
# A Survey of Vulnerability Markets

## FIRST 2014

**Art Manion**
**amanion@cert.org**

# Copyright

# Vulnerabilities

A vulnerability is an abstract idea, a collection of conditions and behaviors that allows security to be violated.

- Often the violation affects an implied security policy: “Unauthorized access or activity is not permitted.”
- Artifacts or manifestations of a vulnerability can include source code, debugging or reverse engineering output, exploit or proof-of-concept code, URLs, network data, and more.
- For practical purposes, a vulnerability can usually be described as a design or implementation error.

Vulnerabilities are used to perform unauthorized activity and gain unauthorized access to data…

…and now it’s incident response time.

# Secrets

"The more value of an idea, object, activity, or sentiment is predicated on the restricted distribution of information about that idea, object, activity or sentiment, the more likely those persons who so define the value will organize as a secret society."

– Simmel's Proposition #1

# Secrets 2

"Control is a slightly different motivation for secrets. In this case, the information being kept secret is believed by the keeper to relate directly to the control of assets, processes, or knowledge that might give others the ability to more directly do harm or gain advantage."

– Towards a Taxonomy of Secrets, NSA Cryptologic Quarterly, Spring/Summer 2001-Vol. 20, Nos. 1-2

# Markets

Grand Bazaar, Istanbul, Turkey

# Vulnerabilities, Secrets, and Markets

A secret vulnerability has value to those who know about it

A secret vulnerability can be sold or licensed

- Or shared with affected vendors or other private groups

Value drops as soon as knowledge becomes widespread

- Using (“burning”) a vulnerability
- Independent discovery

Vulnerabilities exist, knowledge about a vulnerability does not preclude other’s discovery

- No guarantee of exclusivity

# Vulnerability Disclosure at CERT/CC

## Harm reduction

- Reduce number and impact of vulnerabilities
- One at a time when necessary, but we look for ways to scale

## Discovery

- File format fuzzers (BFF, FOE)
  - Current focus on crash validation and prioritization

## Coordination

- Identifying scope and affected vendors
- Private communication with researchers and vendors

## Public disclosure

- Vulnerability Notes Database

# Questions

What effects do vulnerability market activity have on the existing vulnerability coordination and disclosure ecosystem?

Who are the market actors and what can we find out about them?

What exactly is being traded, and how?

What are appropriate incentives to balance the benefits and costs of such markets?

How do you measure the cost-effectiveness of a bug bounty program?

# Terms

**Vulnerability**: Set of conditions, often design or implementation defects, that allow security violation and cause impact

**Exploit**: Software or actions that use a vulnerability to achieve impact

**Vendor**: Organization responsible for fixing vulnerabilities, typically a developer, manufacturer, or maintainer

**1st Party**: Organization that trades vulnerabilities in their own software

**3rd Party**: Organization that trades vulnerabilities in other's software

# 1st Party, 3rd Party

## 1st Party

- Vendor bug bounty
  - Vendors, buyer, own software

## 3rd Party

- Original finder
  - Finder, seller, other's software
    - VUPEN, Exodus Intelligence
- Broker
  - Buyer, seller, other's software
    - the grugq, Beyond Security
- Sponsored bounty
  - Bounty payer, other's software
    - IBB

# Survey Methodology

Identify and characterize market actors

- Buyers, sellers, brokers, 1st party, 3rd party, pricing, exclusivity
- Dates: March 1997 – June 2014

Analyze results

Review existing literature (incomplete)

- Characterize and compare
- Look for notable observations and conclusions

# Data Sources

## Open/publicly available

- Primary sources include bug bounty websites, official social media outlets, blogs, contracts
- Secondary sources include news articles, interviews, blogs
  - Also lists: Bugcrowd, HackerOne, Bugsheet, and others

## Quality and accuracy

- Best effort collection
- Manual characterization
- Lack statistically valid pricing data
  - Exception: Google and Mozilla bounty data

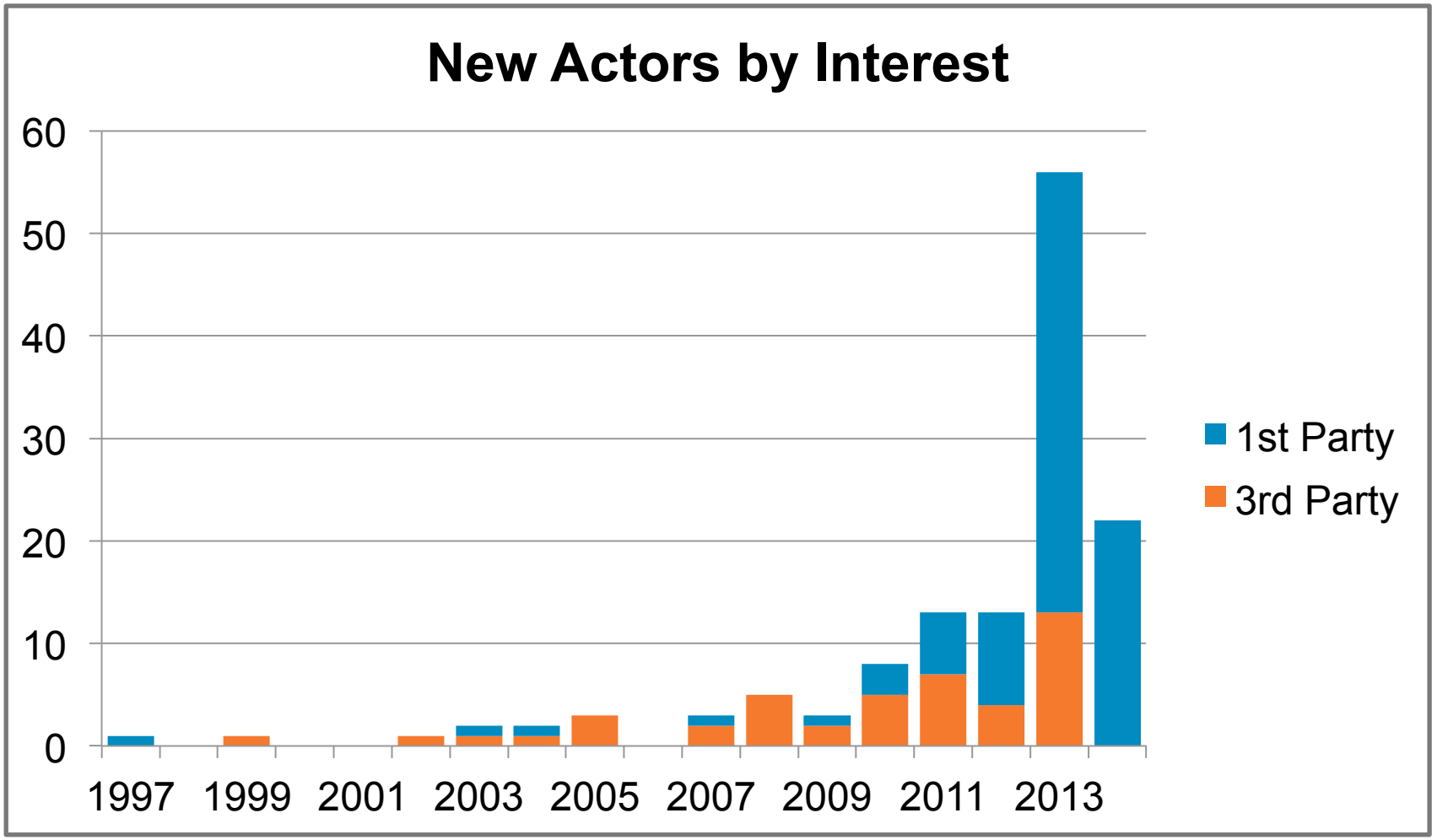
# Market Actors

| Role | Count |
|---|---|
| Actors | 128 |
| Buyers | 105 |
| Sellers | 18 |
| Brokers | 17 |

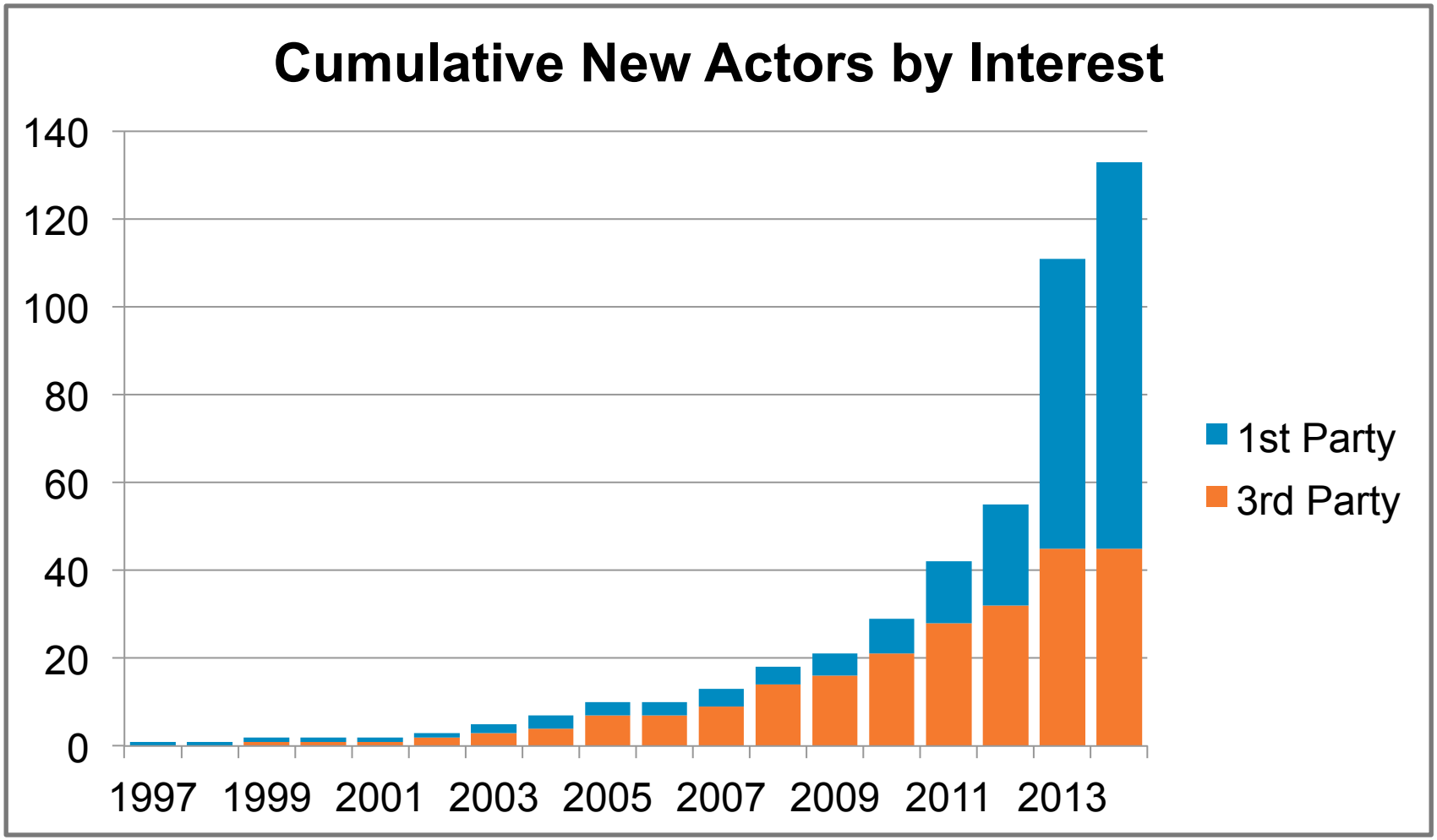
# Prices (USD)

| Price and Range | Minimum Buy | Median Buy | Maximum Buy | Maximum Sell |
|---|---|---|---|---|
| Low | 1 | 3 | 325 | 3,500 |
| Median | 713 | 8,169 | 5,874 | 1,033,857 |
| High | 25,000 | 150,000 | 75,250 | 6,000,000 |

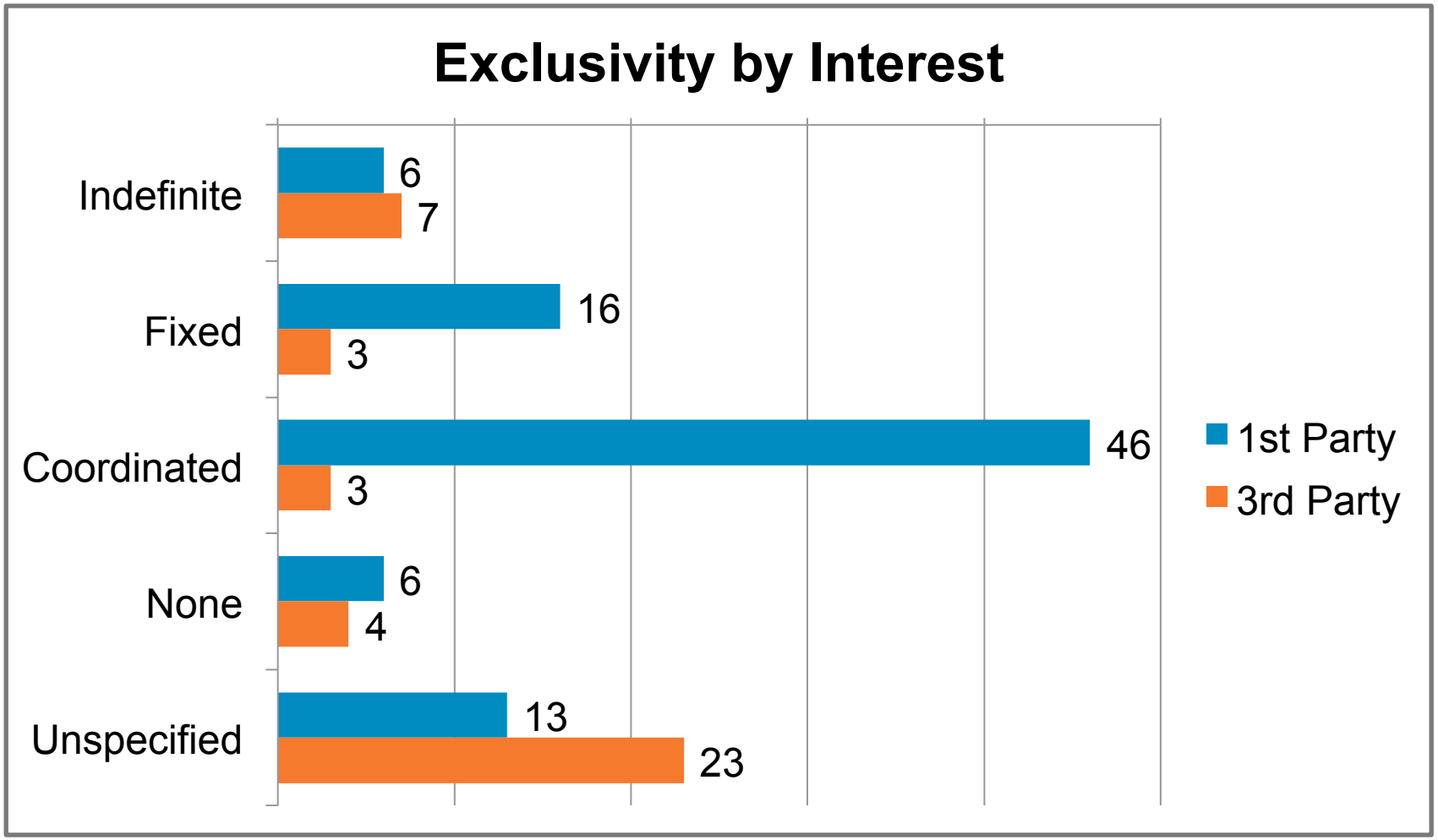
# Trends


New Actors by Interest
60
50
40
30
20
10
0
1997
1999
2001
2003
2005
2007
2009
2011
2013
1st Party
3rd Party

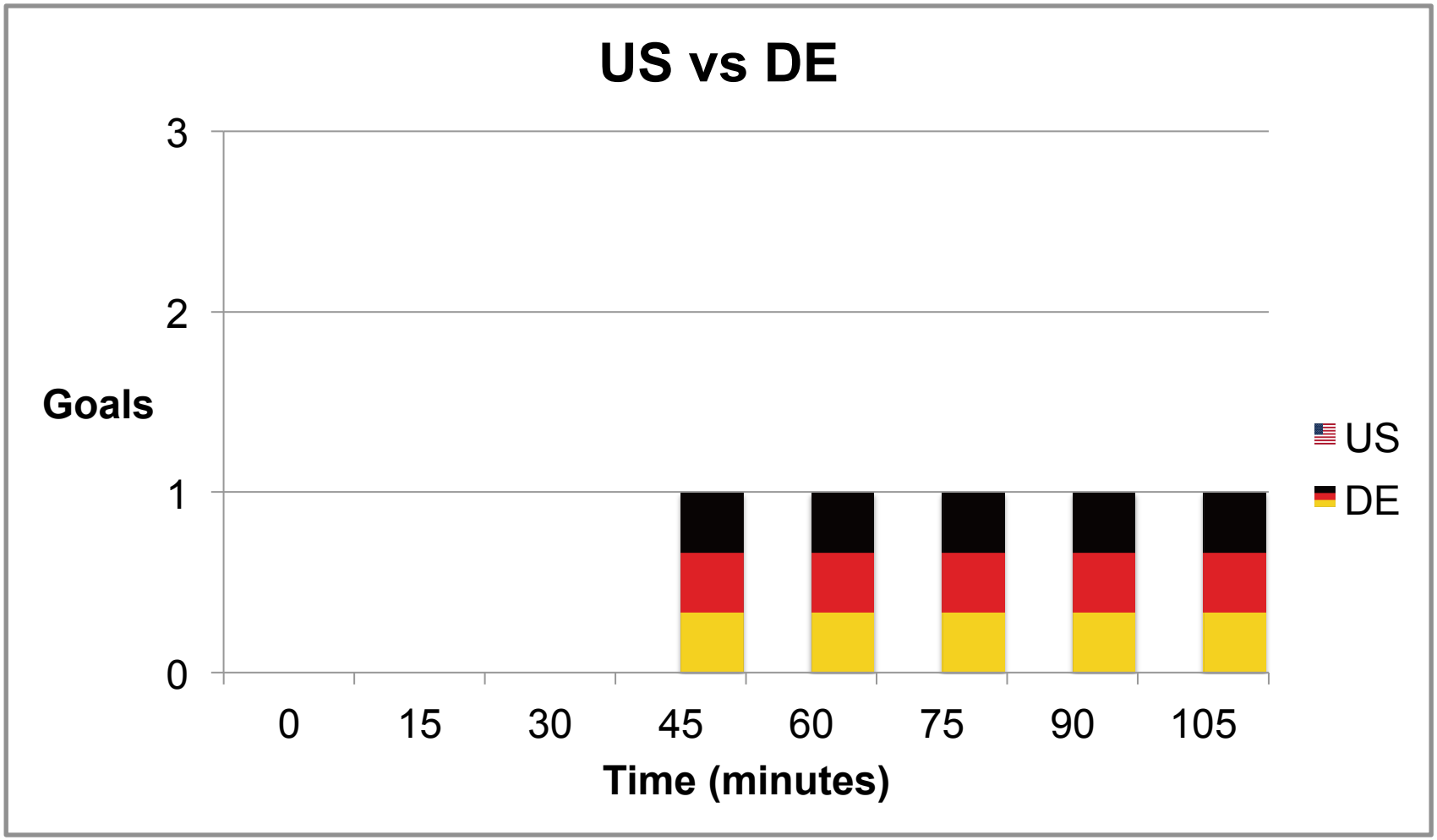
# Trends 2


Cumulative New Actors by Interest
140
120
100
80
60
40
20
0
1997
1999
2001
2003
2005
2007
2009
2011
2013
1st Party
3rd Party

# Trends 3


Exclusivity by Interest
Indefinite
6
7
Fixed
16
3
Coordinated
46
3
None
6
4
Unspecified
13
23
1st Party
3rd Party

# Trends 4



# Support Market

Are you a vendor who doesn't want the hassle of developing your own bug bounty management tools? …Outsource!

Emerging market of bug bounty platforms and services

- HackerOne
- Bugcrowd
- CrowdCurity

Further indication of market growth

# Influencing Markets

## Observation

- Operate a marketplace
  - Stock exchange

## Manipulation

- Proliferation of vendor (1st party) bug bounties
  - Microsoft IE 11 Preview Bug Bounty
- "international vulnerability purchase program" (IVPP, Frei, …and also Arce)
- Flood market with lemons?
  - Reputation barrier to entry
  - Lemon vulnerabilities would be detectable

# Perspectives

Common good

- The internet and supporting software can be considered a common good (or service)
- Some degree of personal privacy
- Global public interest is best served by vulnerabilities being fixed

Law enforcement, military, and intelligence capabilities

- National/public interest

# Observations

Offense pays better than defense

Security for those able to pay

Exclusivity

Increased secrecy around new vulnerability discovery techniques

- Use-after-free vulnerabilities in web browsers

Market competition

- Bug bounties versus zero-day sales

Recent research from Berkeley suggests that 1st party bug bounties are cost-effective

- Frei suggests a global purchasing program (IVPP)

# Acknowledgements

CERT/CC

- Joel Land
- Allen Householder

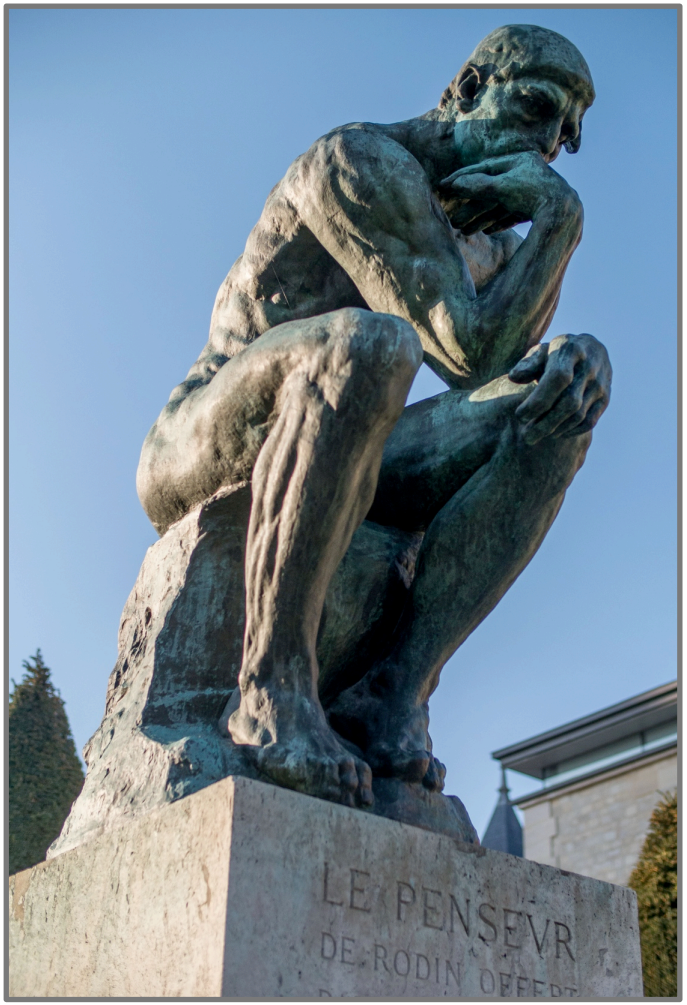
Carnegie Mellon University

- Nicolas Christin
- Rahul Telang

Others

- Too many public sources to list here, but worth mentioning are: Bugcrowd, Bugsheet, HackerOne, Stephan Frei, Finifter/Akhawe/Wagner

# Questions




Le Penseur

Rodin