Cybersecurity for the Unbanked

Stephen Ambore,Dr. Christopher Richardson, Dr. Huseyin Dogan, Dr. Edward Apeh, Prof. David Osselton
Cybersecurity Unit, Bournemouth University,
Dorset, UK
{S. Ambore, C.J. Richardson, H. Dogan, E. Apeh, D. Osselton}@bournemouth.ac.uk

Abstract—Governments and institutions now use mobile platforms as a channel to provide financial services to over half of the world's population that hitherto had no access to formal banking services: the unbanked. Banks in particular have recently strategically increased their drive to move their core operations to mobile platforms in other to drive down their operational costs and increase profitability. However, cybercrime has also increased with the advent of mobile connectivity. In order to facilitate the adoption of Mobile Financial Services, the threat of cyber-crime to the uptake of mobile connectivity must be mitigated. This research work will be undertaken within the context of a PhD. It will analyse and provide an understanding of the key elements of cybersecurity in the provisioning of Mobile Financial Services. It aims to develop, implement and evaluate a Cybersecurity Framework for the Mobile Financial Services Socio-technical System (STS).

Keywords—Mobile Financial Services; Cybersecurity; Sociotechnical Systems; Mobile Banking; Financial Inclusion;Unbanked;Cyber-crime

I. BACKGROUND

Over half of the world population does not have access to formal banking services but have access to mobile platforms [1]. Governments and institutions now use mobile platforms as a channel to provide services to this segment of the world's population. Banks and other financial services providers are now increasingly using mobile platforms to drive down costs and increase the uptake of banking products [4]. This development along with new trends in mobile connectivity has introduced new challenges, in particular the continuous emergence of new cyber threats and attacks [2]. These cyber-attacks have continued to result in profound financial and economic impact on countries, organizations and individuals. Such financial and economic impact include financial losses, loss of confidential information or intellectual property, unauthorized alteration/modification of sensitive data, damage to critical information systems of an organization, system disruption to organization's services, unquantifiable reputational damage, and loss of customer confidence [3].

The development of procedures, policies and frameworks for tackling cyber-crime has however not kept pace with its proliferation. So much so that cost effective and convenient mobile platform services such as Mobile Banking and Payment services are at threat of reduced uptake.

There is therefore a need for a robust framework for tackling cyber-crime; one which will be holistic yet easy to use specifically to address cybercrime threats on mobile platforms for banking and payment transactions [5, 6, and 7].

II. AIM

The aim of this PhD. research is to develop a novel framework for Information Assurance for Mobile Financial Services STS. This framework is aimed at providing a methodology for mitigating the risks posed by cyber-crime on the uptake of Mobile Financial Services and will serve in boosting the capability of technology to facilitate financial inclusion.

The developed novel framework for Information Assurance for Mobile Financial Services will be demonstrated through the development of novel cyber-security procedures and policies for the unbanked

III. OBJECTIVES

The objectives of this research are:

- To investigate the state of art in Information Assurance, Mobile Banking, Human Factor and Capability Maturity as it affects Mobile Financial Services STS;
- To analyse requirement for Information Assurance framework for Mobile Financial Services STS;
- To develop Information Assurance framework for Mobile Financial Services, comprising a Capability Maturity framework;
- To validate the developed framework; and
- To exploit and disseminate the framework by applying it to Mobile Financial Services, specifically Mobile Banking and Payment services.

Copyright (c) PGCS, 2016.

IV. SIGNIFICANCE OF STUDY

The use of mobile platforms for banking and payment operations; Mobile Financial Services is a Sociotechnical problem [8,9]. It involves complex interaction within processes, people and technology across physical and logical boundaries of organizations and geographies. A Cybersecurity framework for Mobile Financial Services will help:

- Provide understanding of the Mobile Financial Services STS;
- Provide understanding of information flow within the system;
- Identify key stakeholders in the ecosystem and facilitate common understanding of challenges in the ecosystem; and
- Developed a cross-functional approach that will help mitigate the risk of cybercrime in the ecosystem.

V. CONTRIBUTION TO KNOWLEDGE

This research will contribute the following to the existing body of knowledge:

- An Information Assurance framework for Mobile Financial Services STS
- A Capability Maturity framework for Information Assurance for Mobile Financial Services STS
- Best practice case studies for adopting of the Information Assurance framework

VI. METHODOLOGY

In order to achieve the objectives of this research, a 6 stage approach, depicted in the activity flow in Fig. 1, will be used. This will ensure the gradual movement from the current state of affair "As-Is" situation to the desired target state "To-be" state. Soft Systems methodology and Integration Management techniques will be used in stages "1" to "3" to ensure the stepwise resolution of this real world problem from a larger problem space to a more specific space.

The 1st stage – State of the Art will involve understanding of the current state of play in the environment. Requirements for a Cybersecurity framework will be developed in the 2nd stage. The framework will then be built, validated and implemented in subsequent phases.

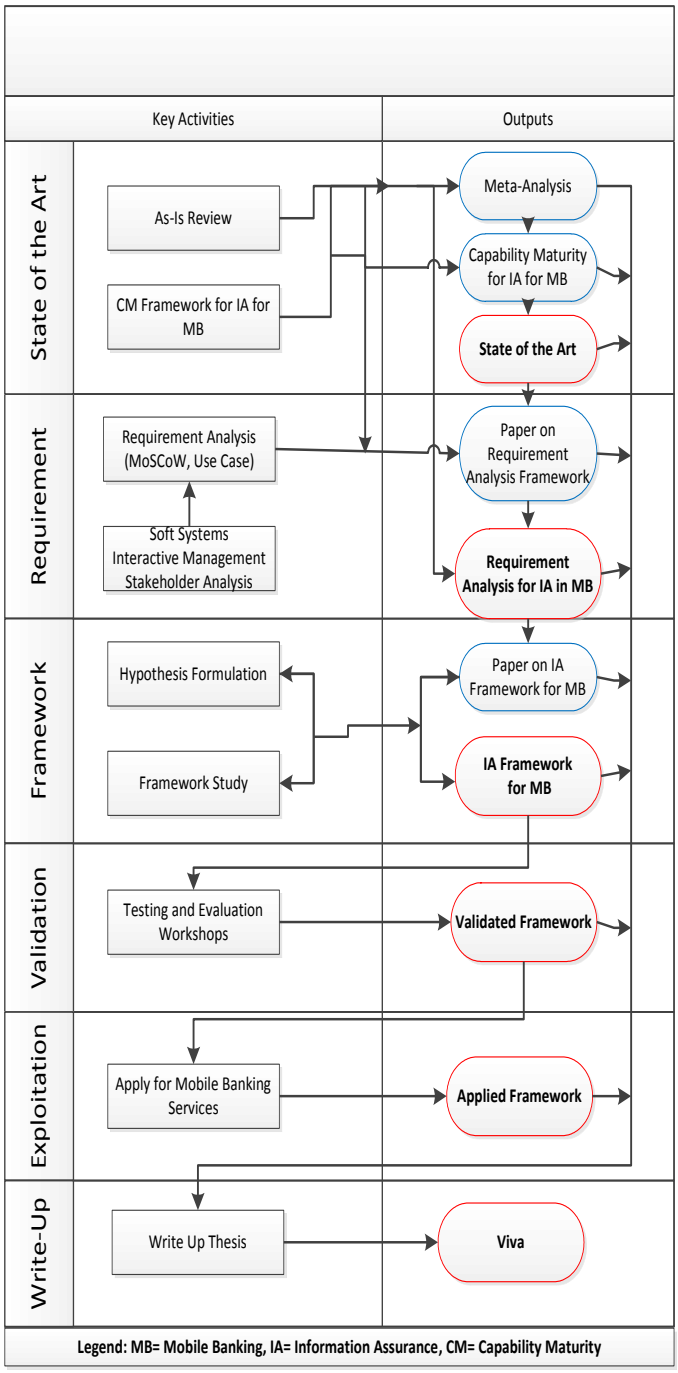
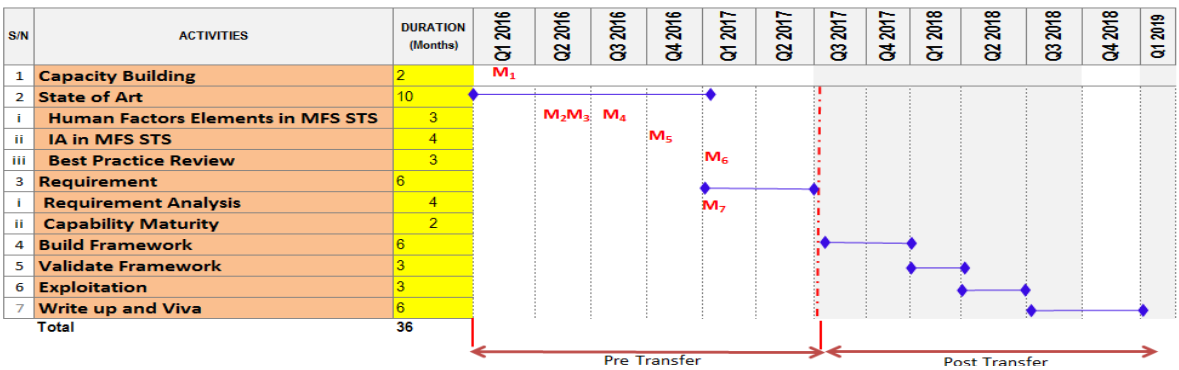


Fig. 1. *Activity Flow*

VII. TIMELINE

This research will be undertaken as part of a PhD. which commenced in January 2016 and will be completed within 36 months. Figure 2.0 below shows the research time line.

Fig. 2. *High Level Schedule*



Copyright (c) PGCS, 2016.

REFERENCES

[1] Chatain,P., Hernández-Coss, R., Borowik, K., Zerzan,A, 2008, Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing, World Bank working paper no. 146

[2] Nathan E., 2014, Online Retail Security Breaches, Mobile Malware Threats Grow, eWeek, 15306283

[3] Tech and Gadgets, 2014 Cyber Crime Causes $445 Billion Loss Annually in Global Economy, B2C, 2014.

[4] Valcke, J, 2016, Best practices in mobile security, Biometric Technology Today, Volume 2016, Issue 3, March 2016, Pages 9–11

[5] Malaquias,R.F, Hwang, Y, 2016, An empirical study on trust in mobile banking: A developing country perspective

[6] Vaithilingam, S, Nair, M , Guru, B.K 2013, Do Trust and Security Matter for the Development of M-banking? Evidence from a Developing Country, Journal of Asia-Pacific Business , Volume 14, Issue 1

[7] Gao, L. Waechter, K. A., 2015, Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation, Information Systems Frontiers, pg 1-24

[8] Carayon P, 2006, Human factors of complex sociotechnical systems, Applied Ergonomics 37 (2006) 525–535

[9] De Bruijn, H., Herder, P.M, 2009, System and Actor Perspectives on Sociotechnical Systems, IEEE transactions on systems, man, and cybernetics—part a: systems and humans, vol. 39, no.5

Copyright (c) PGCS, 2016.