Responsibility for the Harm and Risk of Security Flaws
(Why Things are the Way They are)

Presented at OWASP AppSec Research 2010
by Cassio Goldschmidt
Sr. Manager, Product Security
What is Software?
Does it Matter?!?!
The Importance of Reviewing Our Beliefs
A Product
A Service

Responsibility for the Harm and Risk of Security Flaws
Speech

Responsibility for the Harm and Risk of Security Flaws
A Common Good

Responsibility for the Harm and Risk of Security Flaws
Common Goods can be “bad”
...and we all contribute to it.
...and we all contribute to it.

Today’s Agenda

Security Flaws

Corp. Users

Home Users

Sec. Researchers

Manufacturers

Government
Manufacturers
Industry Best Practices – SAFECode.org
No Effective Way to Prove Software Correctness
Investing in Security

Responsibility for the Harm and Risk of Security Flaws
Adopters
(Home Users, Corporate Users)
Users Want Features

US$28,724

- Reliable

US$28,724

- Convertible
- Rear Spoiler
- Alloy Wheels
- And Red!
Security Is Not “Visible”

Will home users be able to tell which one is more secure?
Network Effect Affects Decisions
Creation of an Ecosystem Affects Security

Responsibility for the Harm and Risk of Security Flaws
Ignoring updates put all of us at risk

• How often home users ignore this pop up?
Choosing to Adopt Software in Corporate Environments
Weaknesses Can Come From Different Sources

Partial Representation of the CWE Tree
Quarterly Freezes

December 2010

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
<th>Sunday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td>29</td>
<td>30</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Responsibility for the Harm and Risk of Security Flaws
Security Researchers
Security Researchers

- **Motivation:** Fame, money, curiosity, ideal
- **Consequences:** full disclosure vs. responsible disclosure

<table>
<thead>
<tr>
<th>Full Disclosure</th>
<th>Responsible Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fame</td>
<td>Fame (and work)</td>
</tr>
<tr>
<td>Virus as a byproduct</td>
<td>Slower to provide a fix</td>
</tr>
<tr>
<td>Poor fixes (zero days), can use Firewalls for immediate protection</td>
<td>Better fixes</td>
</tr>
</tbody>
</table>

- **Incentives:** Vulnerability market
  - iDefense pay for *finding* vulnerabilities
  - Will it pay for *creating* vulnerabilities?
  - Will it *leak* information to increase the value of their subscription?
Government
Government

• Hard to create effective laws
  – Banning Hacking tools
  – Cutting Internet access of users spreading virus
• Certifications (code reviews)
• Using Government buying power to promote security
  – Federal Desktop Core Configuration (FDCC)
• Providing incentives
  – Treating vulnerabilities like pollution
  – Will it kill the small players?
• Cases that went wrong: USC vs. Eric McCarty
• Industry moves too fast, will laws be able to keep up with it?
Conclusions
Summary

• Economics play a larger role than technical solutions
• Industry is moving in the right direction
  – Small players will follow industry leaders
• Government does not necessarily understand the problem
  – Creation on laws can cause more damage than good
• The creation of a vulnerability market can have unintended consequences
• Users need to step up with their education
Thank you!

Cassio Goldschmidt

This presentation is based on chapter 6 of “Information Assurance & Security Ethics” by Cassio Goldschmidt, Melissa Dark and Hina Chaudhry

ISBN: 978-1-61692-245-0 (hardcover)
ISBN: 978-1-61692-246-7 (ebook)