Security, Availability, and Multiple Information Sources:
Exploring Update Behavior of System Administrators

Christian Tiefenau, Maximilian Häring, Katharina Krombholz, Emanuel von Zeeschwitz
@chrizzlz @cathykxx
Usable Security and Privacy Lab, Universität Bonn, Fraunhofer FKIE, CISPA Helmholtz Center
End user

“...no one can hack my mind”: Comparing Expert and Non-Expert Security Practices

Iulia Iones
Google
iuliona@nlon@gmail.com

Rob Reeder
Google
rreeder@gmail.com

Sunny Consolvo
Google
sconsolvo@gmail.com

ABSTRACT
The state of advice given to people today on how to stay safe online has plenty of room for improvement. Too many things are asked of them, which may be unrealistic, time consuming, or not really worth the effort. To improve the security advice, our community must find out what practices people use and what recommendations, if unmanaged well, are likely to bring the highest benefit while being realistic to ask of people. In this paper, we present the results of a study which aims to identify which practices people do that they consider most important at protecting their security online. We compare self-reported security practices of non-experts to those of security experts (i.e., participants who reported having the carefully considered the most worth-while advice to recommend in imperative. Even if this data [23, 41] is not thought about what is that is effective and read

Betrayed By Updates: How Negative Experiences Affect Future Security

Kami VanLeeuwen, Emilee Bader, Rick Wash
Department of Telecommunication, Information Studies, and Media
Michigan State University
{vanleeuwen, emilee, wash}@msu.edu

ABSTRACT
Installing security-relevant software updates is one of the best computer protection mechanisms. However, users do not always choose to install updates. Through interviewing non-expect Windows users, we found that users frequently decide not to install future updates, regardless of whether they are important for security, after negative experiences with past updates. This means that even non-security updates (such as user interface changes) can impact the security of a computer. We discuss three themes impacting users’ willingness to install updates: unexpected new features in an update, the difficulty of assessing whether an update is “worth it”, and confusion about why an update is necessary. Additionally, some updates combine security and non-security components, and it is not always clear to users which updates will improve security and which updates might make other changes. Some software updates are technically cumulative: all prior updates must be installed before the latest update can be installed. This means that security updates cannot be installed until the user decides to install earlier, non-security updates. This lack of differentiations, and the decisions companies make about how to roll out non-security updates, combined with the decisions users make about whether to install these updates, can potentially affect the overall security of users’ computers.

We interviewed Windows users about their opinions and be-
Updates and administrators?
Interviews

80 x Clients
35 x Virtual Machines
16 x Servers

300 x Clients
150 x Virtual Machines

170 x Clients
26 x Servers

600 x Clients

Zelko
Markus
Alexander
Milan

5 x Virtual Machines
10000 x Virtual Machines

5 x VM
100 x VM

Unknown

Lorenz
Cyril
Julian
## Process and Obstacles

<table>
<thead>
<tr>
<th>Phase</th>
<th>Step</th>
<th>Obstacles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Becoming aware</td>
<td>Unsatisfying communication with the publisher*</td>
</tr>
<tr>
<td></td>
<td>Further details</td>
<td></td>
</tr>
<tr>
<td>Deciding</td>
<td>Discussion</td>
<td>Stability (1); Risk of exploits (2); Performance (1); Priority (2); Missing expertise (1)</td>
</tr>
<tr>
<td>Preparation</td>
<td>Planning</td>
<td>Planning itself (3); Time of release (3); Communication (1); Missing documentation about the system and processes*</td>
</tr>
<tr>
<td></td>
<td>Backup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Waiting for release</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtaining the patch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Informing users</td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td>Test system</td>
<td>Testing itself (1); Broken dependencies (4); Resources*; Frequency of updates*</td>
</tr>
<tr>
<td></td>
<td>Pilot system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Problem solving with manufacturer</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>Installation itself</td>
<td>Failure (2); Missing configuration options (1); Social pressure; System resources (2); Complexity (3); Missing tools (3); Heterogeneous system (6); Company structure (3); Impact on systems/users (2); Downtime (1); Installation method (manual/automatic) (1,1)</td>
</tr>
<tr>
<td></td>
<td>User interaction</td>
<td>Waiting for users (1)</td>
</tr>
<tr>
<td></td>
<td>Reboot</td>
<td>Reboot itself (3); Old/Slow hardware (1)</td>
</tr>
<tr>
<td>Post-Installation</td>
<td>Documentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testing/Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reversing</td>
<td>Missing backup, failover, or redundancy*</td>
</tr>
</tbody>
</table>

Table 1: Overview of phases, steps, and obstacles. The number in brackets denotes the number of participants who mentioned this aspect in the interviews. *Additional obstacles were found through the questionnaire.
Process and Obstacles

- Information
- Deciding
- Preparation
- Testing
- Installation
- Post-Installation

- Complexity
- Planning
- Obstacles
- Heterogeneous Systems
- Broken Dependencies
Online Survey

Reddit
Twitter
Forums

67 Participants
22-55 years

41 Europe
19 North America
7 Rest of the world

34 SME
33 Large
Company size
Findings

Introducing Errors (n=66) 42%
Priority/Time (n=66) 39%
Downtime (n=67) 45%
Risk (n=67) 46%
Stability (n=67) 46%
Lack of Information (n=65) 52%
Breaking Dependencies (n=66) 50%
Performance (n=67) 76%
Lack of Education (n=67) 81%

Response 1 2 3 4 5

Introducing Errors
Priority/Time
Downtime
Risk
Stability
Lack of Information
Breaking Dependencies
Performance
Lack of Education

100 50 0 50 100

Percentage

Your Users
External Services
Other
Mailing Lists
Publisher Newsletter
Update Management Software
Online Publication/News

Main Source Additional Source

Process
Sources
Discussion

Keepers of the Machines: Examining How System Administrators Manage Software Updates

Frank Li
University of California, Berkeley
frankli@cs.berkeley.edu

Lisa Rogers
University of Maryland
lmrogers@umd.edu

Arunesh Mathur
Princeton University
amathur@cs.princeton.edu

Nathan Malkin
University of California, Berkeley
nmalkin@cs.berkeley.edu

Marshini Chetty
Princeton University
marshini@princeton.edu

ABSTRACT
Keeping machines updated is crucial for maintaining system security. While recent studies have investigated the software updating practices of end users, system administrators have received less attention. Yet, system administrators manage numerous machines for their organizations, and security lapses at these hosts can lead to damaging attacks. To improve security at scale, we therefore also need to understand how this specific population behaves and how to help administrators keep machines up-to-date.

In this paper, we study how system administrators manage software updates. We surveyed 102 administrators and interviewed 17 individuals to understand their experiences and how their methods compare.

While prior studies have investigated how end users deal with software updates [18,19,22,30–32,35,40,45,46,49,50], there has been less attention on system administrators, whose technical sophistication and unique responsibilities distinguish them from end users. Industry reports and guides on administrator patching exist (e.g., Sysadmin 101 [41]), but these lack peer-review and transparent rigorous methods. Prior academic work on system administrators is often dated and focuses on aspects of administrator operations other than updating (e.g., on general tools used [11]) or specific technical (rather than user) updating aspects. Given the critical role that system administrators play in protecting an organization’s machines, it behooves us to better understand how they manage updates and
Conclusion

Process  Obstacles  Sources  Tools
Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators

Christian Tiefenau, Maximilian Häring, Katharina Krombholz, Emanuel von Zezschwitz
@chrizzlz @cathykxx
Usable Security and Privacy Lab, Universität Bonn, Fraunhofer FKIE, CISPA Helmholtz Center

THANK YOU!