DRMACert: Certification for Disaster Response Mobile Applications

Youna Jung*
Computer and Information Sciences,
Virginia Military Institute
jungy@vmi.edu

Tanner P. Mallari
Computer and Information Sciences,
Virginia Military Institute
mallaritp22@mail.vmi.edu

Emily E. Hattman
Computer and Information Sciences,
Virginia Military Institute
hattmanee22@mail.vmi.edu

ABSTRACT

As the scale of damage of natural disasters is increasing, it is required to have effective and secure disaster response mobile applications that collect disaster-related data, disseminate vital information about shelters, emergency personnel, and surrounding area, and generate escape routes. As we have seen in the recent disaster situations, the existing mobile applications do not fully address the needs to secure people's lives and properties. In this paper, we identify the problems on the existing application and derive the requirements for disaster response applications. To satisfy the requirements, we propose the DRMACert, a standard certificate that proves the effectiveness, security, and compliance of a disaster response application. In addition, we present its certification process that employs both an expert-based evaluation and a system-based evaluation for rapid and unbiased examination.

CCS CONCEPTS

• **Social and Professional topics** → Management of computing and information systems; Software management; Computing profession; Testing, certification and licensing.

KEYWORDS

Regulations, Standards, Mobile Application, Disaster Response

ACM Reference Format:
Youna Jung, Tanner P. Mallari, and Emily E. Hattman. 2021. DRMACert: Certification for Disaster Response Mobile Applications. In *2021 4th International Conference on Computer Science and Software Engineering (CSSE 2021) (CSSE 2021), October 22–24, 2021, Singapore, Singapore.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3494885.3494921

1 INTRODUCTION

With the advent of wireless networking and mobile device technologies, many services including banking, shopping, entertainment, and social networking services have been shifted to more interactive and instantaneous services in these days. Unlike general-purposed mobile applications providing entertainment or social networking services, some mobile applications are offering security-critical services that may affect citizen's lives and properties. One of the well-known examples of critical applications is the disaster-responsive mobile applications (DRMAs). The Forbes article, titled "A Surprising solution to surviving natural disasters: Mobile apps", emphasizes the legitimate utility of DRMAs [1]. As stated in the article, the AtmaGo app had been used during flooding in Jakarta, 2015 to share safe evacuation routes, shelter locations, and give warnings of waterborne diseases, reaching and aiding 2.5 million Indonesians. Several social networking apps had also been used during the Tsunami in Japan, 2011. As we can see in these examples, several DRMAs provide essential information related to disasters or epidemic diseases and give us action guides to escape distressed areas or prevent getting infected. However, existing DRMAs often fail to deliver critical information and services or remain in their passive ways in a disaster situation [2, 3].

As many people may rely on the services provided by DRMAs in a disaster situation, it is important to ensure the performance and the security of DRMAs. Unfortunately, many DRMAs however are still in its infancy. One of the most critical issues is that there is no standardized certification related to the disaster-responsive applications. This problem might bring a serious problem because unqualified applications could lead people to undesirable situations. To address the issue, in this paper, we propose a certificate that ensures development of effective, trustworthy and ethical applications for disaster response. This certificate verifies the essential features of DRMAs by collaborating with professionals, and in turn, enables people to use better DRMAs that provide vital disaster information in a timely manner while maintaining security and ethical standards.

The rest of the paper is organized as follows. In Section 2, we identify the problems on existing DRMAs and list the requirements to address the problems. In Section 3, we propose our certificate for disaster response applications with four evaluation aspects and its hybrid certification process and explain how the proposed certificate addresses all the requirements. We then summarize our contributions in Section 4.

2 MOTIVATION AND REQUIREMENTS

2.1 Motivation

As global warming continues, we have recently experienced serious natural disasters such as bush fires in Australia, flash floods in Indonesia, and hurricane Laura in Haiti in 2020. To mitigate the damage, government agencies maintain their own disaster response systems but the systems are often faced with the lack of

*Corresponding Author: Youna Jung, Associate Professor in the Department of Computer and Information Sciences at Virginia Military Institute. Email: jungy@vmi.edu, Telephone: +1-540-464-7498

CSSE 2021, October 22–24, 2021, Singapore, Singapore

ACM ISBN 978-1-4503-9067-5/21/10…$15.00
https://doi.org/10.1145/3494885.3494921

resources and infrastructures. As a remedy, non-profit organizations and industrial companies have developed disaster-responsive mobile applications (DRMAs) that enable people in a disaster area to receive vital information related to disasters or epidemic diseases. Our research however shows us that several problems exist as follows.

1) **Lack of universal definition of mandatory services on disaster response applications** - Many DRMAs have been developed with different types and levels of services so it is not easy for users to select a right application providing necessary services in a disaster situation. Since we do not have rigorous standards for disaster response applications, people have to examine all the applications by themselves to find the best option for them. If a person tries to find an application after a disaster occurs, he or she may not be able to find a proper application. This failure may lead to loss of citizen's lives and properties. By the nature of disaster, the lack of standards could bring a critical issue.
2) **Misunderstanding of applications' capability and liability** - To cope with a disaster using DRMAs effectively, users must clearly know the capability and reliability of a DRMA that they are using. Misunderstanding of what an application can do and cannot do may cause critical situations. For example, let us assume that a user believes that his application can generate an emergency escape route in real time without a WiFi connection because the app has a menu for GPS-based route generation. However, the menu is indeed an ongoing work and not providing the service at that time. The menu button on the app and the lack of notification of the unimplemented service could cause users to overestimate the application's capability and in turn put people in danger.
3) **Privacy breach** - Information and services required by users in disaster areas often vary depending on their situation. It is the reason that many DRMAs collect and use personal data including age, gender, location, occupation, social relationships, and medical records to provide personalized services [2, 3]. In a disaster situation, people may be desperate and give consent to use their private data without a second thought. However, the private data consumed and stored in an application can cause a serious privacy issue if the data is shared with the third parties against a user's wish. A breach of privacy may bring serious issues after people recover from a disaster. Currently, we have the Health Insurance Portability and Accountability Act (HIPAA) to protect citizen's private data on healthcare and well-being applications and systems, but there is no obligation for developers to apply HIPAA to disaster-responsive applications.
4) **Ephemeral evaluation of DRMAs** - To provide effective and secure services, it is required for DRMAs to have a quality assurance system that continuously monitors compliance with regulations and standards after the applications are verified. If there is any violation, it is required to fix all the issues. To do so, we need a systematic approach to monitor and enforce standardized regulations for DRMAs.

2.2 Requirements

To secure citizen's lives and properties as much as we can, we need to address the problems listed above. To this end, DRMAs are required to satisfy the following requirements.

1) **Definition of DRMAs' services** – There is a need for a universal definition on mandatory services of DRMAs. A set of experts which includes emergency personnel such as firefighter, paramedics, and policemen, software engineers and mobile app developers can define functional and non-functional services of the DRMAs. The mandatory services may include notification of updates on disaster situations, establishment of ad-hoc network connection between nearby users, or emergency route generation. The definition must consider not only an application's performance and security but also maintenance service of applications. To be effective during disaster situations, an application needs to update geospatial data such as building locations, highways, and local streets and disaster relief information constantly [5].
2) **Mandatory user education about applications' capabilities** - To help users be aware of the applications' capability, the applications must correctly, and if necessary repeatedly, notify and educate users about applications' capability. To do so, the developers need to provide a clear definition of terminologies and conditions for services. For better understanding, we recommend to provide some example scenarios that show how users can use an application's services in a disaster situation with visual aids. In addition, an application needs to provide a disclosure statement to the users stating hardware and software requirements to run the application if there is any. To help users to deal with unexpected situations when an application is not able to provide an expected service, an application must have a reliable notification service. Note that it is users' responsibility to read and react to notifications.
3) **Ethical development of DRMAs** - To guarantee the privacy protection of DRMAs, we need an ethical development framework, similar to the ACM Code of Ethics [6], for DRMAs. Within the ethical development frame, we need to check whether: 1) an application will not deceive users of its capability, 2) an application will not invade users' privacy, and 3) an application will have the users' best interests at hand in the context of disaster response. The compliance of the ethical development framework must be verified.
4) **Quality assurance for DRMAs** - Towards rigorous quality assurance of DRMAs, the mobile application markets like Google Play and Apple App Store may require DRMAs to receive a certificate that prove the compliance with all the regulations and standards related to disaster response to be released for public use. All the aspects of the applications must be monitored by a trustworthy party and periodically re-evaluated to make sure applications' compliance.

3 DRMACERT: DISASTER RESPONSE APPLICATION CERTIFICATE

To fulfill the urgent need for effective and secure DRMAs, in this paper, we propose the Certificate for Disaster Response Mobile

Applications (DRMACert) that addresses the requirements listed above. The certificate will ensure a reasonable level of disaster-responsive services and enable the certified apps to receive the attention of users. To issue the certificate, we propose a hybrid procedure consisting of an expert-based evaluation and a system-based automatic evaluation. The proposed certificate and its issuance process help the developers adhere to effective and ethical development of disaster-responsive mobile applications.

3.1 Aspects of the DRMACert

1) **Unified definition of mandatory functionalities and service effectiveness** - Each DRMA has a different scope of functionalities and its own definition of effectiveness, but we found some common ground on their definitions and services such as pertinent messaging and computation, disaster data dissemination, Big Data analysis, and user-friendly interfaces [7]. In a disaster situation, immediate attention is required. The continuously changing status needs to be captured and distributed to emergency personnel and citizens to help civilians escape from distressed areas. To grasp a situation, the analysis of Big Data collected from satellites, environmental sensors, mobile devices, and social media is also critical. Indeed, Big Data and crowdsourcing technologies have actively been used by governments to collect and disseminate disaster-related data like locations of injured victims and up-to-date traffic information. In addition, DRMAs need to deal with a wide range of users and must not assume a certain level of IT knowledge and skills. To provide vital help during disaster situations, DRMAs must be easy to use for everyone including people who are not familiar with mobile devices and services. Towards this goal, the usability of DRMAs must be considered.
2) **User education and notification** - It is important that users correctly understand the purpose of the applications and its functionalities to utilize an application in a disaster situation properly. To this end, the DRMACert reviews the *terms and conditions* document and the notification system of an application. To determine the extent to which terms and conditions could genuinely be understood by average people, the DRMACert employs the *Simple Measure of Gobbledygook* (SMOG) formula [10]. The SMOG formula scores a *terms and condition* document high if it is readable and acceptable by the public. In addition, the information about an application's capability and limitations must be notified. To measure the level of a notification service, the DRMACert utilizes the measurement matrix that evaluates a notification's relevancy, expeditiousness, and context [9]. The notifications must be in line with a user's interest and sent at the right time.
3) **Privacy protection** - A DRMA must ensure the protection of private data all the time. The application developers need to implement security measures in their source code and an application must pass the penetration tests that exploit vulnerabilities of an application [10]. Towards this goal, the DRMACert evaluates the code security and the host security first. The code security requires the protection of the code from malicious hackers who try to alter the source code while the host security requires the protection of the host platform from malicious attackers attempting to gain access to unauthorized resources of the platform. As for the code security, the DRMACert checks if the application does not contain any potential risk on their code. According to the research in [10], utilizing a trustworthy third-party server protecting source code could be a good way to guarantee the code security in DRMAs. Along with the use of third-party verification servers, implementation of mobile agents has been proved an effective way to guarantee code security. In this case, a third-party server undertakes the verification of execution traces of a mobile agent on behalf of the platform agent to ensure the safe execution environments on heterogeneous host platforms. In addition, the DRMACert evaluates an application's privacy protection through penetration tests. The penetration tests have been useful measurement tools for discovering and addressing vulnerabilities.
4) **Continuous assurance and enforcement of compliance** - As DRMAs are critical to secure citizens' lives and properties, it is required for DRMAs to adhere to regulations and standards [19]. Any violations against regulations and/or standards can cause significant damage. The laws and regulations we need to consider are as follow: 1) *FTC Privacy Guidelines* [4] that prohibits unfair trade practices and privacy concerns on all types of applications, 2) *Electronic Communications Privacy Act* that prohibits interception, unauthorized access, knowingly disclosing communications, and disclosure of video records without consent, 3) *Computer Fraud and Abuse Act* that prohibits unauthorized access of devices to obtain prohibited information and knowingly trafficking device passwords and using extortion to damage a protected computer, 4) *Restore Online Shoppers' Confidence Act* that prohibits disclosing billing information to third-party sellers, 5) *HIPAA* and *HITECH* that are applicable to all applications that collect, create, use, store, or maintain protected health information, 6) *California Online Privacy and Protection Act* that is applicable to applications that collect California Residents' personal identifiable information.
In addition to the laws and regulations, DRMAs need to consider ethical standards as well. The *American Psychological Association* introduced three principles [12]: 1) An application must be in accordance with previously established principles and standards, 2) An application must inform users about the app's degree of empirical support, and 3) An application must have its developers be ensured of their own competence before implementing it into treatment or response. Unlike the general-purpose mobile applications, DRMAs need to follow more thorough guidelines, called *Crisis Standards for Care* [16]. According to the *American Public Health Association*, the *Crisis Standards for Care* must be at the highest standard of care within the developer's constraints, clarifying duty to care, caregiver responsibilities, obligations to caregivers, and ethical considerations for delegation of resources. We all are witnesses of the Coleman v. Garrison case in 1974 that shows us failure to ensure reliability of an application can result in a legal liability. In

Table 1: Checklists for each evaluation aspects of DRMACert

Aspects	Checklists
Effectiveness and Functionality	• Application fails to accept given data from a disaster response situation. • Application provides no assistance to a user in a disaster response situation. • Application analyzes disaster response data, but fails to formulate information for the user • Application provides average analysis of disaster response data and provides users with an abstract instruction plan. • Application provides excellent analysis of disaster response data and provides clear instruction for users.
User Education and Notification	• Application fails to provide terms and conditions statements and fails to provide users with notifications. • Application provides terms and conditions statement, but statement is not accurate in applications functionalities. • Application provides an ambiguous and lengthy terms and conditions statement. In addition, notifications are not useful to users. • Application provides clear and easily readable terms and conditions. However, notifications are overbearing and not useful to the user. • Application provides clear and easily readable terms and conditions. In addition, notifications are properly displayed and in a timely manner.
Privacy Protection	• Application contains malicious code that exploits the user's information. • Application does not contain malicious code or application does not pass the penetration test. • Application passes the penetration test, but developers are not completely confident in security measures. In addition, the application was not developed with ethical considerations. • Application provides proper security measures to protect user data. However, the development of the application did not abide by ethical considerations. • Application provides proper security measures to protect user data. In addition, application abides by ethical considerations.
Compliance	• Application complies with Laws, Regulations, and Ethical Standards shown in 3.1.4).

addition to the specific regulations and standards, it is the responsibility of the developer to adhere to application stores' guidelines to publish their applications. Note that a set of regulations/laws/standards that are applicable to an application will be determined by a group of experts on software engineering, mobile application development, and disaster response. Before an application is published on the Apple or Google App stores, it must pass the review process of those stores [17, 18]. If an application violates regulations and/or standards, mobile app stores could deny it.

3.2 DRMACert

The proposed certificate evaluates four aspects of the disaster response applications. Each aspect is graded on a scale from 1 to 5 based on the checklist shown in Table 1. To receive a DRMACert, an application must receive full credits for the *Compliance* aspect and a score set by an expert group created for an application for the rest of three aspects.

3.3 Certification Process

Several research have been conducted to verify the quality of software and applications. Jeffery Voas proposed some certification processes for the component-based software development that implements software by integrating existing software components [21]. He introduced a certification process maintained by an independent third-party agency, named Software Certification Laboratories (SCLs). This approach however may face a liability issue if evaluators in SCLs make a mistake on the certification process. As a remedy, an automatic certification process is proposed to eliminate human interference during the issuance procedure. The proposed process utilizes customer testing with software engineering professionals on real-life scenarios. To do so, SCLs create application usage scenarios based on the product and then conduct a series of tests with testers. Depending on the test results, SCLs determine if the product is eligible for a certification. However, the proposed certification process poses several issues when we consider DRMAs. An automated certification process could eliminate the possibility

of miscertifications by human mistakes but not able to evaluate the effectiveness of an application' services in an actual disaster situation. On the other hand, an expert-based process could evaluate the effectiveness of the application based on their experiences but be subject to human error.

To issue a DRMACert, we propose a hybrid certification process having both expert-based and system-based evaluations. First, the system-based evaluation process reviews and tests an application's source code to find any malicious behavior that could be a security threat. In the second round, disaster response professionals and software engineers evaluate mandatory services and compliance of an application based on diverse disaster scenarios. At last round, cybersecurity experts conduct penetration tests to exploit any vulnerabilities of an application. Note that the proposed process is managed by an independent and trustworthy third party to eliminate the potential for bias assessments. The proposed certification process is scalable, applicable, and reliable. The proposed process maintains its scalability by evaluating a least set of checkpoints essential for each evaluation aspect. As for its applicability, our process evaluates applications with real-world disaster situations containing actual geography data and anonymized citizens' data collected from previous disasters. The liability of the certification process is maintained with the separate rounds of process through not only automatic systems but also expert panels.

4 CONCLUSION

With the DRMACert, we can address the problems of existing DRMAs by evaluating four aspects: 1) Capability and effectiveness of disaster response services, 2) User education and notification, 3) Privacy protection, and 4) Continuous assurance and compliance. The proposed certificate and its certification process enable us to define the user and developer responsibilities separately and prove an application's capability and security during disaster situations. In addition, it helps to monitor and enforce an applications' compliance with standards for ethical development and regulations related to mobile applications and disaster response. To prove the performance and applicability of the proposed work, we plan to evaluate a wide range of DRMAs currently published in the market using the DRMACert in near future.

ACKNOWLEDGMENTS

This material is based upon work supported in part by the Jackson-Hope Fund of Virginia Military Institute and the Virginia Center for Undergraduate Research. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Virginia Military Institute.

REFERENCES

[1] Neil Yeoh. 2019. A Surprising Solution to Surviving Natural Disasters: Mobile Apps. Forbes. https://www.forbes.com/sites /neilyeoh/2019/05/23/a-surprising-solution-to-natural-disasters-mobile-apps/?sh=58bb0bf11158.

[2] Youna Jung. 2019. Community-Based Localized Disaster Response through Temporary Social Overlay Networks. Mobile Networks and Applications Journal. ACM/Springer 24 (5). 1641 -1653.

[3] Youna Jung, Renato Figueiredo, and Jose Fortes. 2015. Emergency Response using Ephemeral Social Communities across Online Social Networks. EAI Endorsed Transactions on Collaborative Computing. EAI, Vol. 1 No. 5 e(4), 1-15.

[4] Robert Hale. 2013. Recent Developments in Mobile Privacy Law and Regulation. The Business Lawyer, Vol. 69, No. 1, 2013, pp. 237–243. JSTOR, www.jstor.org/stable/43665657.

[5] Shashi Shekhar, Kwangsoo Yang, Venkata Gunturi, and Lydia Manikondal. 2012. Experiences with Evacuation Route Planning Algorithms. Science, Vol. 26, No. 12, pp. 2253–2265. EBSCOhost, doi:10.1080/13658816.2012.719624.

[6] Don Gotterbarn, Amy Bruckman, Catherine Flick, and Marty Wolf. 2018. ACM Code of Ethics: A Guide for Positive Action. Communications of the ACM, Vol. 61, No. 1, Jan. 2018, pp. 121–128. EBSCOhost, doi: 10.1145/3173016.

[7] Silvino Cumbane, Silvino Pedro, and Győző Gidófalvi. 2019. Review of Big Data and Processing Frameworks for Disaster Response Applications. ISPRS International Journal of Geo-Information, Vol. 8, No. 9, p. 387.

[8] Fuming Shih, Oshani Seneviratne, Ilaria Liccardi, and Evan Patton. 2013. Democratizing Mobile App Development for Disaster Management. In Proceedings of the Workshop on AI Problems and Approaches for Intelligent Environments and Workshop on Semantic Cities. ACM. 39-42.

[9] Lakhdar Meftah, Romain Rouboy, and Isabelle Chrisment. 2021. Empowering Mobile Crowdsourcing Apps with User Privacy Control. Journal of Parallel & Distributed Computing, Vol. 147, Jan. 2021, pp. 1–15. EBSCOhost, doi:10.1016/j.jpdc.2020.07.011.

[10] Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for all: revealing the hidden complexity of terms and conditions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13). Association for Computing Machinery, New York, NY, USA, 2687–2696. DOI:https://doi.org/10.1145/2470654.2481371.

[11] Nick Babich. 2016. Notifications for Mobile App. Medium, UX Planet, 2 June 2020, uxplanet.org/notifications-for-mobile-apps-bfba06f203f9.

[12] Deris Stiawan, Mohammad Idris, Abdul Abdullah, Fahad Aljaber, and Rahmat Budiarto. 2017. Cyber-Attack Penetration Test and Vulnerability Analysis. International Journal of Online Engineering (IJOE), Vol. 13, No. 01, p. 125, doi:10.3991/ijoe.v13i01.6407.

[13] Hock Tan and Luc Moreau. 2002. Certificates for Mobile Code Security. In Proceedings of the 2002 ACM Symposium on Applied Computing. ACM. 76–81. https://doi.org/10.1145/508791.508807

[14] Jamie Seligman, Stephanie Felder, Maryann Robinson. 2015. Substance Abuse and Mental Health Services Administration (SAMHSA) Behavioral Health Disaster Response App. Disaster Medicine and Public Health Preparedness, 9(5), pp.516-518.

[15] Committee on Guidance for Establishing Crisis Standards of Care for Use in Disaster Situations. 2012. Institute of Medicine. Crisis Standards of Care: A Systems Framework for Catastrophic Disaster Response. Washington (DC): National Academies Press (US), Introduction. Available from: https://www.ncbi.nlm.nih.gov/books/NBK201083/.

[16] Jonathan Leider, Debra DeBruin, Nicole Reynolds, Angelica Koch, and Judy Seaberg. 2017. Ethical Guidance for Disaster Response, Specifically Around Crisis Standards of Care: A Systematic Review. American Public Health Association. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5551597/.

[17] https://developer.apple.com/

[18] https://developer.android.com/

[19] Charles Macedo, Richard Zemsky, Amster, Rothstein, and Ebenstein LLP. 2015. Mobile Device and Applications Key Laws Chart. https://www.arelaw.com/downloads/ARElaw_MobileDeviceApplications_KeyLawsChart_rev061815.pdf

[20] IAEM. 2021. IAEM Code of Ethics and Professional Conduct. https://www.iaem.org/About/Code-of-Ethics.

[21] Jeffrey Voas. 2000. Developing a usage-based software certification process in Computer, Vol. 33, No. 8, pp. 32-37, doi: 10.1109/2.863965.