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

O tym ze jest teraz IoT, o tym ze wazne jest bezpieczenstwo tego IoT (vide botnet Mirai), ze brak jest metod przystepnych dla userow, ze sa dostepne tylko prymitywy, ale brak zebrania tego wszystkiego razem w cos, w czym nie da sie popelnic bledu.

2. Metody uwierzytelniania

2.1. Kryptografia asymetryczna

RSA ECC ElGamal DSA
Czym sie charakteryzuja, kto je rekomenduje i dlaczego.
https://www.keylength.com/en/4/

2.2. Kryptografia symetryczna

ECBC-MAC OMAC CCM HMAC

3. Charakterystyka platformy sprzętowej

AVR, szeroko używane w IoT, jest fajne Arduino. 8-bitowy. Od ATtiny4 z 32B SRAM (*http://www.atmel.com/Images/Atmel-8127-AVR-8-bit-Microcontroller-ATtiny4-ATtiny5-ATtiny9-ATtiny10_Datasheet-Summary.pdf*) do ATxmega384C3 z 32KB SRAM (*http://www.atmel.com/Images/Atmel-8361-8-and-16-bit-AVR-XMEGA-Microcontrollers-ATxmega384C3_Datasheet.pdf*).

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

?