Multi-factor Authentication using Accelerometers for the Internet-of-Things

Julian Murphy and Gareth Howells
School of Engineering and Digital Arts
University of Kent,
Canterbury, United Kingdom (UK)
{ j.murphy-2060@kent.ac.uk, w.g.j.howells@kent.ac.uk }

Klaus D McDonald-Maier
School of Computer Science and Electronic Engineering
University of Essex,
Colchester, United Kingdom (UK)
{ kdm@essex.ac.uk }

***Abstract*—Embedded and mobile devices forming part of the Internet-of-Things (IoT) need new authentication technologies and techniques. This requirement is due to the increase in effort and time attackers will use to compromise a device, often remote, based on the possibility of a significant monetary return. This paper proposes exploiting a device's accelerometers in-built functionality to implement multi-factor authentication. An experimental embedded system designed to emulate a typical mobile device is used to implement the ideas and investigated as proof-of-concept.**

Keywords—Internet-of-Things; IoT; authentication; sensor security; security harvesting

I. INTRODUCTION

The advent of the IoT has given rise to a new wave of end-user focused embedded and mobile devices, which now form an increasingly important part of our everyday lives. A mobile software "app" is available for virtually any conceivable usage senario, and often used to interact wirelessly with embedded devices e.g., environment control, health or life-style monitoring devices. This wireless capability, in both embedded and mobile devices, is largely what is driving the growth of the IoT and creating a plethora of new uses.

At the same time, the underlying hardware technologies have also developed at a rapid pace e.g., sensor, power management, screen and processor technology. Indeed, the devices themselves and the IoT could not make such quantum advances if the hardware underneath did not evolve too. It can be noted a lot of this effect is due to a high-level of system integration. Whereby more and more technology is crammed onto a silicon die (System-on-Chip) or PCB.

Nevertheless, such tiered technology development creates new ways and opportunities for a determined attacker to compromise a device's security. This is notoriously, and has been historically speaking, the case with all rapid technology progression. Indeed, the sheer significance of the problem has justified its own label, "cyber-security"; and a variety of sub-taxonomies. While attackers (and defenders) typically require a deep understanding and knowledge of: hardware design, software development, operating systems and networking technologies to effectively compromise a device or system.

Therefore, and with all of the above in mind, it is important that security technologies chart a similar course; from low-level hardware all the way to high-level software. It has been shown that both multi-factor authentication and accelerometer sensors can be used to enhance authentication in the IoT [5]. Accordingly, in this work we:

- combine these two technologies to implement a proof-of-concept and multi-factor authentication scheme (protocol) using both accelerometer offset values and tap detection technology; and,
- use a field programmable gate array (FPGA) based emulation system equipped with a ADXL345 accelerometer and Bluetooth capability to evaluate the ideas.

The logic and reasoning behind the work is as follows.

First, accelerometers are mechanical MEMs [7] structures containing elements that are free to move, which makes them very sensitive to mechanical stresses and manufacturing lot-to-lot variability. They are also impacted by additional stresses applied during PCB system assembly arising from component soldering, board mounting and application of any compounds on or over the accelerometer. These points introduce unique and "device specific" offsets in axis readings, which is important because they, the offsets, define the baseline for measuring acceleration. Accordingly, accelerometers often incorporate calibration functionality to compensate for these effects (typically mid-range accelerometers), which is implemented either directly in hardware or programmatically in software. Here, offset values are established by taking many axis samples to form an average for each axis while the accelerometer is in one plane, termed one axis calibration. The calculated offsets are then stored in memory-mapped registers and subtracted from subsequent axis readings automatically by the accelerometer's hardware circuitry.

Secondly, tap detection technology [13], which is also prevalent in mid-range accelerometers, has proved profoundly useful for interaction in mobile applications and operating systems e.g., gesturing. Based on this, we observe tap detection technology provides an opportunity for the purpose of multi-factor authentication by acting as an input data source. Even more interesting is the possibility of harnessing the signature,

the fingerprint, of how the user interacts via tap detection. The latter is subject of future work, however.

A. B. Paper Organization

The remainder of the paper is structured as follows: Section II gives a discussion of related work; Section III presents the methodology and Section IV an evaluation; and, lastly Sections V and VI draw conclusions and discuss future work.

II. RELATED WORK

The following sub-sections give an overview of the relevant and related work in this area; the referencing targets the main citations fitting within the constraints and length of this paper.

A. ICMetrics

In [1] and [2] ICMetrics technology was presented and proposed. The scientific principle behind ICMetrics is to derive solely in software secret encryption keys and hardware identifiers, by statistically analyzing Gaussian distributions of the manufacturing differences or system characteristics present in one device compared to another. Possible variations, for example, are: PCB construction anomalies; integrated circuit (IC) lot-to-lot lithography variations; or, processor level-1/2 cache access signatures.

Papoutsis [3] completed the most complete work on ICMetrics, where he analyzed and sought to prove the viability of ICMetric technology. While the first practical work applied ICMetrics to battery-powered wheelchairs to provide security in Healthcare services in [4]. More recent work in [5] has used ICMetrics technology with accelerometers for authentication in a Healthcare setting.

We build on this latest work in this paper. However, here, and instead, we investigate the possibility of actually exploiting the built in functionality of accelerometers rather than just using raw or post-processed accelerometer axis readings. ICMetrics actually, and naturally, emulates one of the functions we use here for authentication regardless. And, thus providing continuity in the overall research ideas i.e., axis sample averaging.

B. Physical Unclonable Functions

Similar approaches to ICMetrics are used in physical unclonable functions (PUFs), which use on-chip integrated circuit lot-to-lot lithography variations to extract secret keys for use with a challenge response protocol [6]. This technique has been shown to be highly difficult to implement with consistency; and usually requires some form of helper data to generate a stable and reproducible secret key. It also requires integration into a silicon layout, which is notoriously difficult and once manufactured it is fixed. One of the prime benefits of ICMetrics, and the approach taken here, is it is software-based, while still being able to exploit hardware functionality, lot-to-lot lithography variations and characteristics.

C. MEMS Accelerometers

MEMS technology [7] is utilized in a wide range of devices. Recent research [8–11] in the field of sensor based device identification has proven it is feasible to generate device identifiers using accelerometer sensor data. This work was improved upon in [5] and applied in a Healthcare setting. Note, the work in [5] is also the precursor to the research presented in this paper as mentioned in sub-section A.

Since accelerometer sensors have been shown to be useful for security, they have naturally become a point of interest and possible attack. Indeed, work in [12] has shown that is possible to use sound waves to manipulate an accelerometer in an “acoustic attack”.

III. METHODOLOGY

The ADXL345 accelerometer, shown in Figure 1, is used in this work to implement a proof-of-concept and multi-factor authentication scheme using both accelerometer offset values and tap detection technology. It has built-in registers to hold calibration offset values, which are used automatically to compensate axis readings after calibration. The offset values are stored in 8-bit twos complement format and have a scale factor of 15.6mg/LSB. While the values are generated in software and programmed into the OFSX, OFSY and OFXZ registers respectively. Note, the offset registers do not retain their values when power is removed or cycled; and can be re-generated on demand in-field.

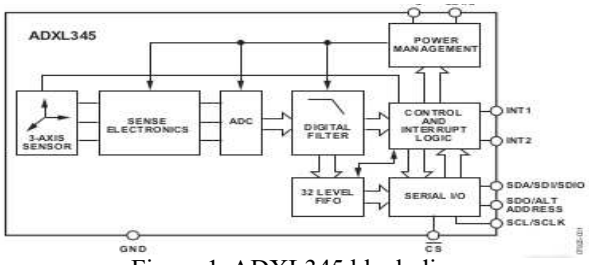

Figure 1, ADXL345 block diagram

To calibrate the ADXL345 one axis calibration is required. This orientates the part such that one axis, typically the z-axis, is in the 1g field of gravity and other axes are in a 0g field. The accelerometer axis readings are then measured by taking the average of a series of at least 10 samples. The final three averages represent the offset values for each of the three axes and are stored in the OFSX, OFSY and OFXZ registers. Since the offset values are intrinsic to the accelerometer, that is, innate to its hardware architecture, while at the same time being unique to the overall device using the part. Here, we propose using them directly for multi-factor authentication by using them to form a 128-bit secret encryption key. However, to generate a usable 128-bit encryption key it is necessary to ensure sufficient diversity, uniqueness and length. We propose to satisfy this requirement by 1) combining the 24-bits of the offset register values with both a device’s 64-bit EUI network identifier (MAC address) and zero-padding, to give a 128-bit string; and, 2) post-processing this 128-bit string with a crystallographic function, here AES S-boxes, to ensure it is cryptographically sound.

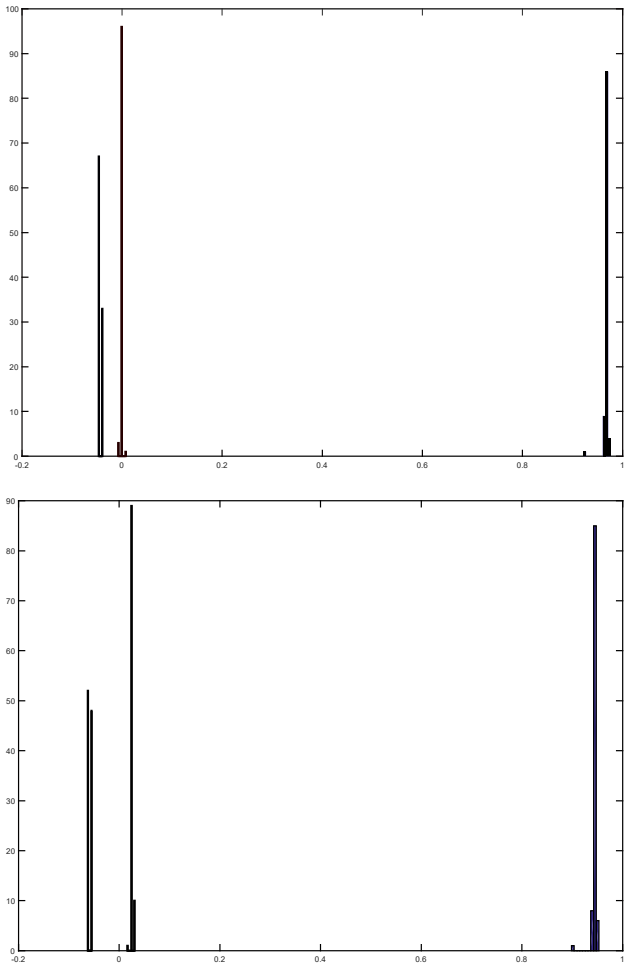

Figure 2, Two ADXL345 three axes readings

Note, for clarity, the underlying approach deviates from the previous work using ICMetrics in [1-2], which builds Gaussian distributions and uses the graph parameters to generate secret encryption keys or hardware identifiers. However, in ICMetrics the graph's average is one of these parameters. This effectively correlates to the ADXL345's calibration offset values, which are the average of 10 or more axis readings. Therefore, the principles of ICMetrics are actually in-built into the hardware functionality of the accelerometer. Figure 2 plots 100 readings taken to generate the offset values for the three axes using two ADXL345 accelerometers. It can be observed they form unique Gaussian like distributions albeit at a low sample count.

The ADXL345 is also capable of recognizing taps, which induce a detectable vibration as shown in Figure 3. This is implemented via a number of in-built parameters, namely the tap detection threshold; the maximum tap duration time; and latency defining the waiting period from the end of the first tap until the start of the time window when a second tap can be detected. In this work, we propose to use the ADXL345's tap detection technology to require the user to tap out the digits of a four-digit personal identification number (PIN) to form part of a multi-factor authentication scheme. For example, 1234 would correspond to: one tap, one-second time separator, two taps, etc. So far, both of the features of the ADXL345 have been described, which can be used as data sources for multi-

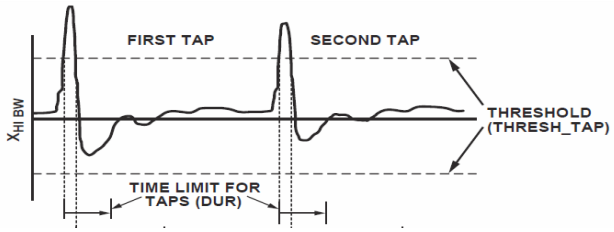

Figure 3, ADXL345 tap detection

factor authentication. Therefore, we now discuss a suitable method to combine them to implement a multi-factor authentication scheme, which can verify whether an arbitrary device is trusted and known. Section IV actually implements and evaluates all of this as a whole note, the methodology is presented in this section only. The first part of the scheme requires that a device is enrolled, which could take place during PCB system assembly, for example. During enrollment, a given device is calibrated and the resultant 128-bit key recorded in a secure database and a four digit PIN generated, which is supplied to the end-user later. It is possible other protocol schemes may not require a database note. Now given the device can re-generate its key in-field as discussed, while the user will know their PIN, which can be tapped out into the device. Therefore, with use of a suitable protocol a multi-factor authentication scheme can be implemented. One possible protocol solution we propose is as follows.

To authenticate a device:

- the host sends a data block of encrypted AES 128-bit data ciphered using the device's enrollment key, it holds another 128-bit AES encryption key inside known only to the host;
- when the device receives the encrypted data block, it re-generates its 128-bit enrollment key, and if the device is authentic it will be able to decrypt the received block of data to get the new 128-bit AES key;
- assuming it has derived the new key, the user now taps out their four digit PIN;
- the PIN the accelerometer works out is encrypted with the new key and sent back to the host;
- if the host can decrypt the received block representing the PIN it will therefore successfully validate the device.

Thus, a multi-factor authentication scheme is accomplished. At the same time, it is all encrypted plus exploiting the functionality of accelerometers; while implemented all in software as per ICMetrics.

Note, the tapping profile will also be user specific and possible to analyze and incorporate for more rigorous authentication, but considered the subject of future work. Furthermore, the protocol and authentication routine suggested above is exemplary. Obviously, cryptographers versed in

formal protocol design, proofs and validation may have improvements and alternatives. The novelty of this work is the possibility of use of in-built accelerometer functionality for multi-factor authentication.

IV. Evaluation

To evaluate this approach an IoT and mobile device emulation system was developed and replicated three times, which is shown in Figure 4. It is based on a commercially available Xilinx FPGA development board (ARTY by Diligent Inc.), which allows various smaller PCB modules to be plugged in as desired. The only requirement is that these modules, known as peripheral modules (PMODs), have either an I2C or SPI interface. Various PMODs are available for purchase from electronics distributors; or they can be constructed relatively easily on a 2-layer PCB.

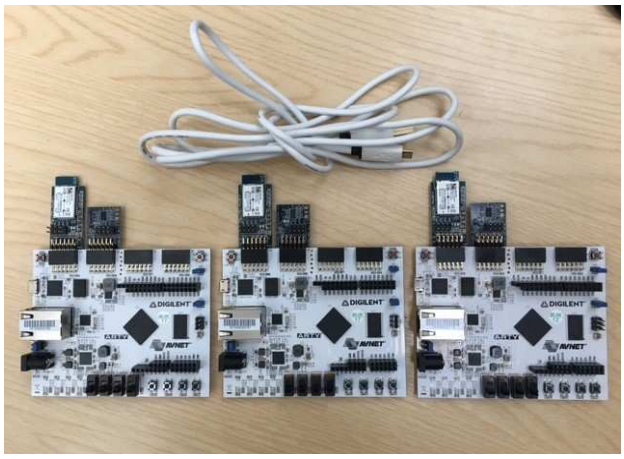

Figure 4, FPGA emulation system boards

Two PMODs are used in the emulation system on each of the three boards: a Bluetooth PMOD and accelerometer PMOD featuring the ADXL345. While a complete SoC system is implemented on the FPGA using Xilinx's 32-bit Microblaze processor. This allows full software control of the emulation system's features and the two attached PMODs i.e., the PMODs can be accessed directly in C code. A more rigorous testbed setup would allow for temperature, voltage and stress testing. However, this system design is aimed, and sufficient to, validate the functionality of the ideas presented.

Key generation proceeds as follows. The offset calibration routine is implemented as a dedicated C function recording 100 samples for each axis, which can be called anywhere in the main execution thread of the 32-bit Xilinx Microblaze processor. Initial experiments revealed the most consistent offset value readings are obtained when the emulation system is placed on a hard and level surface. This also ensures the axes are in 0g (Z-axis) and 1g (X and Y-axes) as needed. Obviously, for in-field use a user would need to do the same to authenticate their device, and feedback given to the user if authentication was not successful. Once the offset calibration C function returns the accelerometer registers, X_offset, Y_offset and Z_offset hold the three 8-bit twos complement offset values (24-bits in total). A synthetic 64-bit EUI network identifier is used as the Bluetooth PMOD only allows a UART interface. This is then combined with the offset register values and zero-padded. This result is then passed through sixteen AES S-boxes to get a final 128-bit key.

The key generation process described above was used for each of the three boards to simulate an enrollment phase, and the 128-bit keys transmitted to a host (MS Windows 8.1 laptop running Matlab) over UART via the Bluetooth PMOD. While three different four digit numbers were generated to simulate user PINs and stored along with the keys on the host. To implement the multi-factor authentication scheme the host encrypted arbitrary 128-bit data strings to send to the emulation boards, and then checked the received result containing the PIN to authenticate the device or not. The setup simply times-out if as response is not received back note.

We next investigated whether the ADXL345 accelerometer could be used effectively for key re-generation as proposed using the aforementioned emulation system hardware and software setup.

We note use of a post-processing function will always ensure the keys are unique between devices and combination with a 64-bit EUI network identifier. Alternatives to using S-boxes may give more uniqueness, and will be explored in future work; for example using a more specific hash function such as SHA-2 or MD6. We also observe it is possible that two offset values for the same axis and different devices could map to the same value. However, that combining with a 64-bit EUI network identifier and zero-padding and post-processing removes how meaningful this could be to an attacker.

Besides uniqueness, what is also important for key re-generation is robustness. That is, how consistently a device's 128-bit key can be re-generated in the field. If this was not possible, or a relatively low hit rate resulted, a device would not be able to be authenticated regardless of the protocol being used. Therefore, to investigate key generation robustness we recreated the enrollment keys 1000 times at 1-second intervals.

It was found that re-generating the keys resulted in a 94.45% accuracy. Predominantly one axis reading slightly differed causing an incorrect key to be generated. We note a deeper investigation into the likelihood and which axis, if any, is predisposed to this effect is warranted. However, this provides an idea of how consistently it can be expected a device using the ADX342 accelerometer can regenerate its key.

Further improvement could be achieved by employing more values for averaging in the calibration routine (currently 100), perhaps programmatically if a device could not be authenticated. Another approach would be to use majority voting scheme after generating a buffer full of axis calibration offset values. However, any extra filtering and post processing of calibration values increases the time to authentication; which on a low performance system, perhaps a fitness tracker, could be a potential disadvantage i.e., selling points.

Further experiments investigated the operation of the protocol and whole system using the three emulation boards. In Matlab the host generated an 128-bit AES encrypted data block (second key) using the relevant stored enrollment key, which was sent via Bluetooth to the board under test. Then the top of the FPGA IC packaging was lightly tapped to simulate input of

a PIN. Approximately, one second between digit taps was used, and a quarter of a second between taps forming a specific digit. The result was then transmitted back to the PC, and the received data (the encrypted PIN with the second key) validated.

This multiple factor authentication experiment was repeated multiple times for each of the emulation boards. It was found the data was being decrypted correctly from key re-generation; however, where the proof-of-concept system lacks and introduces false authentication results even though the correct PIN was tapped is in the tap detection sequence. Further experiments and modifications proved tap detection is highly sensitive requiring tapping to be implemented consistently. Approximately, only two out of five authentication attempts were identified correctly due to this issue.

V. Conclusions

We have proposed combining two technologies in mid-range accelerometers for multi-factor authentication, namely calibration functionality and tap detection technology. A protocol has also been suggested to implement multi-factor authentication. Evaluation on a proof-of-concept emulation system has demonstrated the viability of the initial research, while highlighting the areas where further investigation is required. In particular, there is a need for further research into tap detection technology post-processing.

VI. Future Work

The authors note that there is great scope for both fine-tuning and expanding the idea of using built-in accelerometer features and sensors for multi-factor authentication as discussed in this work.

As example, the latest generate of mobile devices contain ambient light sensors to automatically adjust a screen's contrast, the underlying hardware technology uses phototransistors, which exhibits silicon variability—typically lot-to-lot—meaning readings vary between devices for the same light level.

Acknowledgment

This work has been supported by the CHIST-ERA under the User-Centric Security, Privacy and Trust in the Internet of Things topic through the EU SPIRIT project, funded via EPSRC grants EP/P015956/1 and EP/P016006/1.

References

[1] Y. Kovalchuk, G. Howells, and K. McDonald-Maier, "Overview of ICMetrics technology—Security infrastructure for autonomous and intelligent healthcare system," Intern. J. Serv. Sci. and Technol., vol. 4, pp. 49–60, 2014.

[2] R. Tahir, H. Hu, D. Gu, K. McDonald-Maier, and G. Howells, "A Scheme for the Generation of Strong ICMetric Based Session Key Pairs For Secure Embedded System Applications," In Proceeding of the International Conference on Advanced Information Networking and Applications, Spain, pp. 689–696, March 2013.

[3] E. Papoutsis, "Investigation of The Potential of Generating Encryption Keys For ICMetrics," Ph.D. Thesis, The University of Kent, Canterbury, UK, June 2009.

[4] A. Kokosy, et al., "SYSIASS—An Intelligent Powered Wheelchair," In Proceedings of the 1st International Conference on Systems and Computer Science, France, August 2012.

[5] R. Tahir, H. Tahir and K. McDonald-Maier, "Securing Health Sensing Using Integrated Circuit Metric," Sensors 2015, Vol. 15, no. 10, pp. 26621-26642, 2015.

[6] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science., vol. 297, issue 5589, pp. 2026–2030.

[7] "Defence Advanced Research Project Agency, Micro Electro-Mechanical Systems (MEMS)," Annu. Rev. Fluid Mechan, pp. 579-612, 1998.

[8] M. Feng, Y. Fukuda, M. Mizuta, and E. Ozer, "Citizen sensors for SHM: Use of accelerometer data from smartphones," Sensors, vol. 15, pp. 2980-2998, 2015.

[9] S. Dey, N. Roy, W. Xu, R.R. Choudhury, and S. Nelakuditi, "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable," In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS), USA, 2014.

[10] "Mobile Device Identification via Sensor Fingerprinting," National Research & Simulation Center, Rafael, Internal Report 2014. Available online: https://crypto.stanford.edu/gyrophone/sensor_id.pdf (accessed on 1 June 2017).

[11] A. Aysu, N.F. Ghalaty, Z. Franklin, M.P. Yali, and P. Schaumont, "Digital Fingerprints for Low-Cost Platforms Using MEMS Sensors," In Proceedings of the Workshop on Embedded Systems Security, Canada, 2013.

[12] http://spectrum.ieee.org/tech-talk/telecom/security/smartphone-accelerometers-can-be-fooled-by-sound-waves

[13] http://www.analog.com/media/en/technical-documentation/data-sheets/ADXL345.pdf