Summary Report

Project summary

The project “Active Behaviour Demands Active Security: New Approaches to Mobile Device Security (ACTIVMOBSEC)” (PIIF-GA-2011-301536) ran from 28/09/2012 to 27/09/2014. This project investigated efficient modelling techniques to establish behaviour profiles on smart phone mobile devices. We hypothesized that behaviour remains stable under day-to-day use while anomalies will be observed under attack. Our results confirmed this hypothesis.

Project objectives

The project had four objectives.

- O1. Determine the most suitable sources for data modelling.
- O2. Develop scalable algorithms for behaviour modelling.
- O3. Determine suitable system status views for the user to make better-informed decisions.
- O4. To provide means for analyzing unknown behaviour. through the use of clustering of collected legitimate and malicious behaviour.

For O1 we developed a sensor collection application, and ran several small data collection studies to find viable sensor outputs from mobile devices. From this work, we collected data from sensors that record activities *on* the phone (application, phone, CPU, and battery use) as well as activities *around* the phone (light, noise, rotation, magnetic field, cell towers, and WiFi access points).

For O2 we investigated the use of existing modelling techniques, e.g., based on decision trees, and defined our own spatial and temporal models. We adapted them to measure both discrete and continuous data from sensors from which we (i) built dictionaries of frequent sensor events (e.g., frequent app use at particular locations), and (ii) measured “comfort” for each individual sensor.

For O3 we created some innovative ways of not overburdening participants when determining the “ground truth” of the data. We also built a data collection app with a user-friendly interface for collecting sensor data, and used this with our data collection and analysis.

Objective O4 was carried out during months 16 to 24. For this objective we defined threat models in order to measure the security of implicit authentication, and simultaneously evaluated trade-offs for battery consumption with different techniques for optimizing sensor use.

Project results and impacts

Our research resulted in several publications, some published after project completion:

- Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, Gunes Kayacik, “Why aren’t users using protection? Investigating the usability of smartphone locking”, to appear at MobileHCI 2015. (**Awarded Honorable Mention** – top 5% of submissions.)
- Nicholas Micallef, Gunes Kayacik, Mike Just, Lynne Baillie, David Aspinall, “Sensor use and usefulness: Trade-offs for data-driven authentication on mobile devices”, in

Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, 2015. **14.8% acceptance rate (29 of 196 submissions)**

- Adnan Muhammad, Mike Just, Lynne Baillie, Gunes Kayacik, "Investigating the work practices of network security professionals", in *Information and Computer Security (ICS) Journal*, vol. 23, iss. 3, Emerald, 2015.
- Gunes Kayacik, Mike Just, Lynne Baillie, David Aspinall, Nicholas Micallef, "Data Driven Authentication: On the Effectiveness of User Behaviour Modelling with Mobile Device Sensors", in *Proceedings of IEEE Security & Privacy Workshop on Mobile Security Technologies (MoST)*, 2014. (**Press coverage: BBC News, New Scientist, Daily Mail**)
- Nicholas Micallef, Mike Just, Lynne Baillie, Gunes Kayacik, "'Stop Questioning Me!': Towards Optimizing User Involvement during Data Collection on Mobile Devices", in *Proceedings of Mobile HCI 2013*, ACM, 2013.
- Nicholas Micallef, Mike Just, Lynne Baillie, Gunes Kayacik, "Non-intrusive and transparent authentication on smart phones", *Trust 2013*, Springer, 2013. **(Awarded best poster prize.)**

At the same time, we led a number of knowledge exchange activities related to our project:

- February 2013. Poster presentation at Glasgow Caledonian University event.
- March 2013. Presentation at Glasgow Caledonian University seminar.
- May 2013. Poster at Scottish Informatics and Computer Science Alliance (SICSA) event. (received award for best poster).
- November 2013. Presentation at Glasgow Caledonian University seminar.
- February 2014. Poster presentation at Glasgow Caledonian University event.
- February 2014. Poster presentation at Networks and Distributed Systems Security (NDSS) 2014 conference in San Diego, California.
- February 2014. Presentation at University of Edinburgh seminar.
- July 2014. Extended abstract presentation at SOUPS 2014 in Mountain View, California.
- July 2014. Poster presentation at ACM Wireless Security (WiSec) 2014 conference.
- October 2014. Poster at Scottish Informatics and Computer Science Alliance (SICSA) "DemoFest" event.

Dr. Kayacik (Marie Curie Fellow) was an active member of Glasgow Caledonian University, our School of Engineering and Built Environment and our Department of Computer, Communications and Interactive Systems. He was also a member of our Interactive and Trustworthy Technologies (ITT) research group (http://www.ittgroup.org). In additional to the above publications and knowledge exchange activities, Dr.. Kayacik was a co-supervisor of one PhD student (Nicholas Micallef) and an advisor for another (Adnan Muhammad).

Conclusions and future work

Our results demonstrate the viability of an implicit authentication solution for mobile devices, and we made key contributions in terms of sensor behaviour models and efficient sensor data collection, and were able to scientifically demonstrate the security and usability of our solutions. As noted above the work resulted in several high-quality publications and received recognition in several press articles (Evening Times and Metro in Feb 2012 at the start of our project, and later with some initial results in BBC News in Feb 2014, and New Scientist and Daily Mail in November 2014).