395	79	38
Critical	32	20	393	142
Unknown	8	13	59	0
Total	**1347**	**501**	**613**	**190**

Fraction of Vulns by Severity



(a) Chrome



(b) Firefox

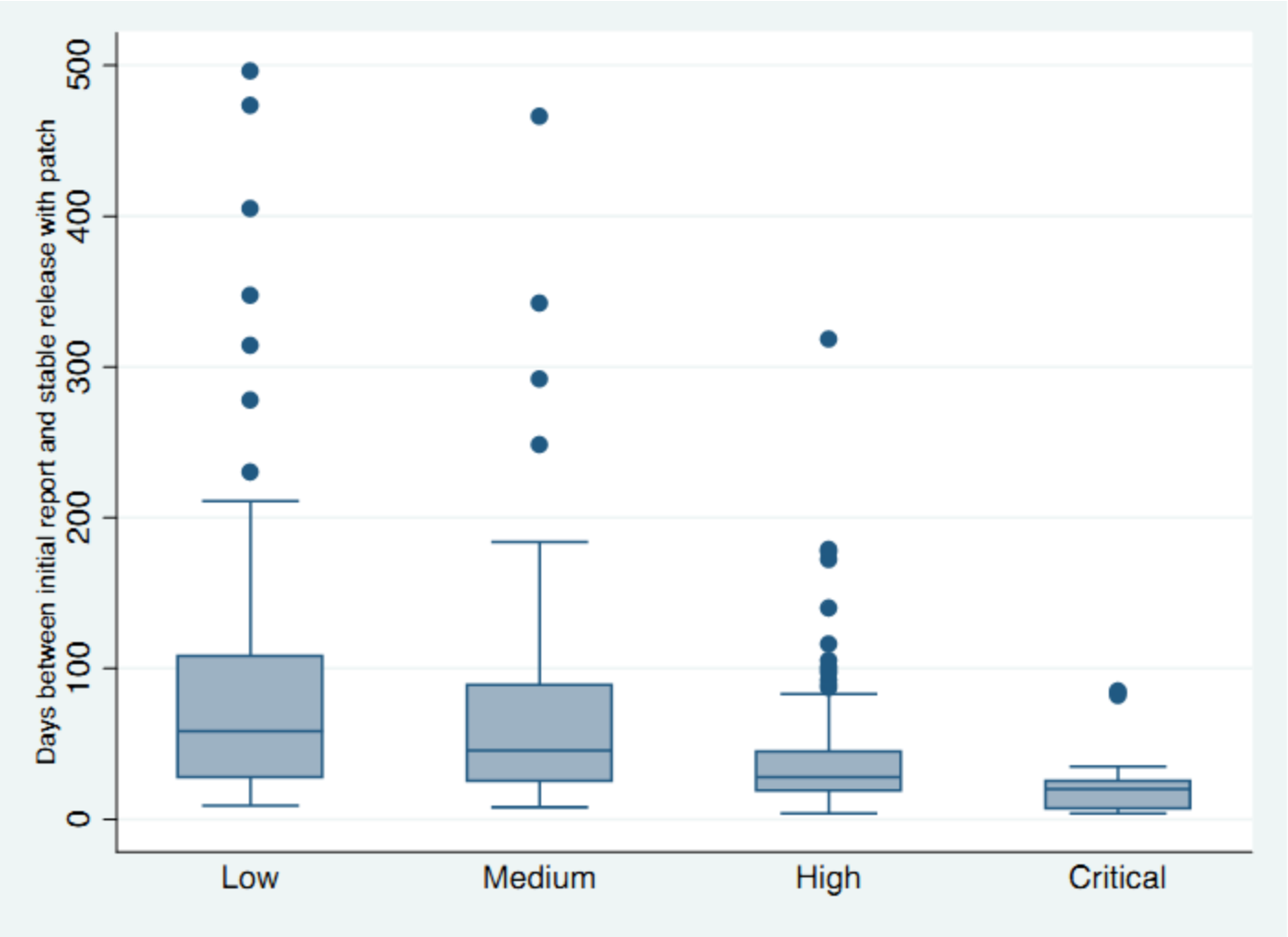
Hypothesis: This difference is due to privilege separation

2

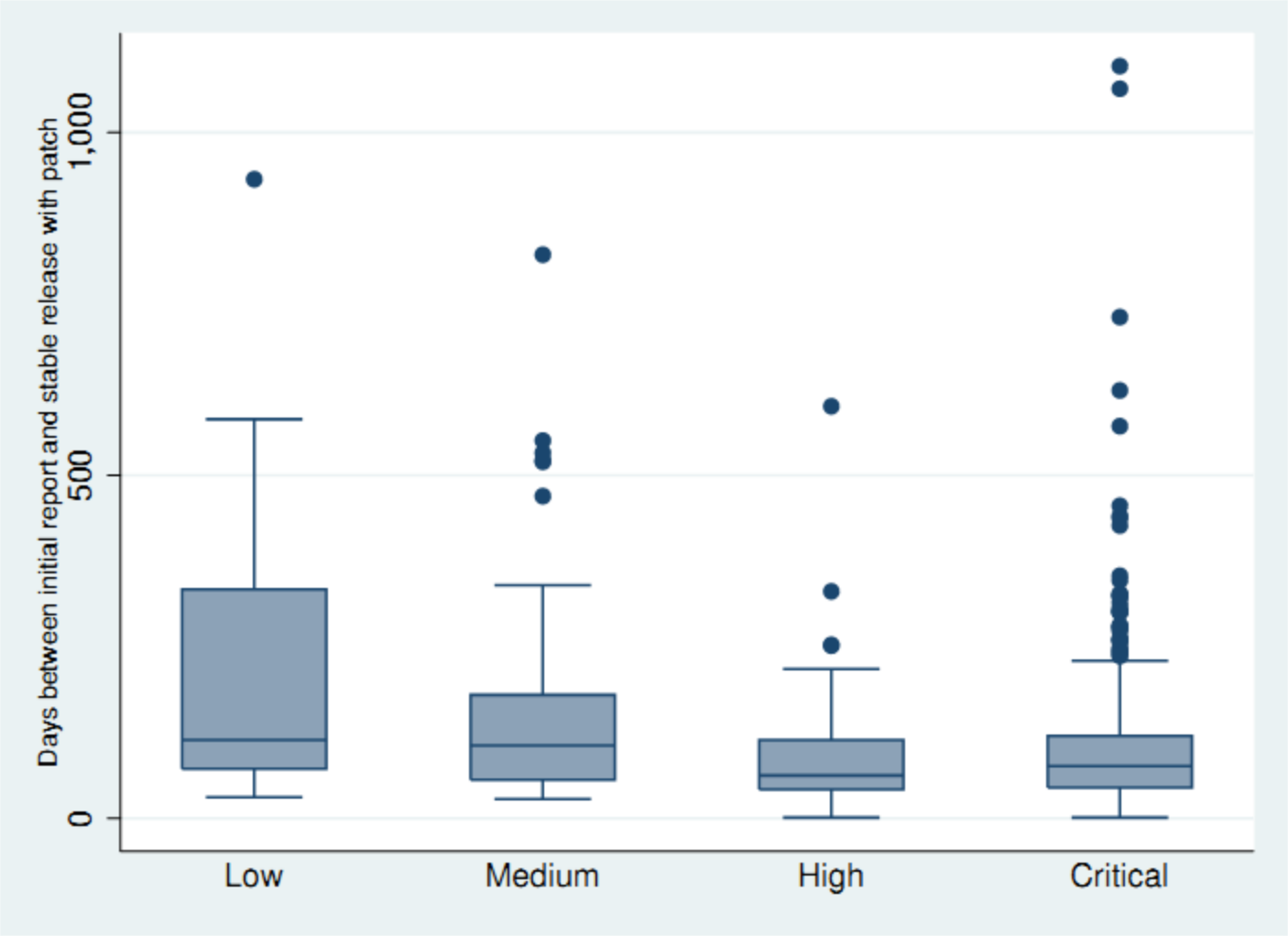
Time to Patch

Severity	Median, Chrome	Std. dev. Chrome	Median, Firefox	Std. dev., Firefox
Low	58.5	110.6	114	256.1
Critical	20.0	26.6	76	116.5

Table 6: Median and standard deviation of number of days between vulnerability report and release that patches the vulnerability, for each severity level.


Days between initial report and stable release with patch
0
100
200
300
400
500
Low
Medium
High
Critical

(a) Chrome


Days between initial report and stable release with patch
0
500
1,000
Low
Medium
High
Critical

(b) Firefox

Severity	Median, Chrome	Std. dev. Chrome	Median, Firefox	Std. dev., Firefox
Low	58.5	110.6	114	256.1
Medium	45.5	78.9	106	157.6
High	28.0	35.3	62.5	85.7
Critical	20.0	26.6	76	116.5

Hypothesis: This difference is due to privilege separation

final thoughts


chrome!
firefox!

Firefox vs Chrome

- Despite costing roughly the same, the Chrome VRP
  - Identified 3x bugs
  - More popular
  - Similar participation between repeat and first-time
  - External Researchers competitive with Internal researchers (for bugs in release versions)
- Why?

Possible Reasons

- Tiered Reward Structure
  - Incentivizes participation, keeps cost low
- Low variance/mean time to patch
  - Researchers like when bugs get patched quickly
- Higher Profile for Chrome
  - Pwnium, a high profile event
  - sudden top-ups for rewards
  - Such “gamification” leads to more participation

Recommendations for Vendors

- VRPs seem cost-effective strategy
- Try to reduce time-to-patch
- Consider tiered incentives like Chrome
- Architecture can have massive impact
  - See impact of privilege separation for Google Chrome

thanks

evil@berkeley.edu

https://www.cs.berkeley.edu/~devdatta

Thanks to Dan Veditz and Chris Evans for all their help