AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

WYDZIAŁ INFORMATYKI, ELEKTRONIKI I TELEKOMUNIKACJI

KATEDRA TELEKOMUNIKACJI

Praca dyplomowa inżynierska

Opracowanie biblioteki programistycznej do bezpiecznego uwierzytelniania urządzeń AVR.

Development of libraries for authentication of AVR devices.

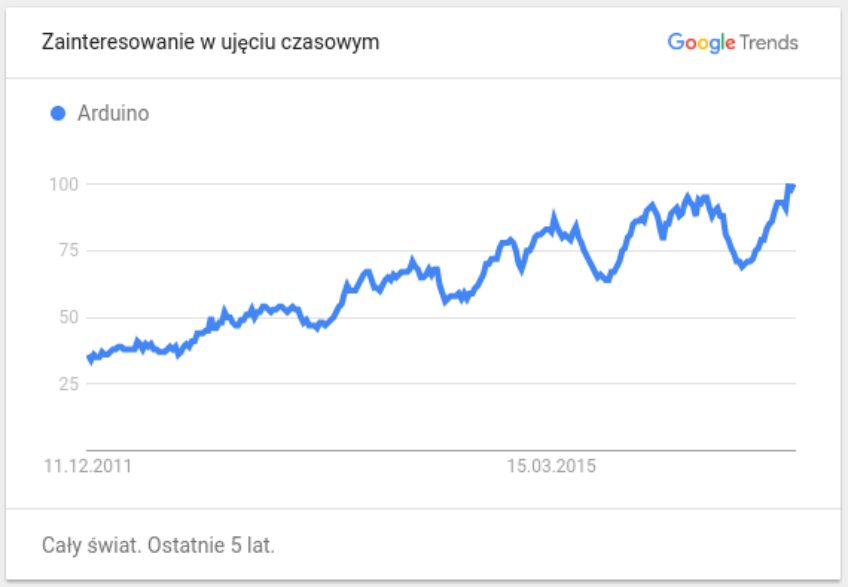
Autor: *Kacper Żuk*
Kierunek studiów: *Teleinformatyka*
Opiekun pracy: *dr inż. Jarosław Bułat*

Kraków, 2016

Uprzedzony o odpowiedzialności karnej na podstawie art. 115 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.): „Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystycznego wykonania albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.", a także uprzedzony o odpowiedzialności dyscyplinarnej na podstawie art. 211 ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (t.j. Dz. U. z 2012 r. poz. 572, z późn. zm.): „Za naruszenie przepisów obowiązujących w uczelni oraz za czyny uchybiające godności studenta student ponosi odpowiedzialność dyscyplinarną przed komisją dyscyplinarną albo przed sądem koleżeńskim samorządu studenckiego, zwanym dalej «sądem koleżeńskim».", oświadczam, że niniejszą pracę dyplomową wykonałem(-am) osobiście i samodzielnie i że nie korzystałem(-am) ze źródeł innych niż wymienione w pracy.

Spis treści

1. Wstęp



Rys. 1.1. Relatywna liczba wyszukiwań frazy „Arduino” w ostatnich pięciu latach. Źródło: Google Trends

AVR to rodzina mikroprocesorów opracowana i rozwijana przez firmę Atmel. Oparta o nią jest m. in. platforma Arduino, która – jak przedstawiono na Rys. 1.1 – z roku na rok zyskuje popularność. Platforma Arduino zaprojektowana została z myślą o osobach, które niekoniecznie posiadają formalne wykształcenie inżynierskie [1]. Jest ona też często używana do prototypowania urządzeń, wpisujących się w koncepcję *Internetu Rzeczy (ang. Internet of Things, IoT)*.

Urządzenia wbudowane podłączone do Internetu są szczególnie narażone na ataki. W 2016 roku podatne urządzenia wbudowane zostały wykorzystane do przeprowadzenia masywnych ataków typu DDoS [2].

1.1. Cele pracy

Istotne jest więc dostarczenie narzędzi, które pozwalają nie tylko na szybkie prototypowanie, ale które pozwolą także zachować odpowiedni poziom bezpieczeństwa. Należy pamiętać przede wszystkim o tym, że urządzenia *IoT* są tworzone także przez ludzi bez formalnego wykształcenia inżynierskiego.

W niniejszej pracy przedstawiono protokół bezpiecznej komunikacji oraz bibliotekę programistyczną na urządzenia AVR zaprojektowane z myślą o prostocie obsługi. Wybrane zostały zestawy algorytmów, które zapewniają niezbędny poziom bezpieczeństwa. Ich złożoność została ukryta za prostym interfejsem programistycznym *(ang. API)*, który nie pozwala na wprowadzenie błędów zmniejszających bezpieczeństwo. Zaproponowane rozwiązanie zapewnia poufność, autentyczność oraz integralność przesyłanych danych.

1.2. Zawartość pracy

W rozdziale 2 scharakteryzowana jest platforma sprzętowa AVR, ze szczególnym uwzględnieniem jej ograniczeń. Następnie w rozdziale 3 przedstawione zostały różne metody uwierzytelniania i uzasadniony został wybór konkretnych rozwiązań. Implementacja została szczegółowo opisana w rozdziale 4. Całość rozwiązania została zwalidowana poprzez porównanie z implementacją na inną platformę, co opisano w rozdziale 5. W rozdziale 6 podsumowano całe rozwiązanie oraz przedstawiono jest ograniczenia i słabe strony.

Całość kodu źródłowego dostępna jest w serwisie GitHub[1].

[1] *https://github.com/kacperzuk/seconn*

2. Charakterystyka platformy sprzętowej

Mikropocesory Atmel AVR są w większości 8-bitowe i na takich skupia się ta praca. Rodzina AVR jest dość szeroka, od ATtiny4 z 32 bajtami SRAM *(ang. Static Random Access Memory)* [3] do ATxmega384C3 z 32 kilobajtami SRAM [4]. W pracy wykorzystywany był model ATmega32u4 z 2.5 kilobajta SRAM [5].

To właśnie SRAM jest głównym ograniczeniem – 32 bajty nie są wystaczające do przeprowadzania operacji, przy których sam klucz zajmuje 16 lub 32 bajty. Należy też pamiętać, że obsługa bezpiecznego połączenia nie może zajmować całości pamięci. Część musi zostać na obsługę peryferiów oraz właściwą logikę programu.

3. Metody uwierzytelniania

3.1. Kryptografia asymetryczna

RSA ECC ElGamal DSA

Czym sie charakteryzuja, kto je rekomenduje i dlaczego.

https://www.keylength.com/en/4/

3.2. Kryptografia symetryczna

ECBC-MAC OMAC CCM HMAC

4. Implementacja

4.1. Generowanie współdzielonego klucza

4.2. Szyfrowanie wiadomości

4.3. Uwierzytelnienie wiadomości

4.4. Protokół komunikacji

5. Walidacja

Informacja o bibliotece dla Javy i przykladowych implementacjach.

6. Podsumowanie

?

Bibliografia

[1] M. Shiloh M. Banzi. *Getting Started with Arduino: The Open Source Electronics Prototyping Platform*. Sebastopol: Maker Media, Inc., 2014.

[2] M. McKeay i in. *Q3 2016 State of the Internet Security Report*. Spraw. tech. Akamai Technologies, Inc., 2016.

[3] *ATtiny4 / ATtiny5 / ATtiny9 / ATiny10 - Datasheet Summary*. Atmel. 2016. URL: *http://www.atmel.com/Images/Atmel-8127-AVR-8-bit-Microcontroller-ATtiny4-ATtiny5-ATtiny9-ATtiny10_Datasheet-Summary.pdf* (dostęp dnia 2016-12-06).

[4] *ATxmega384C3 - Datasheet*. Atmel. 2016. URL: *http://www.atmel.com/Images/Atmel-8361-8-and-16-bit-AVR-XMEGA-Microcontrollers-ATxmega384C3_Datasheet.pdf* (dostęp dnia 2016-12-06).

[5] *ATmega16U4/ATmega32U4 - Datasheet*. Atmel. 2016. URL: *http://www.atmel.com/Images/Atmel-7766-8-bit-AVR-ATmega16U4-32U4_Datasheet.pdf* (dostęp dnia 2016-12-06).