Master Project “Security of Embedded Medical Devices”

INTRODUCTION

Embedded medical devices play a large role in healthcare, e.g. in the form of patient monitors, insulin pumps and pacemakers. Traditionally such embedded devices operated standalone and were built on proprietary closed platforms, but there is a shift towards networked devices and adoption of open platforms, e.g. based on Linux.

With above developments also the importance of security increases, because devices become more vulnerable for attackers that may threaten patient safety and/or privacy. This is also confirmed in recent events by vulnerabilities found in embedded medical devices like pacemakers and insulin pumps. Examples of such vulnerabilities include remote buffer overflows and denial of service attacks.

The medical device industry – including Philips – is tasked to ensure that their devices are implemented securely. This requires the various layers of implementation to be considered, e.g. from applications to operating system, and involves strengthening security across the software development lifecycle touching on implementation architecture, security functionality, coding practices, etc.

This project will focus on one of our embedded Linux-based platforms. Based on a combination of hands-on analysis and desk research, the objective is to come up with countermeasures and architectural recommendations to improve its security and that of future generations of embedded medical devices.

ASSIGNMENT

The assignment is to assess the security of a Linux-based embedded medical device platform and contribute to improving its security. Possible steps include 1) creating an overview of most significant vulnerabilities for this kind of platform, 2) performing a hands-on evaluation of devices and source code by applying relevant methods (e.g. pentesting) and tools, and 3) proposing countermeasures and recommendations for architecture and implementation practices to improve the platform’s security.

PROFILE

Candidates are expected to have a background in computer science / security. A candidate has knowledge of common security vulnerabilities and preferably some experience in (hands-on) security implementation, security evaluation and/or ethical hacking.

CONTACT

For more information or to apply contact:

Paul Koster, Philips Research
r.p.koster@philips.com / +31 6 11764742
http://www.research.philips.com