Soluții de securizare pentru sisteme informatice medicale

Vlad Micu

Rezumat

Pacienții unui spital au nevoie de o monitorizare a parametrilor vitali, atât în perioada de spitalizare, cât și în perioada imediat următoare, la domiciliu. În faza post-operatorie a unui pacient, medicii trebuie sa afle rapid dacă starea acestuia s-a schimbat și să ia o decizie pe baza datelor furnizate de către senzori.

Sistemele de monitorizare la distanță oferă date precise și în timp util, însă, în anumite cazuri, pot beneficia de pe urma unor componenete de securitate robuste. Aceste sisteme pot implica transmiterea printr-o rețea a unor informații confidențiale, cum ar fi datele personale ale pacienților, diagnosticele acestora, rețete medicale și date de monitorizare. În absența unui modul de securitate, aceste informații pot fi ușor interceptate sau accesate de persoane neautorizate.

Cazul cel mai sensibil îl reprezintă monitorizarea pacientului la domiciliu. Persoanele în vârstă, persoanele cu dizabilități sau afecțiuni cardiace pot duce o viață mai liniștită dacă starea acestora este supravegheată de către medici, la distanță. De asemenea, perioada de spitalizare a pacienților ar putea fi diminuată. După urmarea unui tratament sau efectuarea unei operații, pacientul poate fi monitorizat la domiciliu încă din primele zile, dacă starea acestuia de sănătate permite acest lucru. În acest caz, procesul de monitorizare va implica o transmitere de date prin rețele externe, nesigure. Datele vor circula atât în rețeaua de la domiciliu, cât și spre unitatea medicală ce are sub îngrijire acel pacient. Astfel, apare problema unei transmiteri a datelor confidențiale și a unei autentificări sigure a entităților din sistem.

Documentul de față prezintă o astfel de soluție, ce cuprinde metode sigure de autentificare, autorizare și gestionare a identităților. Modulul de autentificare se bazează pe protocolul de autentificare Kerberos și protocolul criptografic SSL. Autorizarea este realizată atât prin intermediul sistemului de gestionare al identităților – LDAP – cât și prin intermediul operațiilor de genul „cerere – aprobare”.

Securizarea transmisiei datelor este un punct foarte important, ce asigură menținerea confidențialității acestora. Protocolul SSL asigură o transmisie sigură și integrală a datelor, printr-o criptografie puternică. Odată colectate, datele trebuie stocate într-o bază de date. Pentru a nu putea fi citite de un atacator, datele trebuie stocate sub formă criptată.

Comunicația este realizată sub o arhitectură REST. Această arhitectură oferă o mapare intuitivă a resurselor și o flexibilitate în ceea ce privește comunicarea între tipuri diferite de dispozitive.