Best Practice Process to Assure Confidence in the Transmission of Data for Mobile Medical Apps

Ceara Treacy, Supervised by: Dr. Fergal McCaffery

1 Research Challenge

» Mobile Medical Apps (MMAs) are becoming an established mechanism for health delivery. A MMA is a mobile app that qualifies as a medical device (MD) and therefore is required to follow the applicable MD regulatory requirements.

» MMAs are routinely designed to store and measure health data that is required to be kept secure and private through regulations and legislation.

» Detections of increased app hacking by security companies and researchers present a significant issue. Breaches of health information can have serious consequences for an organisation, including reputational and financial harm or harm to patients.

» Security of data for MMAs is now attaining serious consideration due to regulatory requirements and potential harm. Health data is now more valuable than credit card data in the U.S.

» Currently, there is no process model or best practice model standardized for developers of MMAs, to assure data security in transmission.

2 Background

» The only MD security standard, IEC/TR 80001-2-2:2012 presents an informative set of 19 high-level security-related capabilities.

» Two of these capabilities are concerned with data transmission:

1. TXCF - transmission confidentiality; and
2. TXIG - transmission integrity.

» IEC/DTR 80001-2-8 (currently at committee draft stage) presents a catalogue of security controls from a number of security standards which assist in the implementation of the 19 security capabilities.

Approach

» The research leverages on the established security controls in IEC/DTR 80001-2-8 relating to the two identified security capabilities from IEC/TR 80001-2-2:2012.

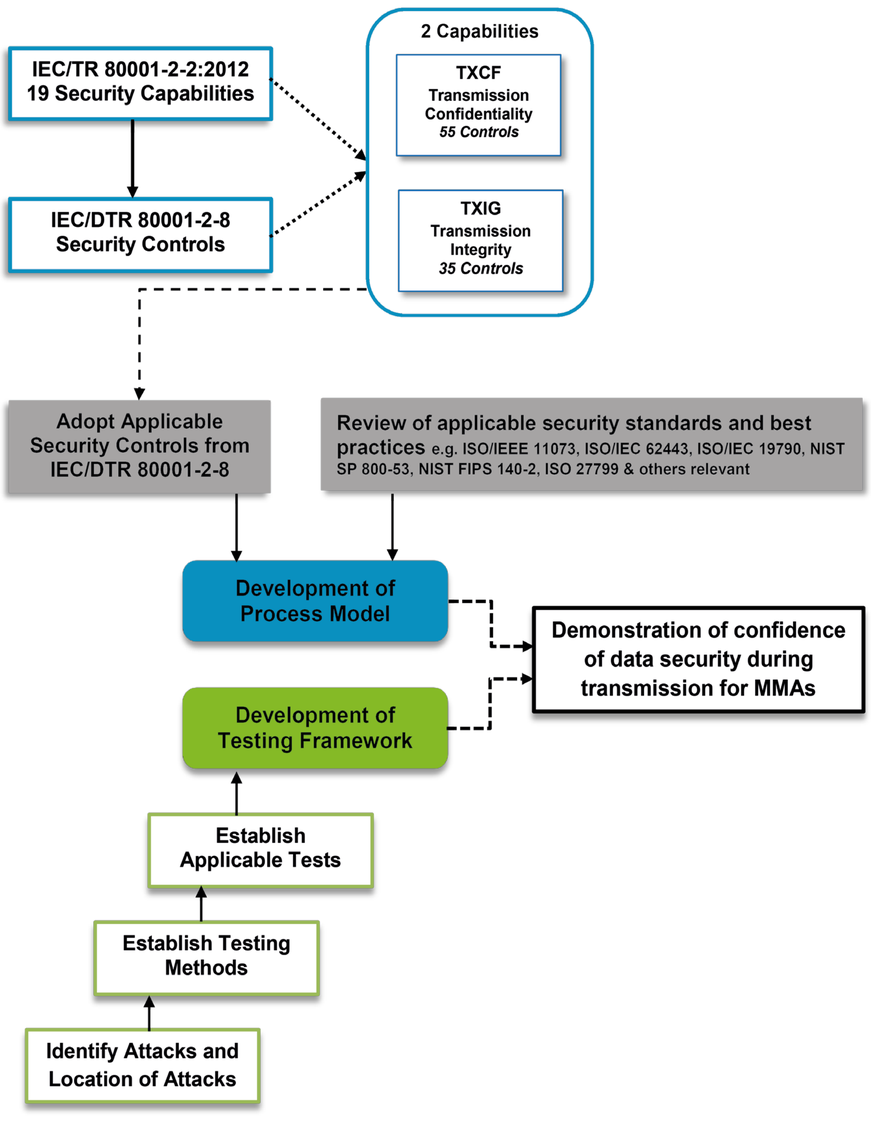
» To establish the Additional Security Controls Pertinent to Mobile Medical Apps, accomplished with comparative expert validation, by means of analysis of applicable standards and best practices.

» To develop process model as an exemplar, for identifying the most applicable objective evidence for implementation of two of the security capabilities, therefore demonstrating confidence of data transmission in MMAs, through:

› Collaboration with an identified data security expert to establish testing methods, applicable tests and a testing framework.

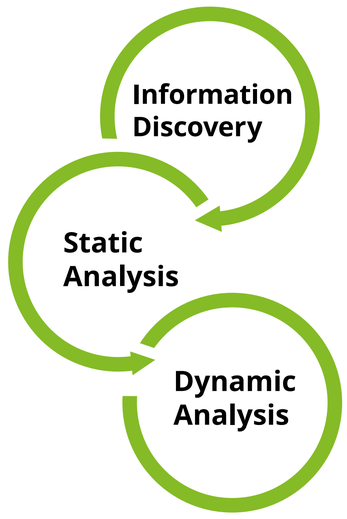
› Collaboration with Irish MMA companies.

3 Approach Overview



4 Testing Approach

» Authentication
» Authorisation
» Session management
» Data storage
» Information disclosure
» Networking



» Analyse functionality
» Analyse attacks
» Determine attack locations

» Dynamic fuzzing, tampering and injection tests of interfaces used
» User authentication, authorisation and business logic by-pass and elevation
» Analysis of cryptography used
» System level authentication and authorisation
» Session management assessment

Research Outputs

The proposed research leverages on the security controls in IEC/DTR 80001-2-8 for networked MDs and consolidates these with further research in mobile security controls, to develop a process model for identifying the most applicable objective evidence for implementation of the two security capabilities, therefore demonstrating confidence of data transmission in MMAs.

Future Directions and Translation

The process model will be established through research to develop a testing base either with the use of current testing methods or developing a suite of new testing processes to demonstrate confidence in data transmission for MMAs. This research will be applicable to MMAs in both the MD and general software development domains.

Acknowledgments

This research is supported by the Science Foundation Ireland Principal Investigator Programme grant number 08/IN.1/I2030 & by Science Foundation Ireland grant 10/CE/I1855 & grant 13/RC/20194 to Lero.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund

SOUTHERN Regional Assembly
Promoting our Region