Kryptografia w IoT

Wiesław Maleszewski

Instytut Informatyki i Automatyki

Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży

wmaleszewski@pwsip.edu.pl

Streszczenie

W ostatnich latach zauważamy dynamiczny rozwój nowoczesnych technologii stosowalnych w infrastrukturze Internetu Rzeczy (IoT). Rozwój ten wpływa na większą dostępność i zarazem popularność urządzeń, które znajdują swoje zastosowania w różnych dziedzinach. Uzyskujemy wiele ułatwień, które niestety jednocześnie generują szereg zagrożeń związanych z bezpieczeństwem informacji oraz ochroną prywatności. Szeroki zakres zastosowań Internetu Rzeczy często daje możliwość śledzenia nas w różnych obszarach funkcjonowania. Producenci, zwłaszcza mniej renomowanych marek, skupiają się na wytworzeniu użytecznych produktów o konkurencyjnych cenach. Stosowanie ciężkich protokołów kryptograficznych znacząco obniża czas pracy urządzeń zasilanych bateryjnie, co negatywnie wpływa na ich funkcjonalność. Konsekwencją tego stanu rzeczy jest częściowe pomijanie gwarantów ochrony danych. Współczesna kryptografia musi sprostać wymogom opracowania protokołów generujących mniejsze koszty obliczeniowe, a jednocześnie niosących odpowiedni poziom ochrony. Protokoły te mają szansę stać się powszechnie akceptowalnym i stosowalnym standardem, jakiego obecnie brakuje – zwłaszcza w urządzeniach z ograniczonym dostępem do zasilania.

Wstęp

W 2020 r. ok. 50 mld urządzeń ma być podłączonych do sieci. Wielu ekspertów zwraca uwagę, że są one słabo zabezpieczone i będzie to raj dla cyberprzestępców.

Przed pojawieniem się Internetu Rzeczy zbieraliśmy tak dużo danych ile trzeba i tak mało ile się da. Urządzenia IoT zbierają tak dużo danych ile się da!

Figura 1: *Obszary rozwoju Internetu Rzeczy (World Scientific News 41 (2016)*

1. Bezpieczeństwo kryptograficzne

Zgodnie z zasadą Kerchoffsa bezpieczeństwo kryptograficzne nie powinno zależeć od stosowanych algorytmów, jedynie klucze powinny pozostać niejawne. Reguła Shannona mówi, że przeciwnik zna system.

Podstawowymi cechami bezpieczeństwa kryptograficznego są:

- **Poufność** jej istotą jest ochrona transmitowanych danych przed nieuprawnionym odczytem.
- **Uwierzytelnianie stron** - wiąże się z kontrolą dostępu do systemu i przyznawaniem uprawnień.

  W przypadku dodawania nowych elementów do systemu, uwierzytelnianie pozwala wykryć próby nieuprawnionego dostępu, co jest szczególnie istotne w przypadku sieci o dynamicznej strukturze.
- **Uwierzytelnianie danych** pozwala ustalić poprawność i prawdziwość informacji dzięki połączeniu pomiędzy informacją a jej dostawcą (źródłem). Pozwala to w łatwy sposób potwierdzić poprawność i prawdziwość danych.
- **Integralność danych** oznacza ochronę transmitowanej informacji przed modyfikacją i dostarcza narzędzi do wykrycia modyfikacji.

Wymagania dotyczące bezpieczeństwa kryptograficznego IoT do powyższych cech dodają jeszcze dostępność, rozumianą jako poprawność działania usług sieciowych i łatwy dostęp do sieci.

Ataki na system dzielą się na:

- ataki aktywne, które wiążą się z dostępem do systemu (przejęciem węzła),
- ataki pasywne, które polegają na analizie przechwyconych informacji o systemie.

Nieskomplikowana budowa sieci IoT oraz ograniczone zasoby węzłów czynią je wyjątkowo podatnymi na różne rodzaje ataków.

2. Urządzenia IoT - cechy szczególne

Specyficzne cechy urządzeń IoT, które należy brać pod uwagę w kontekście bezpieczeństwa kryptograficznego to:

- ograniczone zasoby po stronie sensorowej: niewielkie moduły czujnikowe mają ograniczone możliwości obliczeniowe i komunikacyjne.
- ze względu na mobilność stosowane jest zasilanie bateryjne (lub za pomocą układów pozyskujących energię z otoczenia), co dodatkowo ogranicza wybór potencjalnych rozwiązań.
- ograniczony poziom niezawodności: ze względu na ww. ograniczenia sieci IoT nie mogą zapewniać takiej samej jakości transmisji jak bezprzewodowe sieci telekomunikacyjne ogólnego przeznaczenia.
- komunikacja bezprzewodowa: bezprzewodowe sieci czujnikowe wykorzystują otwarte kanały do komunikacji, co ułatwia przechwycenie czy wstrzykiwanie pakietów. Analizując zagrożenia trzeba więc brać pod uwagę zarówno ataki pasywne jak i aktywne.
- dynamiczne topologie: duża liczba urządzeń w sieci i możliwość dodawania/usuwania elementów sprawiają, że IoT jest szczególnie podatny na ataki. Z tego powodu stosowane rozwiązania muszą również być skalowalne.

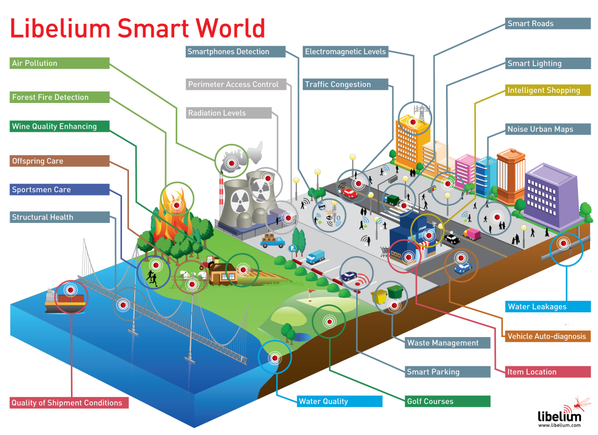
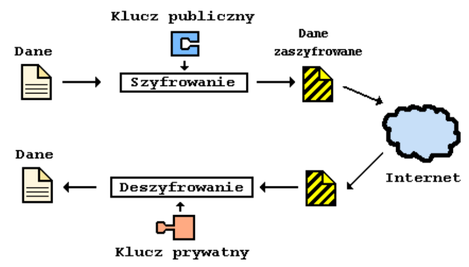


Figura 2: *Zastosowania IoT w różnych obszarach działalności człowieka*

3. Kryptografia asymetryczna

W kryptografii asymetrycznej używa się zestawów dwu- lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych. *Ka.* stosuję się do wymiany informacji poprzez kanały o niskiej poufności oraz w systemach elektronicznego uwierzytelniania.



Algorytmy mające zastosowanie w kryptografii asymetrycznej wykorzystują operacje, które da się łatwo przeprowadzić w jedną stronę a bardzo trudno w drugą. Np. mnożenie jest łatwe, a faktoryzacja trudna (na czym opiera się RSA), potęgowanie modulo jest łatwe, a logarytm dyskretny jest trudny (na czym opierają się ElGamal, DSA i ECC).

W miarę wzrostu poziomu zabezpieczeń długości klucza dla obecnych metod szyfrowania opartych na RSA zwiększają się wykładniczo, natomiast długości kluczy opartych na ECC wzrastają liniowo. Przewiduje się, że ECC będzie w centrum planowania zabezpieczeń systemów IT.

Kryptografia krzywych eliptycznych (ECC) w praktyce jest stosowana przez Bitcoin, wykorzystują ją także niektóre protokoły SSH i TLS oraz jest ona obecnie wykorzystywana w zabezpieczeniach austriackiej karty obywatelskiej oraz w podpisach cyfrowych.

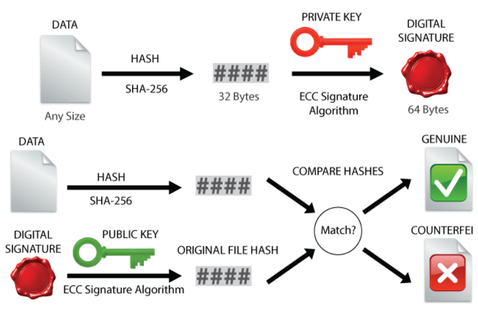


Figura 4: *Elliptic Curve Digital Signature Algorithm (ECDSA) oferuję weryfikację oryginalności danych.*

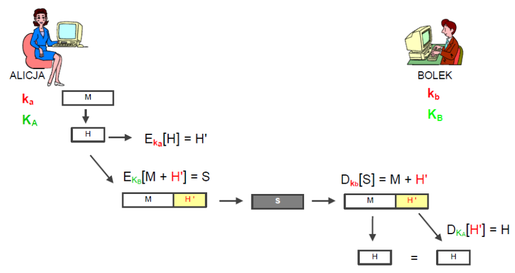


Figura 5: *Przykład algorytmu gwarantującego poufność, autentyczność i nienaruszalność danych.*

Wyzwanie: tanio, bezpiecznie i uniwersalnie...

Literatura

1. **J. P. Olszyna** - *Analiza i projektowanie układów kryptograficznych przeznaczonych do sieci czujnikowych*, Politechnika Warszawska 2013
2. **P. Gaona-García, C. Montenegro-Marin, J. D. Prieto, Y. V. Nieto** - *Analysis of Security Mechanisms Based on Clusters IoT Environments* - Special Issue on Advances and Applications in the Internet of Things and Cloud Computing, 2016.
3. **P. Nandhini, V.Vanitha** - *A Study of Lightweight Cryptographic Algorithms for IoT*, IJIACS v6, 1/2017
4. **S. Gajbhiye, S. Karmakar, M. Sharma** - *Study of Finite Field over Elliptic Curve: Arithmetic Means*, International Journal of Computer Applications, v 47,17/2012
5. **J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow** - *Elliptic Curve Cryptography in Practice*, Financial Cryptography and Data Security, Springer 2014, pp 157-175
6. **T. Nandhini, M. S. Parveen, B. Kalpana** - *A Survey on Internet of Things Architecture*, WSN 41 (2016) p. 159-166
7. www.libelium.com