Copyright

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material was prepared for the exclusive use of FIRST members and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0001442
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
“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.”

Markets

Grand Bazaar, Istanbul, Turkey
Dmgultekin CC BY-SA 3.0
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
1\textsuperscript{st} Party, 3\textsuperscript{rd} Party

1\textsuperscript{st} Party
- Vendor bug bounty
  - Vendors, buyer, own software

3\textsuperscript{rd} Party
- Original finder
  - Finder, seller, other’s software
    o VUPEN, Exodus Intelligence
- Broker
  - Buyer, seller, other’s software
    o the grugq, Beyond Security
- Sponsored bounty
  - Bounty payer, other’s software
    o 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

<table>
<thead>
<tr>
<th>Role</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actors</td>
<td>128</td>
</tr>
<tr>
<td>Buyers</td>
<td>105</td>
</tr>
<tr>
<td>Sellers</td>
<td>18</td>
</tr>
<tr>
<td>Brokers</td>
<td>17</td>
</tr>
</tbody>
</table>
## Prices (USD)

<table>
<thead>
<tr>
<th>Price and Range</th>
<th>Minimum Buy</th>
<th>Median Buy</th>
<th>Maximum Buy</th>
<th>Maximum Sell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>1</td>
<td>3</td>
<td>325</td>
<td>3,500</td>
</tr>
<tr>
<td>Median</td>
<td>713</td>
<td>8,169</td>
<td>5,874</td>
<td>1,033,857</td>
</tr>
<tr>
<td>High</td>
<td>25,000</td>
<td>150,000</td>
<td>75,250</td>
<td>6,000,000</td>
</tr>
</tbody>
</table>
Trends

New Actors by Interest

- 1st Party
- 3rd Party


Interest levels range from 0 to 60.
Trends 3

Exclusivity by Interest

- **Indefinite**: 1st Party - 6, 3rd Party - 7
- **Fixed**: 1st Party - 16, 3rd Party - 3
- **Coordinated**: 1st Party - 46, 3rd Party - 3
- **None**: 1st Party - 6, 3rd Party - 4
- **Unspecified**: 1st Party - 13, 3rd Party - 23
Trends 4

US vs DE

Goals vs Time (minutes)

US

DE
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
Thibswed, CC BY-SA 3.0