Home Telemedicine: Encryption is Not Enough

M. Salajegheh, A. Molina, and K. Fu
University of Massachusetts, Amherst, USA

Implantable medical devices and home monitors make use of wireless radio communication for both therapeutic functions and remote monitoring of patients' vital signs. While our past work showed that lack of cryptographic protection results in disclosure of private medical data and manipulation of therapies (Halperin et al., IEEE S&P, 2008) our present work shows that even using encryption is insufficient to protect the confidentiality of patient telemetry. Our experiment analyzes the security of data traffic patterns of two sets of real medical telemetry: a corpus from PhysioNet (an online biomedical research database) and a network trace of a live disaster drill using Harvard's CodeBlue medical sensor network (Chen et al., DCOSS, 2008). Our work shows that even if a wireless medical device uses encryption, patient data can leak to unauthorized parties who need not be near the patient. Our measurements show that data packet timing information and headers distinguish the types of medical and monitoring devices even if traditional cryptographic mechanisms are used. Furthermore, the highly repetitive nature of medical data, such as ECG or respiration signals, leads to additional privacy vulnerabilities that cannot be easily mitigated by means of encryption without significant modification. Data compression technology further exposes encrypted telemetry to cryptanalysis. The information leakage of telemetry could facilitate unauthorized tracking of a patient because an ECG is known to uniquely identify a person in a predetermined group (Biel et al., IEEE I&M, 2002). Moreover, our study shows that data packet padding, encryption, authentication, and other common defenses against security threats require significant energy, storage, and computation that impose on the already scarce battery and space resources. Two of our experiments show how to automatically recover data from encrypted telemetry using Bayesian classifiers. In one experiment, we encrypted an ECG signal. By observing only the length of the digitally encrypted data, we were able to reconstruct sufficient information about the original ECG data that we determined the patient's heart rate. Using similar techniques, we recovered a leaked respiration signal that visually matches the original signal. Our findings show the weakness of using common cryptographic techniques on highly periodic and often compressed medical telemetry. Our work further discusses techniques to mitigate these security and privacy risks in wireless medical telemetry systems. However, all known techniques require extra energy, computation, and bandwidth from the medical device. The lesson learned is that encryption is not enough to protect the privacy of medical telemetry, and that reasonable assurance for security and privacy will require an energy budget. Future design of medical devices will have to make difficult tradeoffs between battery life versus security and privacy. This work was supported by NSF grants CNS-0627529, CNS-0716386, and CNS-0831244.

The Therapress 1600i: Accelerating Knee Rehabilitation

A. Geronimo, M. Holyoak, M. Oliver, E. Scherm, and M. Paliwal
The College of New Jersey, Ewing, NJ USA

Objective: To design a 'smart' leg press machine that improves upon current rehabilitative practices for degenerative knee disorders such as osteoarthritis as well as injury induced knee pathologies. As its design entails, the machine provides rehabilitative assistance through strength training of upper leg muscles, with focus on the vastus medialis and vastus lateralis of the quadriceps group. The Therapress is designed to further improve the rate and quality of joint rehabilitation. The TP1600i is unique to current physical therapy practices because it incorporates three documented and proven strategies to combat quadriceps weakness: strength training, electrotherapy, and biofeedback [1,2]. The machine is designed to aid the user in regaining lost quadriceps strength, a condition indicative of poor knee health [3]. The machine incorporates a novel package of biofeedback, automated continuous variable resistance, and progress assessment, while maintaining subject specificity. The Therapress system utilizes a LabVIEW interface, which acquires and processes physiological signals recorded from the subject, as well as serves as a controller for output. These signals include surface electromyography (EMG) of the quadriceps, reaction forces at the foot (an indirect measurement of exercise resistance), and knee range of motion (ROM). Additionally, the subject is outfitted with stimulatory electrodes which function to characterize muscle recruitment using the Central Activation Ratio (CAR), as well as to therapeutically excite the muscle and induce accelerated hypertrophy [4]. Automated continuous variable resistance is achieved through a resistive hydraulic cylinder, which utilizes a servo motor to change the orifice size of partially overlapping valves during and between exercise sets. The resistance is adjusted based on user input of exertion and pain levels into the LabVIEW interface. The footplate of the machine houses four force sensing units to measure the resistance offered by the cylinder. A biofeedback arm attached to the system provides the subject with real-time data of their performance, including integrated EMG activity, ROM, and force production. Inclusion of biofeedback in quadriceps exercise regimens has been shown to increase strength gain [2]. The design allows the user to be in control of the exercise intensity at all times, while the machine works to maximize the efficacy of the protocol. The TP1600i is designed as a cost effective and time efficient alternative for the rehabilitation of debilitating knee disorders in a physical therapy protocol, and its ease of operation may qualify it for home use as well.