Energy Consumption of Cryptographic Algorithms in Mobile Devices

J. Toldinas[1], R. Damasevicius[2], A. Venckauskas[1], T. Blazauskas[2], J. Ceponis[1]
[1]*Department of Computer Science, Kaunas University of Technology, Studentu St. 50, LT-51368 Kaunas, Lithuania*
[2]*Department of Software Engineering, Kaunas University of Technology, Studentu St. 50, LT-51368 Kaunas, Lithuania*
robertas.damasevicius@ktu.lt

***Abstract*—Modern business information technologies, such as Cloud computing and Bring Your Own Device (BYOD) raise new requirements for end node security. Cryptographic algorithms must be used to ensure security of business data and communications. However, data encryption decreases battery lifetime on mobile devices such as smartphones or tablet PCs. In this paper, we provide an analysis of energy consumption characteristics of cryptographic algorithms from Bouncy Castle Crypto API. We propose a cryptography-oriented energy-security trade-off model and use it to evaluate energy-efficiency of cryptographic algorithms.**

***Index Terms*—Energy consumption, battery lifetime, mobile device, security, cryptography.**

I. INTRODUCTION

Revolutionary growth of hardware capabilities combined with increasingly small size and low weight brings many opportunities for using mobile devices, such as smart phones, laptops, and tablet PCs, for business and entertainment at home, in airport, at office, i.e., everywhere and everywhen. Modern business information technologies such as Cloud computing [1] and Bring Your Own Device (BYOD) [2] gives a new way for companies to do business not only in a mobile manner, but also using employee's own devices. BYOD describes a novel business trend of using the employee-owned devices in the workplace. It is part of the broader phenomenon of the dual use of personal devices and software of employees for private and professional purposes within commercial enterprises.

However, security of confidential business information is a matter of concern. Companies and their employees must have assurance that information, which is being downloaded and saved on a mobile device, will be accessed only by an authorized user. This requires securing of both data storage and communication and on mobile devices regardless of how the users access information [3].

Manuscript received January 5, 2014; accepted March 12, 2014.

The work described in this paper has been carried out within the framework the Operational Programme for the Development of Human Resources 2007-2013 of Lithuania „Strengthening of capacities of researchers and scientists" project VP1-3.1-ŠMM-08-K-01-018 „Research and development of Internet technologies and their infrastructure for smart environments of things and services" (2012-2015), funded by the European Social Fund (ESF).

The main issue which sill restricts long term usability of mobile devices is battery lifetime because mobile devices are not always connected to a stationary power supply, but are supplied from batteries, and the portability requirement imposes constraints on the size and weight of batteries. Battery technologies are no experiencing such technological progress as semiconductor and wireless communication technologies do. Battery capacity is therefore the main challenge to evolution of modern mobile systems and applications.

Furthermore, a user may install and use many additional applications. Every continuously working application drains power from the mobile device's battery. As a consequence, for new smart phones the average battery life is usually less than two days [4], and for used smart phones it is even shorter. As a response, 80 % of mobile phone users take measures to increase their battery lifetime [5].

Traditional cryptography protocols require significant energy to process and transmit data. To prolong battery lifetime, a mobile device should use the minimum energy level possible while at the same time ensuring the acceptable level of security. Considering limited energy budget of mobile devices, security each algorithm achieves has to be modelled as a function of its energy consumption [6].

Therefore, two issues – security and energy consumption – are most important for mobile end nodes. Extensive research exists on extending battery lifetime of mobile computing systems, understanding charging behaviour and battery indicators, customizing power-saving settings [5], predicting power consumption level [7]. However, any energy management policy requires accurate prediction of energy consumption and battery lifetime, which is impossible without reliable energy measurement and estimation methods and tools. The prediction of the battery lifetime is possible only when the behaviour of the battery can be modelled reliably so that the users could decide themselves how to use the available battery time in a most effective and secure way. The analysis of the energy measurement methodologies has been presented in [8].

In this paper we investigate the influence of the cryptographic algorithms workload on the battery lifetime. We analyse main classes of cryptographic algorithms, propose the empirical cryptography-oriented energy-security

trade-off model and present the experimental results.

II. ENERGY-SECURITY TRADE-OFF MODEL

The task is to identify dependencies between cryptographic algorithms energy consumption, key size and performance trade-offs on one hand, and user used cryptography scenarios on the other hand. A trade-off is a relationship between two aspects of system's quality parameters.

A key issue here to be addressed is to find the right trade-off between energy consumption and the required security performance, i.e., how should the processes in the mobile device be organized such that the battery lifetime (which determines the system lifetime) will be as high as possible while the security characteristics are maintained [9]. In this paper, we consider a trade-off between security strength and energy consumption in mobile devices.

The energy-security trade-off is a utility function U that defines a relationship between energy metric E and security metric S as a weighted sum of objective functions, which is similar to the performance-security trade-off function proposed in [10] as follows

$$\max U = wE + (1-w)S, \tag{1}$$

where w is a weighting factor representing user preference on energy and security, respectively.

The energy and security metrics allow to calculate how much protection a security mechanism (cryptographic algorithm) can provide and how much battery capacity (lifetime) will be reduced by using given security mechanism.

Given the same security strength and energy constraint, the key factor is the selection of the cryptographic algorithm that satisfies both energy and security constrains.

Given the energy-security trade-off function, the best security parameters can be calculated according to the system requirements to achieve the best trade-off between energy consumption and security strength.

With the defined energy metric E and security metric S, the system requirements can be formulated quantitatively. However, both metrics are related, because a more secure cryptographic algorithm usually requires more computations, which in turn leads to higher energy consumption.

Evaluation of security of cryptographic algorithm is a complex problem, because security usually means ability to withstand an attack, which is difficult to evaluate. In practice, key size in bits can be used as approximate measure of security strength, number of rounds, the size of the modulus, the size of crypto-block, the speed-of-the-diffusion/confusion (how fast all bits get affected, are they all equally affected, etc.), the side-channel information the ciphers provide (trapdoor, rainbow-tables), robustness to errors, number of collisions (in birthday attack), etc. are important, too.

We assume that key size k, message length m and battery capacity drain ΔC for a cryptography algorithm are related as follows

$$\Delta C \sim a \cdot m \cdot k^b + £, \tag{2}$$

where a and b are free coefficients, and $£$ is measurement error (noise).

Assuming that the impact of error $£$ is negligible for a cryptography application, we can derive the following model

$$\frac{\Delta C}{m \cdot k^b} \sim const. \tag{3}$$

Given different key sizes for each cryptography algorithm we formulate the problem of finding the characteristic value of free coefficient b as an optimization problem as follows

$$b_{char} = \min_{K}\left[RSD\left(\frac{\Delta C}{m \cdot K^b}\right)\right], \tag{4}$$

where RSD is relative standard deviation (standard deviation divided by mean value), and K is a set of key sizes.

We can calculate the characteristic value of a for a given cryptographic algorithm as follows

$$a_{char} = \frac{\Delta C}{m \cdot k^{b_{char}}}. \tag{5}$$

Then for any available energy budget value C_{budget} we can calculate a key size of a cryptographic algorithm, which can be used to encode a message within energy constraints as follows

$$k = \left(\frac{C_{budget}}{a_{char} m}\right)^{1/b_{char}}. \tag{6}$$

As key size is usually defined in terms of power values of 2, we rewrite (6) as follows

$$k = 2^{\left\lfloor \log_2\left(\left(\frac{C_{budget}}{a_{char} m}\right)^{1/b_{char}}\right)\right\rfloor}. \tag{7}$$

We claim that (7) can be used as energy-security trade-off model to calculate available values of security parameters (i.e., key size) of cryptographic applications within available energy budget.

However, reliability of such model depends upon model of battery capacity measurement, which is considered next.

III. MODEL OF BATTERY CAPACITY MEASUREMENT

Many different battery lifetime models (such as electrochemical, electrical circuit, analytical, kinetic, diffusion, stochastic) have been proposed (see, e.g., [3], [9]). Most of these models have been developed for use in variety areas.

The state of the battery capacity C_{used} is a time-dependent function and at any given time can be described by (8)

$$C_{used} = C_{tsart} - C_{tend}, \quad (8)$$

where C_{tstart} is the battery capacity measured at the beginning of the measurement experiment, C_{tend} is the battery capacity measured at the end of the measurement experiment, and C_{used} is the drain of battery capacity charge used during the experiment.

In practice, the state of the battery is influenced by many factors, therefore, the battery charge values are measured at several consecutive time intervals as described by (9)

$$C_{\Delta t} = C_{tsart} - \sum_{t=t_0}^{t_0+\Delta t} (C_{tstart} - C_t), \quad (9)$$

where $C_{\Delta t}$ is the drain of battery charge, and Δt is time interval of capacity measurement points.

Our battery lifetime model is based on the following assumptions:

1. Battery capacity is measured at an application level;
2. First measurement is a starting point for evaluation given cryptographic algorithm;
3. Δt is equal to 1 second;
4. Measurements can be stopped when the battery capacity drain is less than 50 % of capacity measured at starting point.

IV. Case Study and Experimental Results

The experiments were performed on DELL Latitude D420 laptop PC running Microsoft Windows OS on Intel® Core Duo Yonah 1.20 GHz CPU, 1 GB DDR2-266 SDRAM, Mobile Intel® 945 GM Express Chipset.

We have used the Lena.bmp benchmark image (resolution 512 × 512), which is encrypted with a cryptographic algorithm. During measurements, we registered battery charge level and capacity in mAh every 1 s starting from the charged battery. We have adopted the measurement methodology already described in [8].

The results of measurements are presented graphically in Fig. 1–Fig. 4.

Figure 1 shows average battery capacity drain in mAh per message MB for symmetric cryptography algorithms.

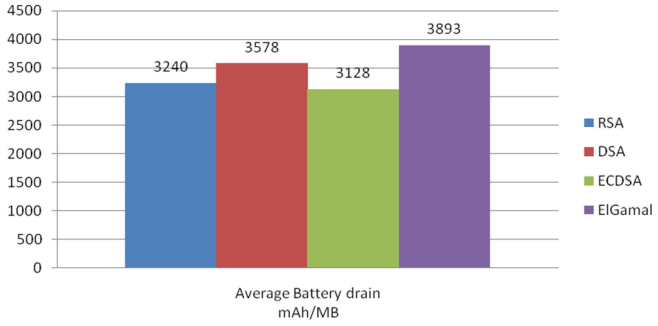

Fig. 1. Battery capacity drain (mAh/MB) for symmetric cryptography algorithms.

Figure 2 shows the same for asymmetric cryptography algorithms.

Figure 3 shows comparison of symmetric cryptographic algorithms by energy required to encode 1 MB of data, while Fig. 4 shows the same for asymmetric algorithms.

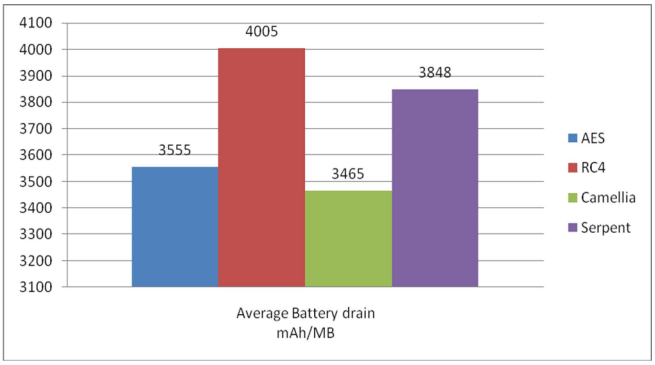

Fig. 2. Battery capacity drain (mAh/MB) for asymmetric cryptography algorithms.

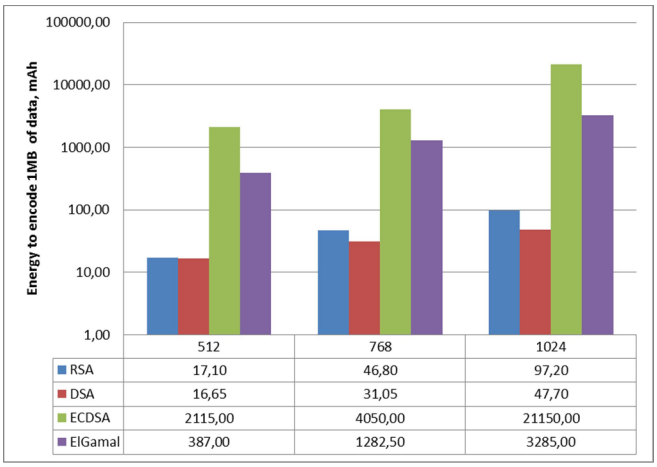

Fig. 3. Comparison of symmetric cryptographic algorithms by energy consumption.

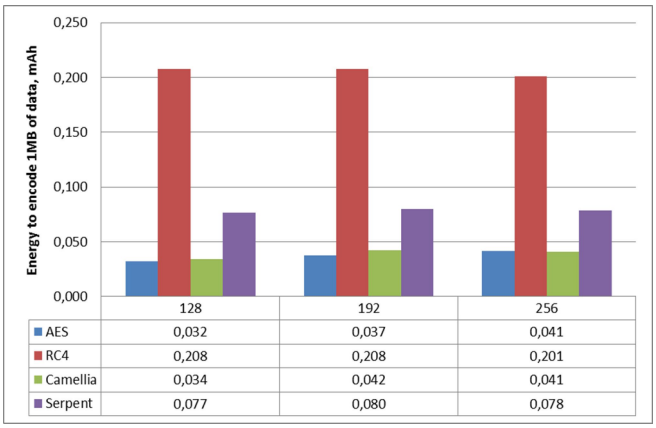

Fig. 4. Comparison of asymmetric cryptographic algorithms by energy consumption.

V. Evaluation

Experimental results (Fig. 4, Fig. 5) show that RSA and DSA are most energy-efficient symmetric cryptographic algorithms, while AES and Camelia are most energy efficient asymmetric algorithms of the analysed ones. The results correspond well to the study reported in [11].

We use the experimental results to evaluate the energy-security trade-off model proposed in Section III. The calculated characteristic model values (4) are presented in

Table I for symmetric cryptography algorithms and in Table II for asymmetric cryptography algorithms.

Our experimental results correspond well to the results presented in [12]. The energy cost of asymmetric algorithms is very much dependent on the key size (the value of the key size exponent parameter value $b_{char} > 1$), while that of symmetric algorithms is not affected to the same extent by the key size ($b_{char} < 1$). The reason is that only a part of a symmetric algorithm, i.e., key set-up (key expansion) depends upon key size. Therefore, as requirements for security strength increase, asymmetric cryptography algorithms become more energy-hungry than symmetric algorithms (also noted in [11], [12]).

TABLE I. CHARACTERISTIC VALUES OF THE PROPOSED ENERGY-SECURITY TRADE-OFF MODEL FOR SYMMETRIC CRYPTOGRAPHY ALGORITHMS.

Symmetric cryptography algorithm	**Exponent of key size (b_{char})**	**RSD**
RSA	2.51	0.0047
DSA	1.52	0.0035
ECDSA	2.36	0.0119
ElGamal	3.08	0.0246

TABLE II. CHARACTERISTIC VALUES OF THE PROPOSED ENERGY-SECURITY TRADE-OFF MODEL FOR ASYMMETRIC CRYPTOGRAPHY ALGORITHMS.

Asymmetric cryptography algorithm	**Exponent of key size (b_{char})**	**RSD**
AES	0.35	0.0030
RC4	0	0.0159
Camellia	0.31	0.0475
Serpent	0.03	0.0116

Finally, we also can use the proposed model to calculate the value of the security parameter (i.e., key size) of the cryptography application given the available energy budget of the mobile device (7).

VI. CONCLUSIONS

1. We have proposed the theoretical energy-security trade-off model for describing relationship between energy consumption and security strength of crypto algorithms.

2. We have performed analysis and experimental research of energy consumption of symmetric and asymmetric cryptography algorithms.

3. We have validated the theoretical energy-security trade-off model with our experimental data. The results show that the energy consumption of asymmetric algorithms is very much dependent on the key size of the algorithm, while energy consumption of symmetric algorithms is not affected to the same extent by the key size. This conclusion is confirmed by the results of other authors [12], [11].

4. The results of the paper can be used by other researchers to evaluate energy-efficiency of designed network and data security protocols and applications.

ACKNOWLEDGEMENT

The authors wish to thank G. Grigaravičius for his valuable efforts in recording the experimental data.

REFERENCES

[1] H. Yu, N. Powell, D. Stembridge, X. Yuan, "Cloud computing and security challenges", in *Proc. of the 50th Annual Southeast Regional Conf. (ACM SE 12)*, Tuscaloosa, AL, USA, 2012, pp. 298–302.

[2] A. Armando, G. Costa, A. Merlo, "Bring your own device, securely", *in Proc. of the 28th Annual ACM Symposium on Applied Computing (SAC 2013)*, Coimbra, Portugal, 2013, pp. 1852–1858. [Online]. Available: http://dx.doi.org/10.1145/2480362.2480707

[3] G. Thomson, "BYOD: enabling the chaos", *Network Security Journal*, vol. 2012, no. 2, pp. 5–8, 2012. [Online]. Available: http://dx.doi.org/10.1016/S1353-4858(12)70013-2

[4] N. Korhonen, "Predicting mobile device battery life", M.S. thesis, Aalto University, Finland, 2011.

[5] A. Rahmati, A. Qian, L. Zhong, "Understanding human-battery interaction on mobile phones", in *Proc. 9th Int. Conf. Human Computer Interaction with Mobile Devices and Services (MobileHCI 2007)*, Singapore, 2007, pp. 265–272.

[6] N. Fotiou, G. F. Marias, G. C. Polyzos, P. Szalachowski, Z. Kotulski, M. Niedermeier, X. He, H. De Meer, "Towards adaptable security for energy efficiency in wireless sensor networks", in *Proc. 28th meeting of the Wireless World Research Forum (WWRF 2012)*, Athens, Greece, 2012, pp. 1–6.

[7] C. Krintz, Y. Wen, R. Wolski, "Application-level prediction of battery dissipation", in *Symposium on Low Power Electronics and Design (ISLPED 2004)*, Newport Beach, CA, USA, 2004, pp. 224–229.

[8] R. Damasevicius, V. Stuikys, J. Toldinas, "Methods for measurement of energy consumption in mobile devices", *Metrology and Measurement Systems*, vol. 20, no. 3, pp. 419–430, 2013. [Online]. Available: http://dx.doi.org/10.2478/mms-2013-0036

[9] M. R. Jongerden, *Model-based energy analysis of battery powered systems*, Ph.D. dissertation, University of Twente, the Netherlands, 2010.

[10] W. Zeng, M.-Y. Chow, "A trade-off model for performance and security in secured Networked Control Systems", in *Proc. of IEEE Int. Symposium on Industrial Electronics (ISIE)*, 2011, pp. 1997-2002.

[11] H. Rifa-Pous, J. Herrera-Joancomarti, "Computational and energy costs of cryptographic algorithms on handheld devices", *Future Internet*, vol. 3, pp. 31–48, 2011. [Online]. Available: http://dx.doi.org/10.3390/fi3010031

[12] N. R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "Analyzing the energy consumption of security protocols", in *Proc. 2003 Int. Symp. Low Power Electronics and Design (ISLPED 2003)*, ACM, New York, NY, USA, pp. 30–35.