Living Dangerously:
A Survey of Software Download Practices

Jon Howell , Galen C. Hunt, David Molnar and Donald E. Porter

Abstract: *Client software, such as Windows .exe files, poses security risks but also adds important functionality that cannot yet be replicated with web applications. These risks can be mitigated by running client software inside a sandbox. Virtual machines offer an easily deployed mechanism to create such a sandbox.*

This motivates two key questions: Are today's virtual machine mechanisms sufficient to prevent harm from malicious software? Even if they are sufficient, does it matter – is it the case that everyone has moved on to web applications? We address these questions by carrying out a survey of three populations of computer users: two within Microsoft and one drawn from U.S. users of the Amazon Mechanical Turk service.

We note three key findings: First, all three populations download and run client software regularly: Over 70% of respondents in all three popluations download and run client software monthly or more often. Second, use of virtual machines for sandboxing is rare and inconsistently applied: 68% of respondents in all three populations say they use virtual machines "occasionally" or less often. Third, of those who gave a reason for not using VMs, 44% say it is "too hard." We conclude that today's users are exposed to risk from client software and that today's sandboxing mechanisms are inadequate to protect them.

1. Introduction

Client software, such as Windows .exe files, poses security risks but also adds important functionality that cannot yet be replicated with web applications. These risks can be mitigated by running client software inside a sandbox. Virtual machines offer an easily deployed mechanism to create such a sandbox. Are today's virtual machine mechanisms sufficient to prevent harm from malicious software? Even if they are sufficient, does it matter – is it the case that everyone has moved on to web applications?

We seek answers to two main questions:

- Do users today still download and run client software?
- If / when users download client software, do they use a virtual machine as a sandbox to protect their machine against unwanted side effects of that software?

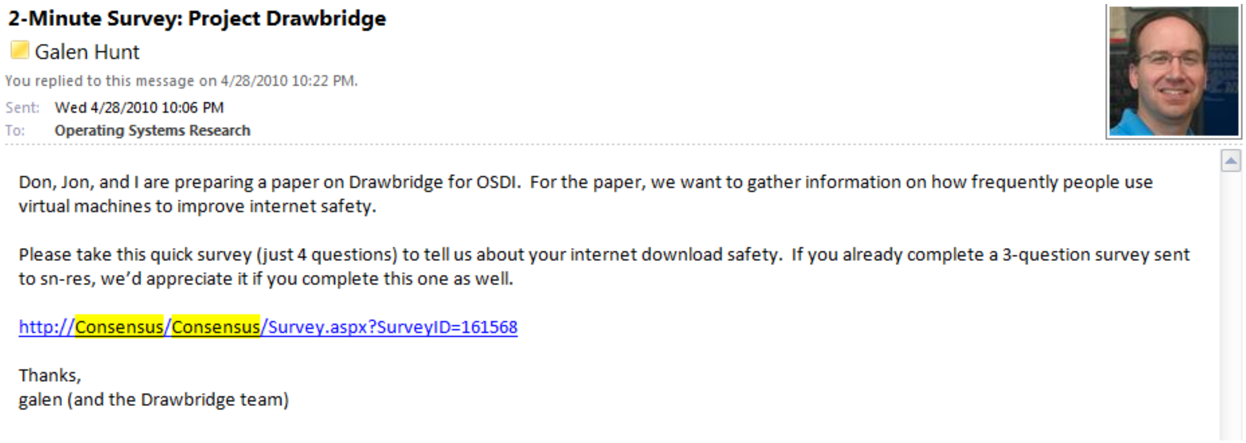
We approached these questions by launching surveys of three populations of computer users. We draw these conclusions:

- First, all three populations download and run client software regularly: At least 70% of every population downloads and runs client software at least monthly.
- Second, use of virtual machines for sandboxing is rare and inconsistently applied: At least 68% of every population uses virtual machines to reduce security risks occasionally or less often.
- Third, of those who gave a reason for not using VMs, 44% say it is “too hard”.

Together, these results indicate the need for more research into transparent sandboxing of downloaded client applications.

2. Survey Methods

Appendix A shows the text of our survey. We used two survey tools in our study. The first tool, **Consensus**, is a Microsoft internal web application developed for general purpose surveys of Microsoft employees. Participants are invited to a survey through e-mail containing a link to a URL with the survey ID.



2-Minute Survey: Project Drawbridge

Galen Hunt

You replied to this message on 4/28/2010 10:22 PM.

Sent: Wed 4/28/2010 10:06 PM

To: Operating Systems Research

Don, Jon, and I are preparing a paper on Drawbridge for OSDI. For the paper, we want to gather information on how frequently people use virtual machines to improve internet safety.

Please take this quick survey (just 4 questions) to tell us about your internet download safety. If you already complete a 3-question survey sent to sn-res, we’d appreciate it if you complete this one as well.

http://Consensus/Consensus/Survey.aspx?SurveyID=161568

Thanks,
galen (and the Drawbridge team)

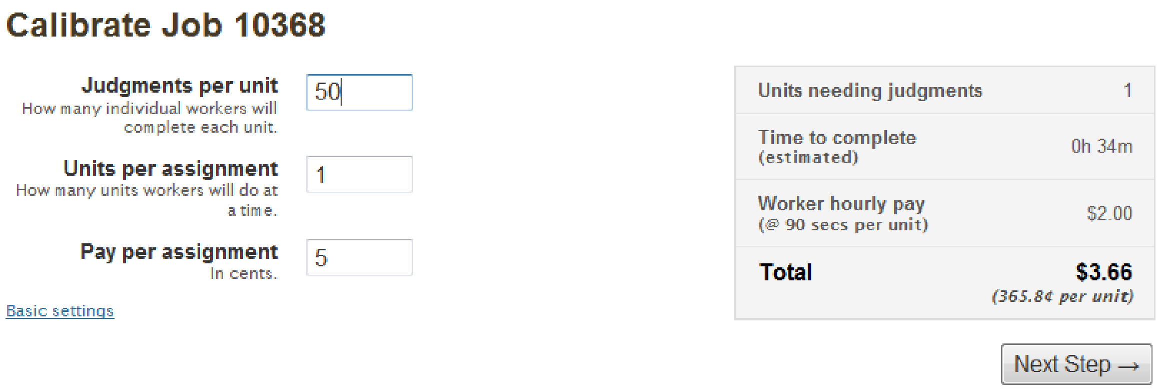
Example e-mail inviting participants to a **Consensus** survey.

Recipients of the e-mail are then free to accept or decline the invitation to the survey. If they accept by clicking on the URL, the **Consensus** application checks that the recipient has not previously completed the survey by using the Active Directory login of the recipient. The tool then shows the survey or shows an error message indicating that the survey may not be taken twice, as appropriate.

We used the Consensus tool for inviting participation from two separate populations within Microsoft. The first population consisted of researchers in Microsoft Research within the “systems and networking area,” which includes operating systems, sensor networks, networking, security, and other groups. The second population was a broader base of Microsoft employees.

The second tool, **Crowdflower** (http://www.crowdflower.com), is a front-end for Amazon’s **Mechanical Turk** “human computation” service. Mechanical Turk allows posting “human interface tasks” that may be completed by anyone on the Internet for a set fee. These tasks typically consist of things that can be done easily by a human but would be difficult for computers, such as identifying objects in pictures, transcribing audio, or summarizing text, but the platform can also be used to launch surveys. Mechanical Turk's greatest advantage is that it is a cost-effective way to reach large numbers of people: we recruited hundreds of respondents to our survey at $0.05 each in under a week.

Crowdflower makes it easier to create and manage Mechanical Turk tasks through a web-based interface. The Crowdflower interface includes tools for creation of the task UI, for specifying that a survey may only be completed by a worker once, and for setting the price offered to the Mechanical Turk worker. We were able to launch our initial Mechanical Turk survey in under an hour using Crowdflower's interface.



Calibrate Job 10368

Judgments per unit
How many individual workers will complete each unit.
50

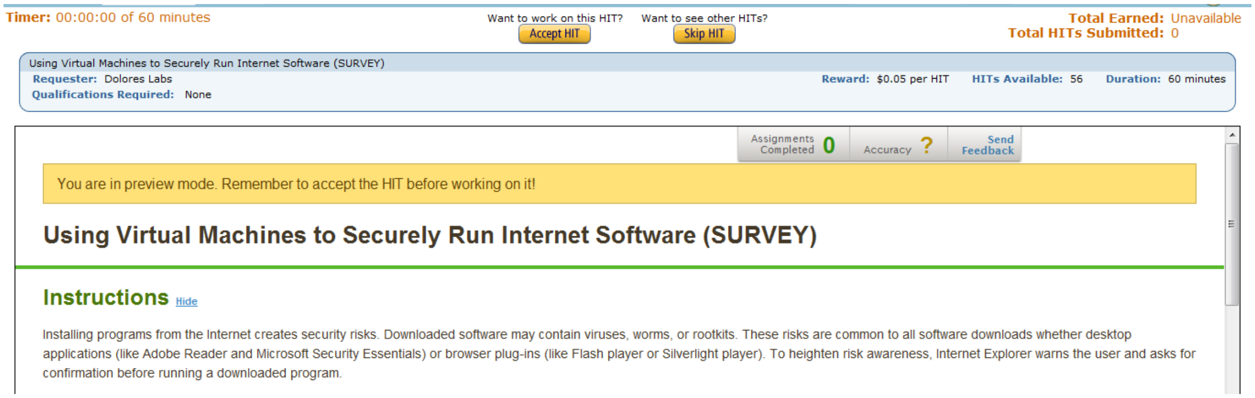
Units per assignment
How many units workers will do at a time.
1

Pay per assignment
In cents.
5

Basic settings

Units needing judgments	1
Time to complete (estimated)	0h 34m
Worker hourly pay (@ 90 secs per unit)	$2.00
Total	**$3.66** *(365.8¢ per unit)*

Crowdflower screen for ordering a Mechanical Turk task. This screen shows an order for a single "unit" (in our case, a unit is a single survey) to have 50 responses and pay 5 cents per response.



Timer: 00:00:00 of 60 minutes

Want to work on this HIT?

Want to see other HITs?

Total Earned: Unavailable
Total HITs Submitted: 0

Using Virtual Machines to Securely Run Internet Software (SURVEY)
Requester: Dolores Labs
Qualifications Required: None
Reward: $0.05 per HIT
HITs Available: 56
Duration: 60 minutes

Assignments Completed 0
Accuracy ?

You are in preview mode. Remember to accept the HIT before working on it!

Using Virtual Machines to Securely Run Internet Software (SURVEY)

Instructions

Installing programs from the Internet creates security risks. Downloaded software may contain viruses, worms, or rootkits. These risks are common to all software downloads whether desktop applications (like Adobe Reader and Microsoft Security Essentials) or browser plug-ins (like Flash player or Silverlight player). To heighten risk awareness, Internet Explorer warns the user and asks for confirmation before running a downloaded program.

Presentation of our survey on Amazon Mechanical Turk. In this screen shot, the worker is in "preview mode" and has not yet accepted the task of answering the survey. If the worker accepts the task, he or she has 60 minutes to complete the survey in exchange for $0.05 credited to an Amazon account.

2.1 Crowdsourced Survey Discussion

Mechanical Turk offers an inexpensive way to reach hundreds of people with a survey in a short time at modest cost. At the same time, Mechanical Turk differs in key ways from traditional surveys found in social science or from internal tools like Consensus. We briefly describe some of these caveats. In

Sections 3.4 and Section 4 we will discuss comparisons between our actual survey data from the Turk population and the Microsoft populations.

First and most fundamentally, Mechanical Turk workers are paid for their responses. This means that respondents are incentivized to “cheat” at tasks if this cheating helps them complete tasks more quickly. Crowdflower and Amazon provide various mechanisms to detect this cheating, but these mechanisms are oriented towards tasks that have a single “right answer” and where the results from one worker can be used to cross-check another. As we discuss further in Section 4, we detected such cheating in a large percentage of responses to our survey coming from outside the United States, leading us to focus only on the U.S. population.

Second, while Amazon makes efforts to ensure that one mechanical turk account maps to one person, the level of verification they can accomplish is less than provided by Microsoft’s internal Active Directory. As a result, it is possible that survey results on Mechanical Turk are influenced by a Sybil attack. We also observed cases where the same Mechanical Turk account was able to answer our survey more than once, despite our requesting the contrary. We removed all such cases from the data, but they show that there may be bugs lurking in either Amazon or Crowdflower.

These caveats have motivated research into the characteristics of Mechanical Turk as a survey tool. Kittur et al. in 2008 reported on initial experiences with user studies of Mechanical Turk workers, including a comparison to the results of a “traditional” user study. In 2009, Ross et al. surveyed demographics of Mechanical Turk workers. They found that when the workers were restricted to come from the United States, their demographics did not significantly differ from those of U.S. Internet users. Jakobsson performed an experiment that ran a survey on Mechanical Turk and the identical survey using an “established, independent survey company.” This test found no significant differences between the two participant pools. Horton et al. find that experiments with participants from Mechanical Turk and other online labor markets follow similar patterns and caveats as experiments with in-person participants.

While these works are not the last word, they suggest that Mechanical Turk warrants serious consideration as a source of participants for a user study. We report on the level of agreement between our Turk respondents and our Microsoft populations in Section 4. We have also included our survey in Appendix A; the reader may replicate our efforts through Crowdflower and Mechanical Turk if desired.

3. Results

The next three sections present the raw results from the three populations.

3.1 Survey of 51 operating systems researchers and engineers.

Our first population consists of researchers and engineers at Microsoft Research in the "Systems and Networking Area." This area includes operating systems, networks, security, and other groups. Members of this population are highly computer literate, most have PhDs in computer science or a related area. A total of 51 people responded between 28 April 2010 and 5 May 2010.

The summary of these responses is as follows:

1. How often do **you** download and run software from the internet?

	Response Count	Response %	
Daily (a few times a day)	4	7.8%	
Weekly (a few times a week)	8	15.7%	
Monthly (a few times a month)	25	49%	
Yearly (a few times a year)	14	27.5%	
Never	0	0%	

2. When **you** download and run software, how often do you use a virtual machine (to reduce security risks)?

	Response Count	Response %
Always	0	0%
Regularly	1	2%
Occasionally	8	15.7%
I may have tried it once or twice	15	29.4%
Never	27	52.9%

3. When running internet software, why don't **you** use a virtual machine more often?

	Response Count	Response %	
I don't download software, I only use web pages.	0	0%	
I only download and run signed programs that I trust.	16	31.4%	
Using a virtual machine is too hard or too expensive.	35	68.6%	

4. When **other people you know** download and run software from the Internet, how often, on average, do they use a virtual machine (to reduce security risks)?

	Response Count	Response %
Always	0	0%
Regularly	1	2.4%
Occasionally	2	4.9%
They may have tried it once or twice	18	43.9%
Never	20	48.8%
N/A (I couldn't say).	10	n/a

3.2 Survey of 173 Microsoft Employees

The second population consisted of a broader base of Microsoft employees within the Research division of the company. While these respondents are likely familiar with computers, they were not specifically researchers in operating systems. We received 173 responses between 30 April 2010 and 5 May 2010.

The summary of these responses is as follows:

1. How often do **you** download and run software from the internet?

	Response Count		
Daily (a few times a day)	7	4.0%	
Weekly (a few times a week)	48	27.7%	
Monthly (a few times a month)	90	52.0%	
Yearly (a few times a year)	28	16.2%	
Never	0	0%	

2. When **you** download and run software, how often do you use a virtual machine (to reduce security risks)?

	Response Count	
Always	2	1.2%
Regularly	10	5.8%
Occasionally	19	11.0%
I may have tried it once or twice	36	20.8%
Never	106	61.3%

3. When running internet software, why don't **you** use a virtual machine more often?

	Response Count		
I don't download software, I only use web pages.	1		
I only download and run signed programs that I trust.	65		
Using a virtual machine is too hard or too expensive.	107		

4. When **other people you know** download and run software from the Internet, how often, on average, do they use a virtual machine (to reduce security risks)?

	Response Count		
Always	0		0%
Regularly	1		0.8%
Occasionally	9		6.9%
They may have tried it once or twice	36		28%
Never	84		65%
N/A (I couldn't say).	43	n/a	

3.3 Survey of 444 Computer Users in the US via Mechanical Turk

Our final population consists of respondents from Amazon's Mechanical Turk service. We received 1005 total respondents from the United States and other countries between 30 April 2010 and 6 May 2010. The first 748 respondents were paid $0.05 for each survey, while the remaining respondents were paid $0.20. We increased the amount offered to speed the rate of response.

On closer inspection of the data, we observed that most of the responses from non-US countries were from India. We further observed that the responses from India were noisy, in some cases consisting of respondents entering all "a" to speed through the survey as quickly as possible. Therefore we elected to use only responses from Mechanical Turk workers in the United States.

The summary of these responses is as follows:

How often do **you** download and run software from the internet?

	Response Count	Response %	Overall %
Daily (a few times a day)	44	9.9%	
Weekly (a few times a week)	131	29.5%	
Monthly (a few times a month)	175	39.4%	
Yearly (a few times a year)	79	17.8%	
Never	15	3.4%	

2. When **you** download and run software, how often do you use a virtual machine (to reduce security risks)?

	Response Count	Response %	Overall %
Always	8	1.8%	
Regularly	30	6.8%	
Occasionally	45	10.1%	
I may have tried it once or twice	56	12.6%	
Never	305	68.7%	

3. When running internet software, why don't **you** use a virtual machine more often?

	Response Count	Response %	Overall %
I didn't know I could	219	49.3%	
I don't download software, I only use web pages.	10	2.3%	
I only download and run signed programs that I trust.	158	35.6%	
Using a virtual machine is too hard.	55	12.4%	
Other (please decribe below)	2		

4. comments from question 3, explain here: (See list below) We have more responses because they could type anything even if they didn't select "other"

5. When **other people you know** download and run software from the Internet, how often, on average, do you think they use a virtual machine (to reduce security risks)?

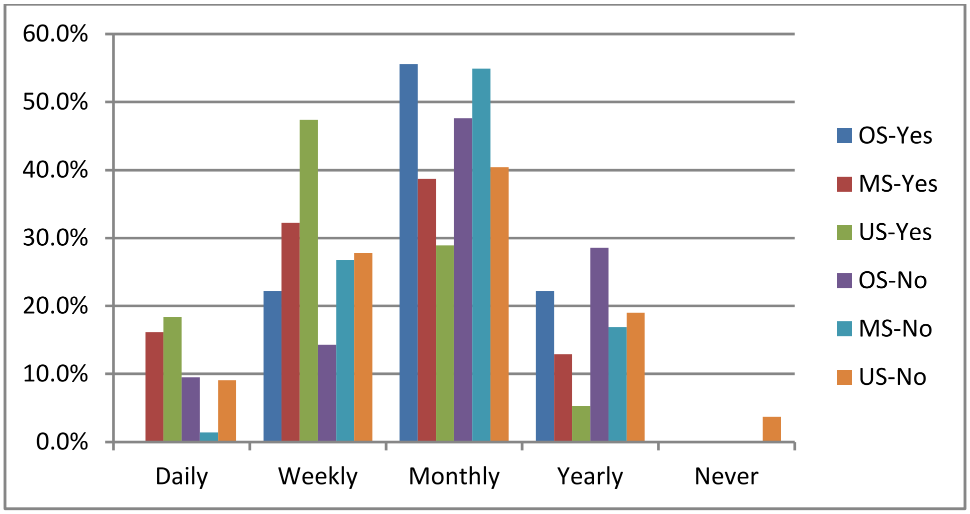
	Response Count		
Always	5	1.8%	
Regularly	15	5.5%	
Occasionally	65	24.0%	

They may have tried it once or twice	53	19.6%	
Never	133	49.1%	
N/A (I couldn't say).	173	n/a	

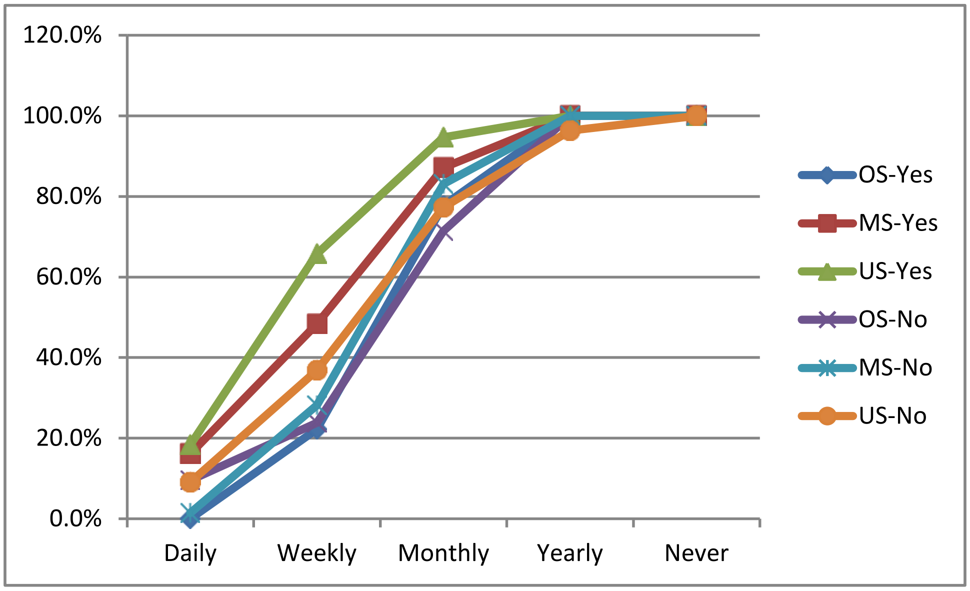
6. I had heard of virtual machine software (e.g. Virtual PC, VMWare, or Parallels) before taking this survey.

	Response Count	Response %	Overall %
Yes	223	50.2%	
No	221	49.8%	

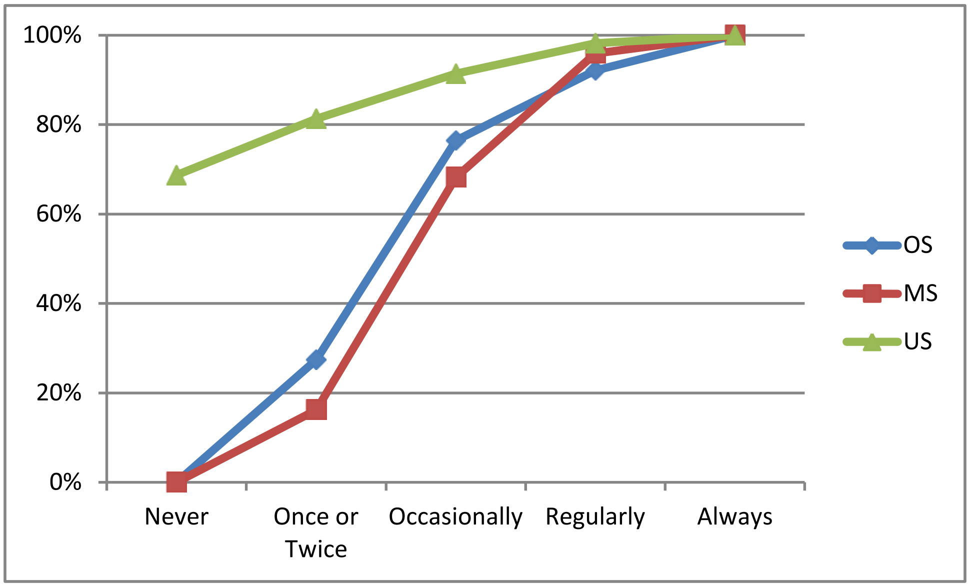
3.4 Comparing Populations



The bar chart above shows the percentage of each population with a given response to the question "How often do you download software from the Internet?" We have stratified populations based on how often the user uses a virtual machine to reduce security risks: "Yes" indicates users that reported "Always" or "Regularly", "No" indicates users that reported "Occasionally" through "Never." For example, a Microsoft employee not in the Operating Systems research area who may have tried using a virtual machine once or twice is counted in the "MS-No" category.



The graph above is a cumulative distribution function for each population with a given response to the question "How often do you download software from the Internet?" There is a weak correlation between using a virtual machine for protection and download frequency; of course, causality is not implied. An important conclusion is that, across all populations, at least 70% of respondents download new software at least once a month.



The graph above is a cumulative distribution function for each population with a given response to the question “When you download and run software, how often do you use a virtual machine (to reduce security risks)?” Note that, in every population, at least 68% of respondents use virtual machines occasionally or less.

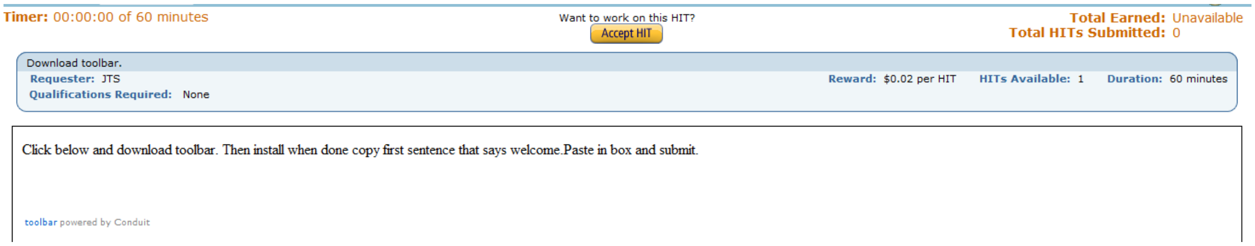
4. Discussion

Mechanical Turk users report downloading software a little more often than the general Microsoft population, and report using virtual machines to reduce security risks much less often than the general Microsoft population.

Some subjects’ free-form responses indicated a belief that the use of a Linux or Mac OS host operating system obviated security risks. Our favorite response from the free-form responses was: “The only people that need to use a virtual machine or a sandbox are those who routinely steal, pirate, and use cracked and illegally obtained software. People of that ilk should be in prison anyway.”

One threat to validity of our results is that each of our populations suffers from selection bias. It could be the case that users who are particularly security conscious and run virtual machines are also particularly reticient to respond to surveys. In the case of the Microsoft populations, we attempted to address this through repeated encouragement of our colleagues, but we had no equivalent social pressure to bear on the Turk population. One approach to address this would be to take a random sample of users and contact them directly.

A second threat to validity is that our survey relies on self reported data. Users are free to lie about their practices. Worse, because the intent of the survey was explicitly stated, users may have changed their behavior to “please” the experimenters. One approach to this problem would be a study that asks users to actually download and install software in exchange for a fee. In fact, we observe several tasks posted on Mechanical Turk that ask users to install browser toolbars or other client applications, in some cases for as little as two cents!



Timer: 00:00:00 of 60 minutes

Want to work on this HIT?

Total Earned: Unavailable
Total HITs Submitted: 0

Download toolbar.

Requester: JTS

Qualifications Required: None

Reward: $0.02 per HIT

HITs Available: 1

Duration: 60 minutes

Click below and download toolbar. Then install when done copy first sentence that says welcome.Paste in box and submit.

A Mechanical Turk task asking the viewer to download and install a toolbar for $0.02 Source: https://www.mturk.com/mturk/preview?groupId=1S2VCEXS18MSL38L5PWT3MNCZ1D95D

5. Related Work

Our study follows in a tradition of studies aimed at discovering users' attitudes towards security and privacy. For example, Jakobsson et al. performed a study to determine whether users would respond to a ``social phishing" e-mail that contained information about their friends. Egelman et al. used Mechanical Turk to discover how different explanations affected users' tolerance for security delays. Despite this tradition, however, we are not aware of a study that asks users about their software download habits, or about whether they use sandboxing mechanisms such as virtual machines.

Finally, as mentioned our work follows on previous work that uses Mechanical Turk as a source of research participants and work that investigates Mechanical Turk's suitability for this purpose. Our results add an additional data point for comparing the results of Mechanical Turk tasks to the same task as performed by a ``traditional" study population.

6. Conclusions

We now report some conclusions from our survey.

Users regularly download and install client software, across all populations. Our data shows that 70% of users download and install client software on a monthly basis or more often, across all reporting populations. 50% of Mechanical Turk respondents who were aware of virtual machines downloaded and installed software on a weekly basis. Client software downloads are not dead.

Even technically sophisticated users fail to use virtual machines. Fully 52.9% of our survey respondents in the Systems and Networking research area population stated that they "never" use virtual machines when downloading and installing software. This number jumps to 61.2% and 68.7% for the broader Microsoft population and the Mechanical Turk population, respectively. In fact, while zero respondents in the Microsoft populations stated that they "always" use virtual machines for sandboxing, 1.8% of respondents in the Mechanical Turk population stated this was the case.

Awareness, performance, and convenience are roadblocks to using virtual machines. Fully 49.8% of the general Mechanical Turk population was not aware that a virtual machine could be used to sandbox downloaded code. While the Microsoft populations were more aware, 68.6% of the Systems and Networking population and 61.8% of the broader Microsoft population cited performance and convenience as the reason they did not use virtual machines more often.

While our survey data has caveats, these results suggest today's users are exposed to risk from client software downloads. Furthermore, state of the art in virtual machine technology for sandboxing downloads is not sufficient for protecting users from malicious software downloads. The key areas for improvement are performance and convenience of sandboxing tools.

Acknowledgements

Thanks to A.J. Brush for lending her expertise in designing robust surveys.

Bibliography

S. Egelman, D. Molnar, N. Christin, A. Acquisti, C. Herley, and S. Krishnamurthi. Please Continue to Hold: An empirical study on user tolerance of security delays. Workshop on Economics and Information Security 2010.

A. Kittur, E.H. Chi, and B. Suh. Crowdsourcing User Studies with Mechanical Turk. In CHI '08: Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems, pages 453-456, New York, NY, USA, 2008. ACM.

J. Ross, A. Zaldivar, L. Irani, and B. Tomlinson. Who are the Turkers? Worker demographics in Amazon Mechanical Turk. Technical Report SocialCode-2009-01, University of California, Irvine, 2009.

M. Jakobsson. Experimenting on Mechanical Turk: 5 HOW-TOs. http://blogs.parc.com/blog/2009/07/experimenting-on-mechanical-turk-5-how-tos/ . July 2009.

Crowdflower. http://www.crowdflower.com

Amazon Mechanical Turk. http://mturk.amazon.com

T. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. Communications of the ACM, Volume 50, Issue 10. October 2007. Pages 94 – 100.

J.J. Horton and D.G. Rand and R.J. Zeckhauser. The Online Laboratory: Conducting Experiments in a Real Labor Market. (April 16,2010). Available at Social Science Research Network: http://ssrn.com/abstract=1591202

Appendix A : Survey Text

Using Virtual Machines to Securely Run Internet Software (SURVEY)

Instructions

Installing programs from the Internet creates security risks. Downloaded software may contain viruses, worms, or rootkits. These risks are common to all software downloads whether desktop applications (like Adobe Reader and Microsoft Security Essentials) or browser plug-ins (like Flash player or Silverlight player). To heighten risk awareness, Internet Explorer warns the user and asks for confirmation before running a downloaded program.

One way to improve safety and reduce the risk of downloaded software is to download and install it within a virtual machine (such as Virtual PC, Hyper-V, VMWare, Parallels, Xen) instead of directly to your computer. Some other ways to improve safety are to run only signed programs from trusted providers.

After taking the survey click "Submit" to save your changes.

This survey **is** anonymous.

1. How often do you download and run software from the internet? (required)

○ Daily (a few times a day)

○ Weekly (a few times a week)

○ Monthly (a few times a month)

○ Yearly (a few times a year)

○ Never

2. When you download and run software, how often do you use a virtual machine (to reduce security risks)? (required)

○ Always

○ Regularly

○ Occasionally

○ I may have tried it once or twice

○ Never

3. When running internet software, why don't *you* use a virtual machine more often? (required)

○ I didn't know I could

○ I don't download software, I only use web pages

○ I only download and run signed programs that I trust

○ Using a virtual machine is too hard

○ Other (please describe below)

4. If you said other on Question 3, explain here:

5. When *other people you know* download and run software from the Internet, how often, on average, do you think they use a virtual machine (to reduce security risks)? (required)

○ Always

○ Regularly

○ Occasionally

○ They may have tried it once or twice

○ Never

○ N/A (I couldn't say)

6. I had heard of virtual machine software (e.g. Virtual PC, VMWare, or Parallels) before taking this survey. (required)

○ Yes

○ No

Appendix B

Comments on Question 4 from Mechanical Turk survey of US population.

1. Too much time involved in running the program in a virtual machine
2. Too much cpu.
3. Too arduous to configure a vm image when antivirus protection is sufficient.
4. The programs I download are very unlikely to be dangerous because I only download from trusted sources and programs for OS X have fewer security risks.
5. The only people that need to use a virtual machine or a sandbox are those who routinely steal, pirate, and use cracked and illegally obtained software. People of that ilk should be in prison anyway. In almost 20 years online and hundreds of software downloads, I have never encountered any issues. Of course I only downloading legitimate, legal software from trusted (preferably the manufacturers) sources. C'mon dudes...do you actually expect me (or your intended market) to believe your nonsense that a download and install of Microsoft Security Essentials direct from Redmond is somehow a security risk? I call BULLSHIT!
6. Takes time and resources to run a VM
7. Setting up a virtual machine is alright for heavy testing of large complex software, but I usually just use Sandboxie for anything I download that seems suspicious.
8. Overkill. I know what I download from trusted vendors, use antivirus, etc. Never had a problem. So why would I go through the trouble of using a VM ?
9. Not all the software I download has the level of risk that I feel warrants installing in a VM.
10. No need. I take the safety precautions in a normal operation environment.
11. Never heard of it before now
12. My computer doesn't have the RAM or whatever. I installed one but when it restarted everything was messed up, I had to do a restore from before that.
13. Most software I download is trusted, and booting up a virtual machine usually takes longer than is desirable.
14. I've never heard of virtual machine. I'd like to know more though.
15. I've never had need of it.
16. it's too much of a pain to install the virtual machine etc. When if i screw something up I can either just restore or reinstall the os on my computer.
17. It's scary downloading random peoples files
18. It's not necessarily that it's too hard, it's more that it's a hassle and I trust most of the software I download enough that a VM is overkill.
19. it's a lot of extra work to install it first on a virtual machine and if it's OK from the normal computer. Besides I try only to download software from official sites.
20. I'm comfortable enough with my technical knowledge that I don't feel the need to take the extra precautions.
21. I usually use a separate "bastion host" computer between (2) hardware firewalls to download & test software. Virtual machines do not solve all of the security issues, especially those of

Microsoft Windows.

22. I use VM's often already.
23. I use it every time.
24. I use a VM (Virtual PC 2007 running a lean XP image) for any software that I am not familiar with. But programs that I am familiar with and plan to install, I just run a AV scan on the downloaded file.
25. I use a virtual machine.
26. I use a virtual machine for most software I download for the Internet, but I feel I can trust signed software I'm familiar with from well-known providers (Microsoft, Google, Apple, etc.) sufficiently to waive the precaution.
27. I tried it once and it made it so that I couldn't use Google Chrome anymore
28. I run Linux
29. I really don't understand the concept or how. usually when i use one it is accidental.
30. I only run software I trust.
31. I never really saw the need for it.
32. i never had a virus
33. I know how to use a virtual machine, but I do not require one except when using software designed for a different OS.
34. I haven't bought any virtual software and never thought of using it for this purpose, but it is a good idea.
35. I have tried virtual software for a project at school but don't understand how it works or how to operate it very well.
36. I generally only download software I trust and I do not know how to set up a virtual machine.
37. I don't use it when I trust the software.
38. I don't know how to use a virtual machine
39. I don't have time to do that.
40. I do I use VMware to test everything before I use it in my main OS
41. i can tell when a program is a virus or not.
42. I always use a virtual machine.
43. Don't think about it.
44. dont really worry about it
45. Don't always want to have to boot into the virtual machine to run things.
46. Did not select other.