UNIVERSITÀ DEGLI STUDI DI MILANO

SCIENZE E TECNOLOGIE

Riassunto di tesi di

Mattia Oldani

(matricola 966668)

Relatore

Andrea Visconti

Corso di laurea in

INFORMATICA- Milano

Titolo dell'elaborato

ASCON: ANALISI PRESTAZIONALE DEL NUOVO STANDARD INTERNAZIONALE PER LA CRITTOGRAFIA LIGHTWEIGHT

1 Ente presso cui è stato svolto il lavoro di stage

Il lavoro di tirocinio è stato di tipologia interna presso il dipartimento di Informatica dell'Università degli Studi di Milano, sotto la supervisione del docente Andrea Visconti.

2 Contesto iniziale

Il lavoro svolto riguarda la parte sperimentale nel contesto dello studio e dell'analisi della famiglia di algoritmi crittografici ASCON, dichiarata come nuovo standard per la crittografia lightweight il 7 febbraio 2023 da parte del NIST.

3 Obiettivi del lavoro

Il lavoro di tirocinio si concentra sull'analisi prestazionale degli algoritmi presentati da ASCON nella gara del NIST. Considerata la natura lightweight degli algoritmi, le piattaforme utilizzate per il testing sono tre dispositivi IoT: Arduino Due, Adafruit ItsyBitsy M0 Express e Raspberry Pi 3 Model B.

Gli obiettivi sono:

I. Mostrare quali algoritmi sono i migliori per tempi di esecuzione e spazio utilizzato;

II. Quali implementazioni sono le migliori per ogni algoritmo.

Le implementazioni riguardano l'architettura del processore (ARM, ESP, AVX ecc.), la dimensione massima di dati che esso può gestire (8 bit, 32 bit, 64 bit, ecc.) o particolari instruction set (funnel-shift, base, ecc.).

4 Descrizione del lavoro svolto

Il lavoro, per ogni dispositivo testato, ha prima richiesto un setup della suite di test, con la creazione dei folder contenenti i file delle implementazioni da testare e un "main" che coordinasse i file precedenti. Il pool di implementazioni da testare è stato selezionato in base all'architettura hardware dei device a disposizione.

Il file "main", invece, è una semplice modifica del file fornito da ASCON per permettere la compilazione della suite di test su Arduino IDE[1] e per eseguire testing su precise dimensione di plaintext[2].

Successivamente si è proseguito con la compilazione e la raccolta dati. Le prime due board presentate si sono affidate all'Arduino IDE per la compilazione, mentre l'ultima si è servita del compilatore "gcc" direttamente dal terminale. L'esecuzione delle suite di test ha generato una serie di dati raccolti e salvati sotto forma di record in file CSV facilmente interrogabili.

In ultima istanza sono stati analizzati i dati raccolti tramite notebook Jupyter.

[1] Per le board Arduino e Adafruit.

[2] Per ogni board.

5 Tecnologie coinvolte

Sono state coinvolte le seguenti tecnologie:

- Famiglia di algoritmi crittografici lightweight ASCON;
- Arduino IDE per la compilazione delle suite di test per i device Arduino e Adafruit;
- Linguaggi C, C++ e Arduino per la scrittura (parziale) del file "main" descritto in precedenza;
- Python e Bash per l'automazione di task quali compilazione, raccolta dati e creazione di folder contenenti le implementazioni da testare;
- Python e Jupyter Notebook per l'analisi dei dati raccolti.

6 Competenze e risultati raggiunti

Le analisi sui dati raccolti hanno evidenziato gli ottimi tempi di esecuzione degli algoritmi presentati da ASCON e, considerando specifiche implementazioni, anche un ottimo spazio utilizzato. Questo risultato sottolinea inoltre la grande duttilità che può fornire ASCON: su architetture con forti limiti di spazio possono essere impiegate implementazioni che, una volta compilate, occupano poco spazio in memoria ma che garantiscono comunque ottime prestazioni; mentre su architetture che danno priorità ai tempi di esecuzione possono essere impiegate implementazioni molto rapide.

Il lavoro di tirocinio ha permesso di familiarizzare con i microcontrollori, per merito di Arduino IDE che ne fornisce una suite di compilatori; inoltre ha contribuito anche nella scrittura, seppur parziale, di programmi eseguibili per questi dispositivi. Il testing e la raccolta dei risultati hanno seguito un approccio nuovo, con una suite di test corposa ma focalizzata su precise grandezze di plaintext.

Infine, il lavoro ha costruito i rapporti con il docente – sempre disponibile per rispondere a dubbi e controllare continuamente lo svolgersi del lavoro – e con i colleghi. Con questi ultimi sono stati cruciali la sincronizzazione nell'utilizzo dei dispositivi fisici e i consigli rapidi ed efficaci – in entrambe le direzioni – che hanno permesso a tutti di poter ottenere il massimo dal proprio lavoro di tirocinio.

7 Bibliografia

[1] *Adafruit ItsyBitsy M0 Express*. URL: https://www.adafruit.com/product/3727 (visitato il 28/08/2023).

[2] *Arduino Due*. URL: https://docs.arduino.cc/hardware/due/ (visitato il 18/03/2024).

[3] *Ascon contact*. URL: https://ascon.iaik.tugraz.at/contact.html (visitato il 27/02/2024).

[4] *Ascon overview*. URL: https://ascon.iaik.tugraz.at/index.html (visitato il 27/02/2024).

[5] *Ascon specification*. URL: https://ascon.iaik.tugraz.at/specification.html (visitato il 03/04/2024).

[6] *Che cos'è l'IoT?* URL: https://www.oracle.com/it/internet-of-things/what-is-iot/#industries-iot (visitato il 12/03/2024).

[7] *Cos'è l'HCP?* URL: https://www.ibm.com/it-it/topics/hpc (visitato il 11/03/2024).

[8] *Introduction to IoT - Advantages of IoT*. URL: https://arxiv.org/pdf/2312.06689.pdf (visitato il 11/03/2024).

[9] *Introduction to IoT - Challenges and Future Directions*. URL: https://arxiv.org/pdf/2312.06689.pdf (visitato il 11/03/2024).

[10] *Lightweight Cryptography - Overview*. URL: https://csrc.nist.gov/Projects/Lightweight-Cryptography (visitato il 19/03/2024).

[11] *Lightweight Cryptography - Round 1*. URL: https://csrc.nist.gov/Projects/lightweight-cryptography/round-1-candidates (visitato il 19/03/2024).

[12] *Lightweight Cryptography - Round 2*. URL: https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates (visitato il 19/03/2024).

[13] *Lightweight Cryptography - Timeline*. URL: https://csrc.nist.gov/projects/lightweight-cryptography/timeline (visitato il 19/03/2024).

[14] *List of ARM processors*. URL: https://en.wikipedia.org/wiki/List_of_ARM_processors (visitato il 28/09/2023).

[15] *RaspberryPi model 3B*. URL: https://www.raspberrypi.com/products/raspberry-pi-3-model-b/ (visitato il 11/11/2023).

[16] *Repository Github di ASCON*. URL: https://github.com/ascon/ascon-c (visitato il 04/03/2024).

[17] *Sistemi embedded: cosa sono e a cosa servono*. URL: https://www.internet4things.it/iot-library/sistemi-embedded-cosa-sono-e-a-cosa-servono/ (visitato il 12/03/2024).

[18] *The Ascon Family: Lightweight Authenticated Encryption, Hashing, and More*. URL: https://csrc.nist.gov/csrc/media/Presentations/2023/the-ascon-family/images-media/june-21-mendel-the-ascon-family.pdf (visitato il 04/03/2024).

[19] *What is the IoT? - Introduction*. URL: https://www.ibm.com/topics/internet-of-things (visitato il 11/03/2024).

[20] *What is the IoT? - Risks and challenges in IoT*. URL: https://www.ibm.com/topics/internet-of-things (visitato il 11/03/2024).