Mitigating Solutions in Insulin Pump System Security

Nathanael Paul, PhD; Brent Lagesse, PhD

Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA
paulnr@ornl.gov

Objective:
Insulin pump systems are now the preferred method of treatment for type 1 diabetes patients. New features of insulin pump systems continue to add convenience and better treatment, including remote programming and continuous blood glucose management. Unfortunately, these new insulin pump features present new vulnerabilities that can result in an unsafe insulin pump system. Our objective is to help create a secure insulin pump system platform that withstands targeted malicious attacks against an insulin pump system.

Method:
The main threats of an insulin pump system can be broken into two parts: monitoring and control. By changing monitored information (e.g., blood glucose values), a patient might use incorrect information to program the insulin pump system. In control, an attacker can transmit commands using an unauthorized device. By analyzing these different components, we can better understand the potential vulnerabilities and build secure insulin pump system architectures.

Result:
In February 2010, we implemented a remote attack on a commercially deployed insulin pump system where we remotely programmed an insulin pump system using an unauthorized device, and we were able to do this attack from 100 ft. away. Since that time, we have continued to identify ways that a malicious attacker could potentially affect a patient's health. We plan to present mitigations against these and similar attacks at the workshop.

Conclusion:
Insulin pump system threats and vulnerabilities exist. Attackers can and will take advantage of insulin pump insecurity. An attacker who is able to influence the insulin pump system presents a very real risk to a patient. Based on our findings, we recommend implementing both new security protocols and securing insulin pump system architectures to protect against these attacks.