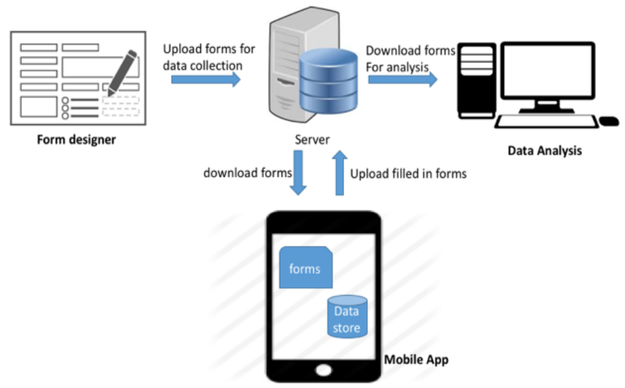
Authentication in Selected Mobile Data Collection Systems

Marriette Katarahweire, Engineer Bainomugisha, Khalid A. Mughal
Department of Computer Science, Makerere University

Introduction

Mobile Data Collection Systems (MDCS) are used in low-resource settings especially in the health sector to collect patient data.

Several security challenges are faced including secure authentication and authorization of users.



Authentication in MDCS

- Authentication ensures that the user registered in the system is the actual one trying to access the system.
- It is essential to have proper authentication and authorization to ensure confidentiality and integrity of the data involved the systems.
- In MDCS, two kinds of authentication can occur that is online authentication and local authentication.
- Local authentication requires the user credentials to be securely stored on the mobile device to avoid being tampered with or even access by unauthorized persons.
- Online authentication requires an active Internet connection which is not possible in low-resource settings.

Methods

- We undertook a systematic study and comparative analysis of the authentication model selected MDCS namely mUzima and DHIS 2, which are systems widely used in East Africa.
- The two reference systems were setup and run to observe their behavior and test authentication w.r.t the different dimensions of the evaluation criteria.
- The evaluation criteria derived from the authentication requirements for MDCS as defined in the SecureMDC framework, a modular framework that was developed to tackle security challenges in mobile data collection systems

Evaluation Results

Evaluation Criteria	DHIS 2 Tracker Capture App	mUzima
Authentication model	Online authentication	Online and offline authentication
Automatic logout	not possible	is available but the user can reset time
Support for multiple users per device	possible since no credentials are stored on the mobile device	yes but local repository is shared among all users
Account recovery	not available on the mobile device	yes
Authentication protocol	Basic Access Authentication	Basic Access Authentication
Data Encryption	available during transfer	yes (only on local storage) not during data transmission
Secure storage of user credentials	not available	user credentials are encrypted

Conclusions

- We present the criteria for evaluating authentication in MDCS and findings for evaluating representative MDCS that is mUzima and DHIS 2.
- Both systems implement some form of authentication, albeit not fully.
- There is need to ensure that the data transferred and user credentials exchanged between the mobile device and the server are secured by encrypting it and passing it over a secure channel.
- The implementation of automatic logout needs further refine to include other conditions for logout beyond timeout e.g., the window for timeout could be adjusted depending on contextual conditions or sensitivity of the data rather than giving users the leeway to misuse the opportunity of resetting this time to say no time outs altogether.
- We plan to implement the authenticator module of SecureMDC framework in mUzima and the DHIS 2 Tracker Capture app.

References

1. "DHIS 2," accessed: 2015-12-01. [Online]. Available: https://www.dhis2.org/
2. "mUzima," accessed: 2016-08-30. [Online]. Available: http://www.muzima.org
3. F. Mancini, S. Gejibo, K. A. Mughal, R. Valvik, and J. Klungsyr, "Secure Mobile Data Collection Systems for Low-Budget Settings." in ARES. IEEE Computer Society, 2012, pp. 196–205.
4. S. Gejibo, "Towards a secure framework for mhealth," Ph.D. dissertation, University of Bergen, 2015.

Acknowldgement

This research was funded by HI-TRAIN project under the NORHED programme and the BRIGHT project 317 under the Makerere-SIDA programme.