Update? Install Now or Later!

A Synopsis of Update Behavior Research

Nazmun Nisat Ontika
University of Bonn
Bonn, Germany
Email: ontika@uni-bonn.de

***Abstract*—User behavior analysis is very important in every aspect and especially to implement security because a simple careless behavior of a user may cause a very harmful security anomaly to the user. There are many great articles in which researchers have analyzed the user behavior regarding the software update. However, there is no succinct work that covers all the research results altogether. In this paper, 25 well-known previous works which focused on update behavior of the end-users from 2012 to 2017 have been summarized and categorized to better understand the update behavior of the user. Moreover, based on the outcomes of those works, some directions to future researchers and to software developers and vendors are also mentioned in this paper.**

I. Introduction

The definition of software update can be stated as, "Software update is a manipulation involving adding, modifying, or deleting data to bring a file or database up-to-date. It can be a relatively minor release or version upgrade to an existing software product that adds minor features or corrects bugs"[1].

Software updates perform innumerable tasks which are available for both the system software and application software. According to Microsoft, all the software updates can fall into the following three basic categories [1].
The first one is 'Service Pack' which is a periodic update that corrects problems in one version of a product. In addition to correcting known problems, service packs provide tools, drivers, and updates that extend product functionality, including enhancements developed after the product was released. Service packs usually keep the product up-to-date, and they update and prolong computer's functionalities. Service packs also contain a number of design changes or features.
The second one is called 'Regular Update' which are done for a patch that is designed to fix a specific problem. Companies might release several patches throughout the month to take care of security flaws or bugs. At the end of the month, normally they release a service pack that includes all of those patches, along with any improvements to the software.
The Third one is known as 'Security Updates' that address security vulnerabilities which are known as security hole or weakness found in a software. An attacker can break into systems and can exploit such vulnerabilities by writing code to target a specific vulnerability, which is packaged into malware. Once this malware infects a computer, it can then steal data, allow the attacker to gain control over the computer. Hence, security updates are very important as well the others.

There are only three possible outcomes to a software update [2]; first, everything goes as planned, bugs are fixed or new functionality is added, and everything proceeds normally. Second, there's no noticeable difference in operation or administration aside from a version number ticking upward or third, the user has just turned a working system into an inactive one.

Users behave differently towards the software update which is very important for desktop, laptop, tablet, mobile and IoT. Researchers can possibly find out the problems of current software update system and even generate new solution to overcome the problems by studying user behavior. Hence, it is very important to study and understand the user behavior regarding the software update.

II. Motivation

Whereupon the update behavior of Android application users has been first studied by Moeller et al. [17] in 2012, this year is considered the starting period for this paper. There has been a lot of good works regarding identifying the update behavior of users since 2012. However, the works were diverse in many aspects and there is no summarized work to know all the major findings. In this paper, we want to summarize and categorize the previous works that focused on this area for better understanding.

III. Systematization of previous works

In this paper, 25 previous works have been clustered under the type of studies, devices and sample population that was picked by the researchers for their works on update behavior.

A. Type of studies

Several kinds of studies were used by researchers to know the behavior of users. However, researchers mainly focused on the online surveys [3] [4] [5] [6] [7] [8]. Excluding survey, some other commonly used studies were semi-structured interview [5] [9] [10], think aloud session [5], field study [3]

[1]www.yourdictionary.com; accessed on 10/04/18

[11]. Participants were mainly recruited from the following two sources for these studies mentioned above Amazons Mechanical Turk crowdsourcing platform and university students who were informed about the studies mainly by advertising on universities, post on social media (Facebook, Twitter) or email.

B. Sample population

In the sample of the population of the studies, three different criteria were noticeable. Firstly, gender, the participants were mostly male (62.3% [7], 62.5% [3], 53.3% [5]) in the studies. Secondly, age, most of the paper focused on young users. Finally, region, researchers mainly focused on the users of the United States [3] [5] and Europe [6].

C. Type of devices

Researchers focused on all the devices but IoT. However, the number of research on desktop or laptop [9] [5] [4] was less than the number of research on mobile or tablet [12] [13] [7] [6] [5] [14] [15] [16] [17] [18] [3].

IV. Findings problems on update scenario and user behavior

The research results on update scenario and the user behavior towards software update have been categorized into following nine categories.

1) Phases of update for user: According to Vaniea et al. [4] in computer environment, users go through six stages while updating. The first stage was awareness in where notifications and automatic updates would be important aspects of updates. Then there was deciding to update stage, once aware of the update, the user had to decide if they were going to install right away, delay, or avoid the update entirely. The third step was preparation which means the preparation of the software or device before they could be safely installed. Preparation activities ranged from making sure a device had power, to create a backup in case the update failed to meet expectations. Then the installation phase in where the downloaded update had to be installed. This process might involve some interaction from the user, computational resources, and reboot. The next one was troubleshooting, users needed to troubleshoot at nearly every stage of the update process, but it was mostly in reference to handling failures in the installer or resolving issues with the post-state. And the last stage was post state which could be either about no problems, more features, and better performance or more problems, worse performance depended on the user's experience.

2) View about update: The reported reasons for concerns about updating were very diverse. Although many users reported in a survey that they were concerned about privacy they may not be able to make informed choices. A few users even explicitly mentioned that they had to read reviews to help them understand the update [15]. Nearly half of the users among 307 who participated in a study said they had been frustrated updating software; only 21 percent users had a positive story to tell [4].

3) Delaying update: Authors found that almost half of all users would use a vulnerable app version even 7 days after the fix has been published. Moreover, up to four outdated versions were still circulating even after two weeks after the latest update has been published [17]. In another research it was found that for third-party apps such as Facebook or games, on average 40% of all users update to a new version on the release day. However, to update all devices, on average 200 days elapsed [16].

4) Reasons behind not updating: There were several reasons behind not updating the software on time or even not updating at all. The top reasons those were found by various researchers [3] [10] [5] [19] were- privacy invasiveness, permission-related concerns, unanticipated user interface changes, unused and unrecognized software, liking the current software, updates interrupt users, users lack sufficient information about updates, under-appreciation of the risks, lack awareness of vulnerabilities, fear of destabilizing their other software, being charged for Internet access and who run pirated software might hesitate to install patches for fear that the installation process would disable the illegal software or detect and report it.

5) View about automatic updates: Tian et al. [3] found that around half of the users use automatic update service in their devices. However, many users do not understand the auto-upadte concept, many users do not even know when their updates were being installed on their devices and the number of those kind of users were also almost 50% [20].

There were mainly three characteristics differentiated those users who avoid auto-updates from those who auto-update their mobile applications. These characteristics were past experiences with software updating, propensity to engage in risk-taking behavior, and displaying greater proactive awareness about their online security [7].

6) Mobile update vs computer update: Authors said that updating process tends to be more complex for mobile systems than desktop systems. When the new update released, thousands of files need to be replaced, added or modified. Each application installed before needs to be configured again according to its attribute and privilege in the former system [21]. People also has different preferences towards these devices. A majority users were equally or more diligent in updating mobile devices than computers [26].

7) The negative impact of updating: Android apps are not getting safer as they are updated. In many cases, app updates serve to increase the number of distinct vulnerabilities contained within apps, especially for popular apps. Some major vulnerabilities predominantly come from different types of code, i.e., developer code or library code. There are several severe threats which can inject during the update in mobile devices. One is an undetected installation of a malicious payload known as Update Attack. Another threat is caused by an uncontrolled updating, namely the Pileup. These threats exploit the flaws in the updating mechanism of the new OS, which the current system is upgraded to [18].

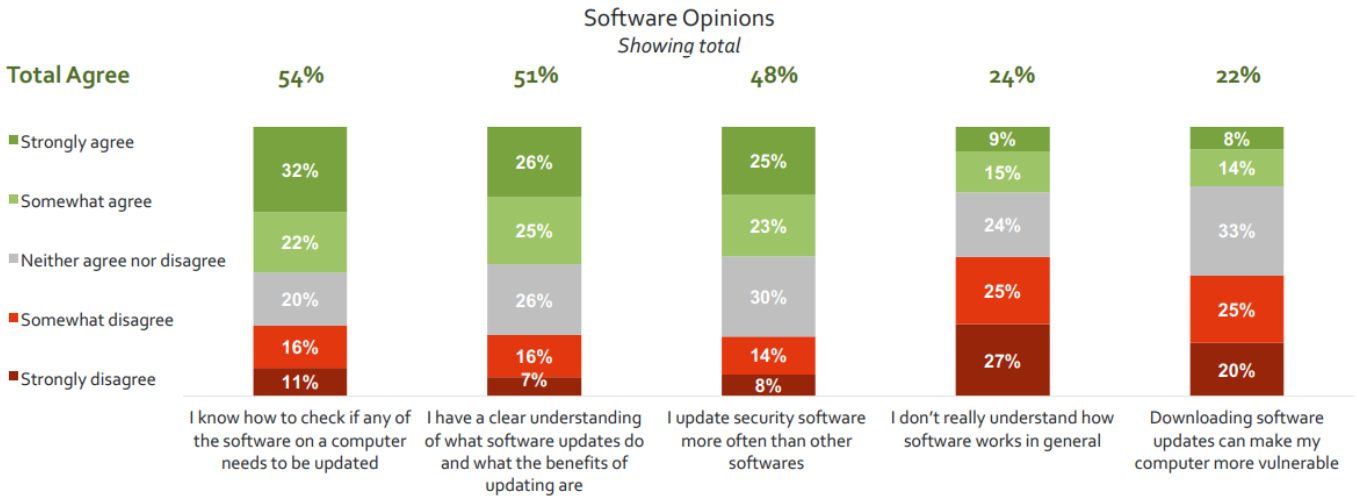

Fig. 1: Findings on general knowledge based on "To what extent would you agree or disagree with each of the following statements?" question[26]. The bar charts showing that the general knowledge of users about software is not satisfactory.

A group of researchers from Indiana University and Microsoft Research has unearthed six Android vulnerabilities that could be exploited to turn apparently harmless apps into malicious ones when a user upgrades the OS. These newly discovered vulnerabilities exist in almost all Android versions and allow unprivileged apps to automatically acquire potentially malicious capabilities including all new permissions added by the newer version of the OS without the users' consent [22]. On the other hand, package management systems designed to provide secure updates have been found to contain vulnerabilities. They also stated that manufacturers fail to provide updates to fix critical vulnerabilities, instead of the users. On average, 87.7% of Android devices are exposed to at least one of 11 known critical vulnerabilities [21].

Taylor et al. [13] analyzed 30,000 apps for two years and estimated that over 35,000 apps in the Google Play Store ask for additional dangerous permissions every three months. Authors observed that free apps and popular apps were more likely to ask for additional dangerous permissions when they were updated.

8) Difference between different kind of users: It can be said that experts understanding over user behavior does not follow a solidified user-model, especially in the general population [6]. And the reason behind this is, though the expert users give importance to software updates then general users to stay safe online [8] only 64 percent of security experts update their software automatically or immediately upon being notified a new version was available where just 38 percent of regular users do the same [8]. Another research project analyzed software update records from 8.4 million computers and found that people with some expertise in computer science tend to update more quickly than non-experts. But it's still slow: from the time an update was released, it takes an average of 24 days before half of the computers belonging to software engineers were updated. Regular users took nearly twice as long, with 45 days passing before half of them had completed the same update [23].

9) Knowledge of software: Nowadays many people (78%) recognize the importance of software updates [26]. However, the general knowledge of users about software is still not satisfactory [26] which can be viewed in figure 1.

V. Solving the Update Problem

Researchers mentioned many ideas to solve various problems regarding software behavior. They recommended some ideas to the developers, vendors, and users. Moreover, the researchers discovered some effective technical solutions that can be used by the developers and vendors to solve the update problems.

A. Recommendation

Several initial recommendations were given to vendors [19], developers [17] [4] [5] [7] and end users [19] [7].

To User: Users should switch on auto-updates via making application update rollbacks more accessible. Public education might dramatically increase patching rates. Users must be aware of their own safety.

To Developer: Developers must keep the application bug-free, provide timely updates in case of problems and provide a recovery path for users. All software should contain mechanisms whereby a patch that has been applied can easily be removed, and the system and data restored to the pre-patch state. Developers should not rely on users reading instructions and employing the built-in feedback functions but they should keep the track of ratings and comments in Google Play which is important. They can introduce support system for users in updating e.g. by built-in update checks within their application and/or forwarding users to the platform marketplace. Developers should Make it easy to find information about an update. Software developers have to ensure

personalized update interfaces, minimize update interruptions, and centralize update management across a device.
To Vendor: Software vendors should be more transparent about what specific configurations and applications they tested. Built-in software can be introduced to check whether all current patches have been applied or not and that might suffice for triggering consumers to be more attentive to downloading patches for their machines. Users get influenced by other users. Hence, the numbers or percentage of the users who have already updated their devices can be displayed to others which just might be enough to push the laggards into applying patches. Subsidize the bandwidth required for update downloads can be a focus area for vendors. Moreover, vendors must prohibit security-patch installation from implementing functionality in support of license-enforcement or any other form of intellectual property protection.

B. New invention

There were several inventions by authors that can solve many problems in software update aspect. Tian et al. [3] proposed a review-based update notification which can better alert users by catching their attention to avoid privacy invasive app updates, especially for apps with less trust from the users, comparing to notifications with permission descriptions only. In another research, authors discussed attempts to use a formal static method based on model checking for detecting update attacks in Android apps in which authors achieved an accuracy very close to 1 in recognizing update attack families i.e., Plakton, AnserverBot, DroidKungFuUpdate, and BaseBridge [18]. On the other hand, a novel android updating model was introduced where Google, manufacturers, vendors, application developers, and other interested parties all join together to improve the security of Android operating systems. In the model, end users can have access to security updates in time and some kernel updates will be installed automatically and silently, which can help to enhance security and prevent the zero-day attack and costs less for vendors and manufacturers to update the OSes [14].

VI. Discussion

In last five years, there have been so many developments in the cybersecurity area. Nowadays people have better knowledge about cybersecurity, companies are offering more easy update environments. Though hackers are finding secret ways to breakthrough, developers are fighting with innovation. In following sections, some important discussions are added including comparisons of different methods, changes over the years, reasons behind today's circumstances, suggestions to vendors and authors for future research.

A. Manual vs auto update

Many users get confused during the selection of the perfect method for a software update in their devices between automatic and update. Hence, it is very important to know the differences between these two methods and chose one of the methods wisely.
Automating updates similar to Windows Update or Firefox will lead to more uniform update installations, but will also result in many users not understanding what is happening on their computers and not being able to change things when they want to. On the other hand, manually installing updates may lead to better understanding of updates and a greater feeling of control, but will also likely result in lower levels of security and compliance.
Automatic software updates are a useful tool, but in some cases, manual updates are a safer solution. Hence, update strategy should be balanced between automatic and manual updates.

B. People's behavior

Over the years people's behavior towards software update has been changed positively. In 2012 video chatting service Skype partnered with Norton by Symantec and TomTom launched a survey in international technology upgrade week [25] and in 2016 Adobe with Edelman published a security survey [26] to learn more about the user behavior. Table I summarized the two surveys mentioned above and displays the behavioral changes of users. Though people's behavior is changing but the percentage of users who do not always update their software decreased just only by 4 percent in this four years which is not satisfactory.

C. Reasons behind the difficulties of software behavior

There could be many reasons why software updates are difficult, some important reasons were mentioned by Jake Soenneker et al. [24] like, users run a massive array of operating systems and environment combinations these days, the underlying frameworks may need to be updated from one version to the next, too. Users continue to tweak security and permissions and may neglect to install updates to their operating system or to the application. With deploys getting more automated, and with teams shipping code faster, bugs and security issues evolve faster as well. Moreover, the update system itself needs updating. Researchers should work on these difficulties to get over them and make software update process better.

D. Common limitation of previous work

From 2012 till now authors found some following common limitations in their studies regarding the software update.
Tech-Savvy Participants: Many researchers recruited participants on the Mechanical Turk platform [3] [8] [4] [7], which is known to provide a younger and more tech-savvy sample than the general population so that should not be considered as a standard for all.
Self Reported Data: All behavioral data that got collected was self-reported and, therefore, unconfirmed. Such data can suffer from several biases, including social desirability, inaccurate recall, lack of understanding, and observation effects.
Limited number of users: Some research had a small sample and their results might be changed in a large sample.

TABLE I: The behavioral change of users from 2012 to 2016

Survey	From Skype	From Adobe
Year	2012	2016
Focused region	America, Britain and Germany	United States
Users who do not always update the software	40%	36%
Top reason for updating	To keep computer safe from viruses and hackers (76%)	i. To keep computer safe and secure from hackers. (68%) ii. Ensures software is free of bugs and runs more smoothly/ crashes less often. (68%)
Top reason for not updating	Worrying about security of computer (45%)	Whether an update is legitimate vs a virus/malware/from a hacker (35%)
Number of notification needs to be prompted before updating	2 notifications (25%)	i. 1 notification (36%) ii. 2 notifications (39%)

VII. Suggestions and Directions

Based on all the prior works we mentioned and discussed here till now, we can say that users do not install updates in their devices. Reasons behind the problem and recommendation from the researchers are also given here. Nevertheless, the update behavior is not changing moderately. Hence, in next two subsections some directions for future research and some suggestions to vendors are included for better result.

A. Directions for future research

Researchers are continuously doing enormous works in cybersecurity field. However, they can change some methods as well as introduce some new methods in their research for a better result.

1) Diverse sample: To have more useful research the sample population should be more diverse with people from different regions, age, and gender.

- Region: There are many good works have been done so far in this area but most of the surveys were performed by the users of United States whereas, in top 50 countries in terms of smartphone users in 2017, 20 countries were from Asia and 16 were from Europe [27]. Hence, participants should recruit from different countries and different continents to get a global result.
- Gender: It was found that men (56%) upgrade their computer software more regularly than women (49%) when prompted to [25]. However, most of the participants were male in all the previous studies and there could be two reasons behind that; whether female users were not contacted to participate or they didn't find the importance of the surveys and didn't participate though they contacted. Therefore, we should encourage and engage the female users more towards cyber-security.
- Age: Most of the paper focused on young users. In each study, there were very few percentage of people who were less than 18 or more than 40. However, teenagers are using the smartphones daily and the rates are increasing rapidly. In 2015, 73% of teens had access to a smartphone [28] which became 87% in 2016 [29]. Moreover, four-in-ten seniors in 2017 own smartphones, more than double the share that did so in 2013 [30]. Hence, researchers should include the teenagers and the senior users in their surveys and count their experiences in.

2) Different devices and environments: Researchers should focus not only desktop and mobile devices but also Internet of Things(IoT) now. Moreover, most of the works were focused on windows and android users but it should focus on other OS too.

3) Different types of studies: There are some common methods of studies that are being used by the researchers as mentioned in subsection III-A. If the researchers use some other qualitative evaluation techniques such as silent observation, conceptual model extraction, constructive interaction, retrospective testing, structured interview etc. for their research it may lead to different and even more accurate findings.

4) Consider real experts: Previously, not many surveys focused on users with different expertise. Moreover, the criteria to be selected as expert was at least five years experience within information and cyber security field [6]. This criteria can be modified and be specific such as, studying advanced software developers and their update development practices to get in touch with more experienced experts for a more accurate result from the real world because even experts in previous works struggled with software update themselves as discussed in subsection IV-8. Thus, all experts behavior should not necessarily be taken as the right standard for non-tech-savvy users.

5) Elimination of the research limitation: As mentioned earlier in VI-D, there are some common limitations such as tech-savvy participants, self-reported data and the limited number of users. Researchers should acknowledge diverse sample and different study approaches as mentioned in VII-A1 and VII-A3 consecutively in their future work to avoid these common but not negligible limitations and provide more precise results.

B. Suggestions to vendors

Vendors should focus on their release schedule of software updates and provide an effective update notification system for users. They should consider the effective technical solutions given by researchers to change the current situation and move forward.

- Proper App update release schedule: Releasing updates in a haphazard manner can prove to be a disaster for the company. This irritates their Application users. Also releasing updates at irregular intervals display an unprofessional profile of the company. Hence, updating the application on a monthly basis can be a smart option for regular vendors and for large app development team, a weekly update can be more appropriate in order to handle the more complicated app development.
- App update notification system: Notification system is very important. However, vendors should focus on introducing such a method that will not disturb the users and can't be ignored completely as well. Push notification is a very good option for that situation.
- Acknowledge new inventions: Vendors should acknowledge researchers inventions. Many researchers developed new methods to avoid security problems, to enhance security, to detect vulnerabilities, to influence users toward safety as discussed in V-B. Companies should try out the new approaches that have been discovered and recommended by authors to check the effectiveness of those models in real software world war.

VIII. Limitation

A lot of major research projects which are available in online are being summarized here. Notwithstanding, there might be a few older or very recent works that have been missed out unintentionally because of lack of time. Although we compared the update behavior among different types of users, for the reason of having the focus area for this project on end-user, some few papers that focused mainly on developers or administrators did not get covered here.

IX. Conclusion

Software updates are very important regardless of the devices. Users should not ignore the prompt next time and be sure to keep their software updated by maintaining balance with manual and automatic updates. Researchers should work in future with more diverse population, different OS, and devices and consider real experts. The government, mobile vendors, security administrators should try some new approaches of teaching security behaviors to the general people such as advice article, edutainment video, security comics etc. to educate the general public more about security. End-users, developers, vendors, researchers should work together to make software updates more user-friendly, bug-free and effective.

X. Acknowledgment

I would like to thank my supervisor, Dr. Emanuel von Zezschwitz (University of Bonn) for his patient guidance, encouragement, valuable advice, and help.

References

[1] Microsoft, "Types of updates." https://technet.microsoft.com/en-us/library/cc526858.aspx. Accessed on 28-12-17.

[2] P. Venezia, "Software updates: The good, the bad, and the fatal." https://www.infoworld.com/article/2615258/data-center/software-updates–the-good–the-bad–and-the-fatal.html, Sep 10 2012. Accessed on 26-11-17.

[3] Y. Tian, B. Liu, W. Dai, L. Cranor, and B. Ur, "Study on users attitude and behavior towards android application update notification," in *Tenth Symposium on Usable Privacy and Security*, SOUPS 14, 2014.

[4] K. Vaniea and Y. Rashidi, "Tales of software updates: The process of updating software," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, (New York, NY, USA), pp. 3215–3226, ACM, 2016.

[5] A. Mathur, J. Engel, S. Sobti, V. Chang, and M. Chetty, ""they keep coming back like zombies": Improving software updating interfaces," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, (Denver, CO), pp. 43–58, USENIX Association, 2016.

[6] V. Gkioulos, G. Wangen, and S. K. Katsikas, "User modelling validation over the security awareness of digital natives," *Future Internet*, vol. 9, no. 3, 2017.

[7] A. Mathur and M. Chetty, "Impact of user characteristics on attitudes towards automatic mobile application updates," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, (Santa Clara, CA), pp. 175–193, USENIX Association, 2017.

[8] I. Ion, R. Reeder, and S. Consolvo, ""...no one can hack my mind": Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, (Ottawa), pp. 327–346, USENIX Association, 2015.

[9] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang, "Do or do not, there is no try: User engagement may not improve security outcomes," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, (Denver, CO), pp. 97–111, USENIX Association, 2016.

[10] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: How negative experiences affect future security," in *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, (New York, NY, USA), pp. 2671–2674, ACM, 2014.

[11] C. X. M. L. T. D. Armin Sarabi, Ziyun Zhu, "Patch me if you can: A study on the effects of individual user behavior on the end-host vulnerability state," in *Passive and Active Measurement - 18th International Conference, PAM 2017, Sydney, NSW, Australia, March 30-31, 2017, Proceedings*, pp. 113–125, 2017.

[12] Z. Yan, Y. Dong, V. Niemi, and G. Yu, *Exploring Trust of Mobile Applications Based on User Behaviors*, pp. 212–226. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[13] V. F. Taylor and I. Martinovic, "To update or not to update: Insights from a two-year study of android app evolution," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, (New York, NY, USA), pp. 45–57, ACM, 2017.

[14] Y. Yang, J. Zhang, and T. Wang, "How to make android updating securer?: A new android updating model," in *Proceedings of the 2016 International Conference on Communication and Information Systems*, ICCIS '16, (New York, NY, USA), pp. 69–72, ACM, 2016.

[15] Y. Tian, B. Liu, W. Dai, B. Ur, P. Tague, and L. F. Cranor, "Supporting privacy-conscious app update decisions with user reviews," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '15, (New York, NY, USA), pp. 51–61, ACM, 2015.

[16] M. Oltrogge, Y. Acar, S. Dechand, M. Smith, and S. Fahl, "To pin or not to pin helping app developers bullet proof their tls connections," in *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, (Berkeley, CA, USA), pp. 239–254, USENIX Association, 2015.

[17] A. Möller, F. Michahelles, S. Diewald, L. Roalter, and M. Kranz, "Update behavior in app markets and security implications : A case study in google play," in *Research in the LARGE : Proceedings of the 3rd International Workshop. Held in Conjunction with Mobile HCI*, pp. 3–6, 2012. Godkänd; 2012; 20121121 (andbra).

[18] F. Mercaldo, V. Nardone, A. Santone, and C. A. Visaggio, "Download malware? no, thanks: How formal methods can block update attacks," in *Proceedings of the 4th FME Workshop on Formal Methods in Software*

Engineering, FormaliSE '16, (New York, NY, USA), pp. 22–28, ACM, 2016.

[19] F. S. Deirdre Mulligan, "Doctrine for cybersecurity," *Ddalus, the Journal of the American Academy of Arts & Sciences*, vol. 140, no. 4, 2011.

[20] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, (Menlo Park, CA), pp. 89–104, USENIX Association, 2014.

[21] D. R. Thomas, A. R. Beresford, and A. Rice, "Security metrics for the android ecosystem," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '15, (New York, NY, USA), pp. 87–98, ACM, 2015.

[22] Z. Zorz, "Flaws in android update mechanism could turn apps into malware." https://www.helpnetsecurity.com/2014/03/24/flaws-in-android-update-mechanism-could-turn-apps-into-malware/, March 24 2014. Accessed on 28-11-17.

[23] A. Nappa, R. Johnson, L. Bilge, J. Caballero, and T. Dumitras, "The attack of the clones: A study of the impact of shared code on vulnerability patching," in *2015 IEEE Symposium on Security and Privacy*, pp. 692–708, May 2015.

[24] J. Soenneker, "How to get your users to actually update your app." https://medium.freecodecamp.org/the-architecture-of-an-intelligent-application-update-system-3fc2f27a4a2, January 29 2017. Accessed on 12-11-17.

[25] Mashable, "Nearly half of consumers don't upgrade software [infographic]." http://mashable.com/2012/07/26/software-study/\#XjSYCbq7SaqN, July 26 2012. Accessed on 02-12-17.

[26] Adobe, "Adobe security survey." http://blogs.adobe.com/security/files/2017/07/About-the-Survey_071817.pdf, October 2016. Accessed on 29-11-17.

[27] Newzoo, "Top 50 countries by smartphone users and penetration." https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/, 2017. Accessed on 28-12-17.

[28] P. R. Center, "Teens, social media and technology overview 2015." http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/pi_2015-04-09_teensandtech_06/, April 8 2015. Accessed on 28-12-17.

[29] eMarketer, "Teens' ownership of smartphones has surged." https://www.emarketer.com/Article/Teens-Ownership-of-Smartphones-Has-Surged/1014161, July 5 2016. Accessed on 28-12-17.

[30] P. R. Center, "Technology use among seniors." http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/, May 17 2017. Accessed on 28-12-17.