Privacy-Invasive Software
and Preventive Mechanisms

Martin Boldt
School of Engineering
Blekinge Institute of Technology
S-372 25 Ronneby
Sweden
martin.boldt@bth.se
The Spyware Problem (i)

- According to Earthlink (an American ISP) 55% of all Internet connected computers are infected with various kinds of spyware.
- Spyware exists because information has value.
- Spyware is a fuzzy concept without any proper definition.
- The fundamental problem is the lack of standard mechanisms for managing users’ informed consent during software installation.
The Spyware Problem (ii)

- We use the Gator software as an example of what users face on the Internet.
- During the installation users face an End User License Agreement (EULA).
  - It contains 6,645 words and is presented in a small window.
- Would you read it?
The Spyware Problem (iii)

- The EULA reveals that the following programs are installed:
  - eWallet
  - Precision Time
  - Date Manager
  - Offer Companion
  - Weatherscope
  - SearchScout Toolbar

- Such programs create large revenues for the their developers

- Spyware corporations report annual revenues in excess of $50 Million each
Agenda
 Introduction
 The Spyware Problem
 Privacy-Invasive Software
 Preventive Mechanisms
 Future Work
Violates existing laws

Might violate existing laws

Confusing experience

Follows required practices and laws

Follows optimal best practices
Software Behaviour

Malicious → Deceptive → Questionable → Acceptable → Exemplary

Spyware

- Violates existing laws
- Might violate existing laws
- Confusing experience
- Follows required practices and laws
- Follows optimal best practices
Privacy-Invasive Software (i)

- We introduce the term *Privacy-Invasive Software* (PIS) instead of using the term spyware
- Software that cause negative privacy implications
- More descriptive and less negatively emotive as other terms such as spyware, evilware, badware, or hijackware
  - Even if we use the term "invasive"
- We believe an invasion of privacy could be both tolerable and requested by the users if fully transparent
Privacy-Invasive Software (ii)

- Legitimate software is shown in white colour
- Spyware in light grey
- Malicious software in dark grey

<table>
<thead>
<tr>
<th>Consent Level</th>
<th>Tolerable negative consequences</th>
<th>Moderate negative consequences</th>
<th>Severe negative consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High consent</strong></td>
<td>Legitimate software</td>
<td>Adverse software</td>
<td>Double agents</td>
</tr>
<tr>
<td><strong>Medium consent</strong></td>
<td>Semi-transparent software</td>
<td>Unsolicited software</td>
<td>Semi-parasites</td>
</tr>
<tr>
<td><strong>Low consent</strong></td>
<td>Covert software</td>
<td>Trojans</td>
<td>Parasites</td>
</tr>
</tbody>
</table>
Preventive Mechanisms (i)

- Today’s anti-spyware tools use the same methods to target spyware as anti-malware tools use to combat viruses and worms.
- These methods are not optimal in the spyware context.
- “Innocent” software is negatively affected by anti-spyware tools.
Preventive Mechanisms (ii)

- We believe that new and more user-oriented countermeasures are needed.
- Mechanisms that inform users about how the software affect them and their computer system.
- We put forward the idea of using collaborative reputation systems to inform users.
- Reputation systems are successfully used by for instance Amazon.com, eBay.com and IMDb.com.
Preventive Mechanisms (iii)

- Gather previous users’ knowledge about software and present it to the new user
- Software reputations highlighted by such a system is the same as users today gain from computer magazines and Web sites
- We have developed a prototype tool, which is integrated into Windows XP’s installation process

http://www.softwarereputation.com
Firefox is about to execute

Program information
Filename: Firefox Setup 2.0.0.1.exe
Path: C:\Documents and Settings\A\o\Firefox Setup 2.0.0.1.exe
Filesize: 5971432 bytes
Rating: 9/10 (Excellent)
Description: Firefox (4.42.0.0)

Vendor information
Name: Mozilla
Rating: 9/10

Comment
1 of 1 users thought this comment was useful
Installer for latest version of Mozilla Firefox. Safe to run and good application, better than IE for safe web browsing. Very nice add-ons, especially mouse gestures.

Statistics
Last week (allowed/denied)
81.2% of 16

Development over last 30 days (allowed/denied)
11
Antagonistic intentions (i)

- In an initial attempt to address antagonistic intentions from community users, we assign each user a *trust factor*
- A user’s vote impact depends on this value
- The system also make use of a meta reputation system that allow community users to rate each others’ contributions
Antagonistic intentions (ii)

- It would also be possible to allow users to subscribe to the contributions from only a predefined subset of all community users, e.g. only a trusted subgroup

- The prototype rely on simple e-mail addresses for distinguishing between different users during registration

- Other measures than e-mail addresses are needed for identification
System impact

- The widespread use of such a system would help users prevent undesired software to covertly install on their computer.
- The PIS classification is transformed in the following way as the user is presented with information about software:

<table>
<thead>
<tr>
<th></th>
<th>Negligible Negative Consequences</th>
<th>Moderate Negative Consequences</th>
<th>Severe Negative Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Consent</strong></td>
<td>Legitimate Software</td>
<td>Adverse Software</td>
<td>Double Agents</td>
</tr>
<tr>
<td><strong>Low Consent</strong></td>
<td>Covert Software</td>
<td>Trojans</td>
<td>Parasites</td>
</tr>
</tbody>
</table>
The End

Questions?

More information is available at:
http://psi.bth.se/mbo/