REZUMAT

Lucrarea explorează tehnicile de dezvoltare a nodurilor Internet of Things cu grad sporit de securitate . Sunt prezentate tendințele actuale în această directie precum si principalele caracteristici ale TPM.

Pentru implementarea proiectului am ales utilizarea unui TPM(eng.Trusted Platform Module) pus în legatură cu R-PI(eng.Raspberry Pi)

O platformă poate fi orice dispozitiv de calcul, spre exemplu , un calculator , server , telefon mobil , sau orice alt aparat capabil să comunice cu un alt dispozitiv pe când o "platformă de încredere" este una ce conține un subsistem hardware cu rolul de a menține siguranța și securitatea între mașini.

Standardul industrial în ceea ce priveste TPM(eng.Trusted Platform Module) este susținut de o gamă largă de companii printre care: HP, Compaq, IBM ,Intel ,Infineon ,și multe altele , toate împreună formând Trusted Computing Platform Aliance (TCPA).Problema pe care au ridicat-o cei de la TCPA este că într-o societate cu informație modernă resursele calculatorului au devenit , tot mai mult , globale și accesibile pentru oricine.Așadar TPM-urile nu joacă doar un rol de dispozitive de calcul ci și de dispozitive de conectare între mașini . Astfel atât utilizatorii locali cât și cei conectați la distanță pot beneficia de o siguranță îmbunătățită și încredere atunci când folosesc sau comunică cu o altă platformă.Există diverse tehnologii pentru securitate cum ar fi identificarea utilizatorului , mecanisme de control al accesului , procesor criptat sau sisteme de operare cu diferite servicii de securitate ce sunt folositoare în general dar nu îndeajuns pentru a asigura siguranța și încrederea necesară.Pentru a completa aceste neajunsuri au fost introduse TPM-urile.

Cea mai importantă proprietate a TPM este aceea că secretele sunt indirect protejate de acestea întrucât un mesaj poate fi trimis de pe o platformă la o alta platforma software numai după ce ,starea platformelor a fost măsurată și raportată.Secretele stocate pot fi eliberate numai după ce platforma a fost verificată.Raportarea , stocarea și regăsirea datelor este efectuată de TCPA(Trusted Computing Platform Alliance) ce reprezintă o serie de platforme ce cuprind toate procesele software.Astfel dacă un proces se bazează pe folosirea de secrete nu poate opera până când nu se stabilește dacă mediul în care se desfășoară este corect.

Ca resursă hardware am utilizat Raspberry Pi întrucat aveam nevoie de un mediu Linux în care să pot folosi openSSL – mecanism criptografic ce sprijină autentificarea pe servere web.

În concluzie proiectul își propune explorarea comenzilor openSSL pentru realizarea principalelor operațiuni criptografice și anume:

→ criptarea simetrică
→ criptarea cu cheie publică
→ semnături digitale
→ funcții hash