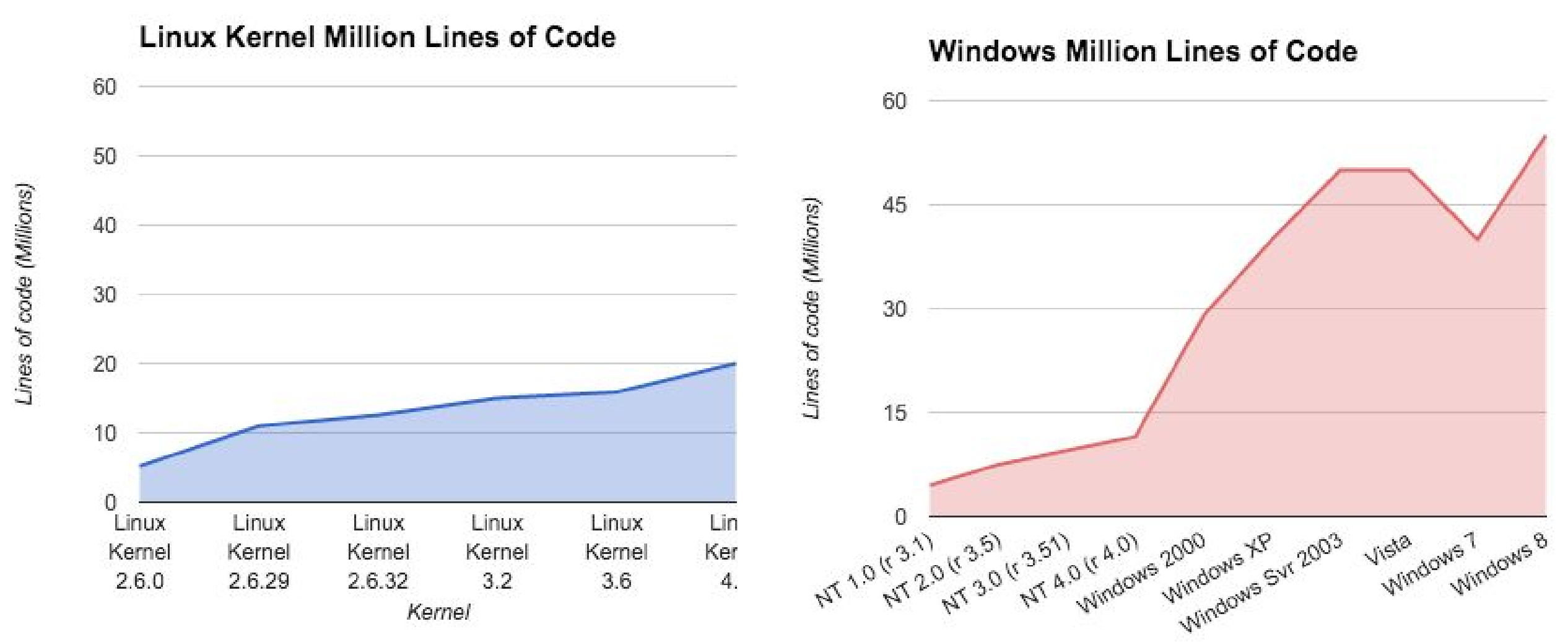
Noninvasive Postmarket Security Monitoring for Medical Devices

Benjamin Ransford, Ph.D., Denis Foo Kune, Ph.D., Ann Gookin, Andrew DeOrio, Ph.D.

Virta Laboratories, Inc.

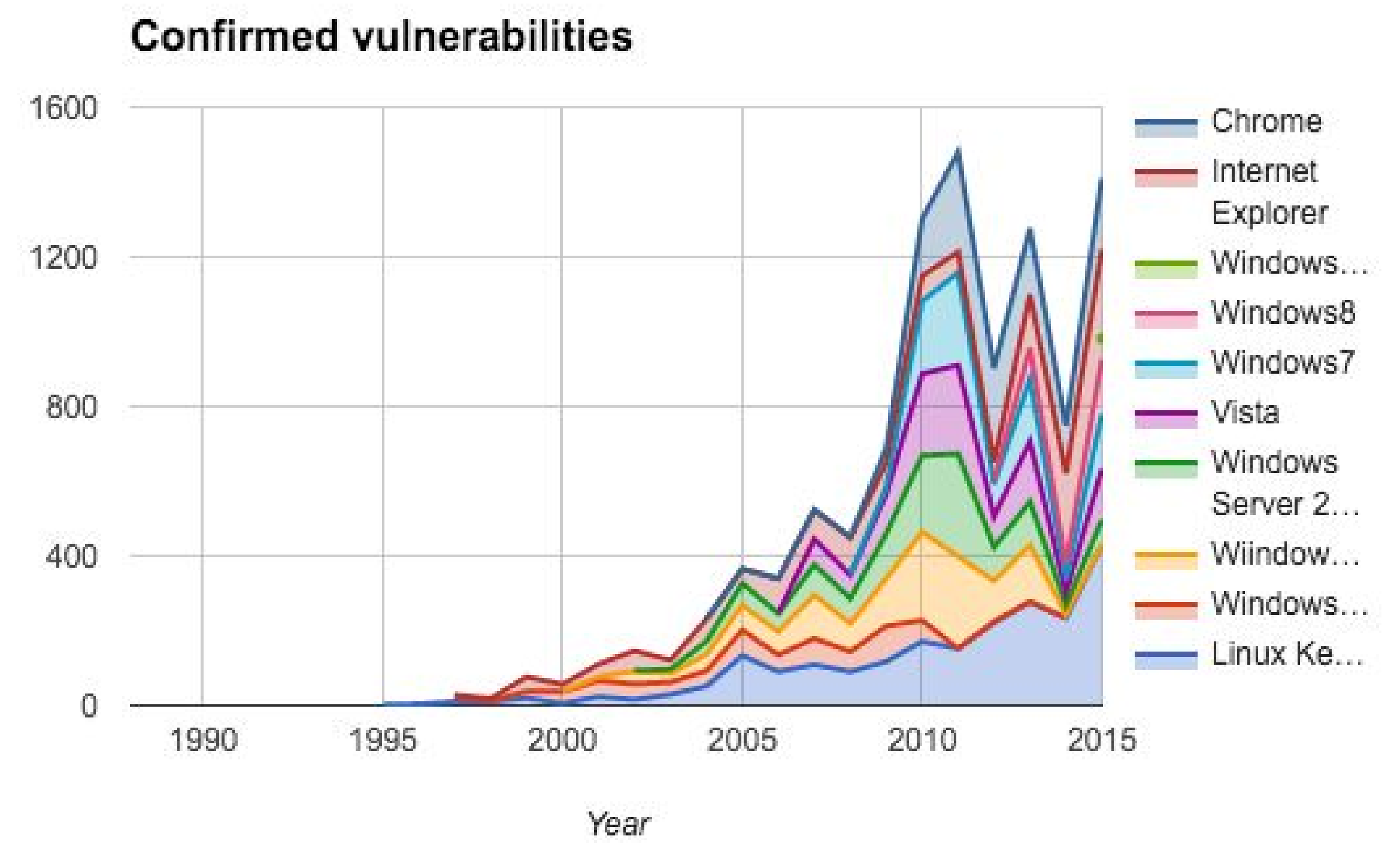
Introduction

Software has become extremely complex. The core operating systems alone (Linux Kernel and Windows) have reached well over 10 million lines of code. Running on top of the operating systems are device drivers and applications that significantly increase the overall complexity of the system.



Data source: The Linux Foundation [1] and Vincent Maraia [2], *"The Build Master: Microsoft's Software Configuration Management Best Practices"*

As system complexity grows, the number of software bugs grows as well. A portion of those bugs manifest as security vulnerabilities.

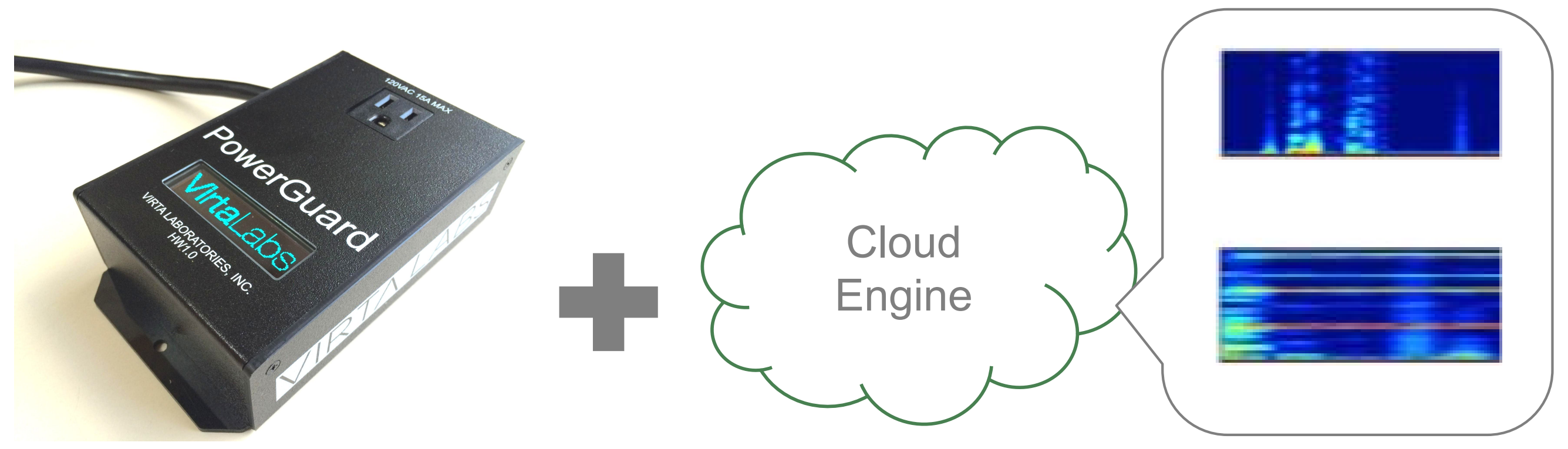


Data source: The National Institute of Standards and Technology, National Vulnerability Database [3].

With the fundamental tension between protecting the ever changing attack surface and minimizing the impact on running software in their current fleet, healthcare delivery organizations and manufacturers are faced with a challenging tradeoff. The system we have developed allows monitoring without the downside of modification.

Methods

Noninvasive postmarket monitoring fulfills requirements of continuous security assessment without modifying the device or interrupting the clinician's workflow. We can monitor electrical power consumption, and the devices on the network. The central analytics framework is offloaded to a cloud service for improved scalability.



Our measurement apparatus sits on the AC outlet at the wall and measures signals coming from the processing unit or electromechanical actuators. It detects deviations from normal software execution or departures from expected system behavior. The processing and data-heavy machine learning modules run on a remote cloud server.

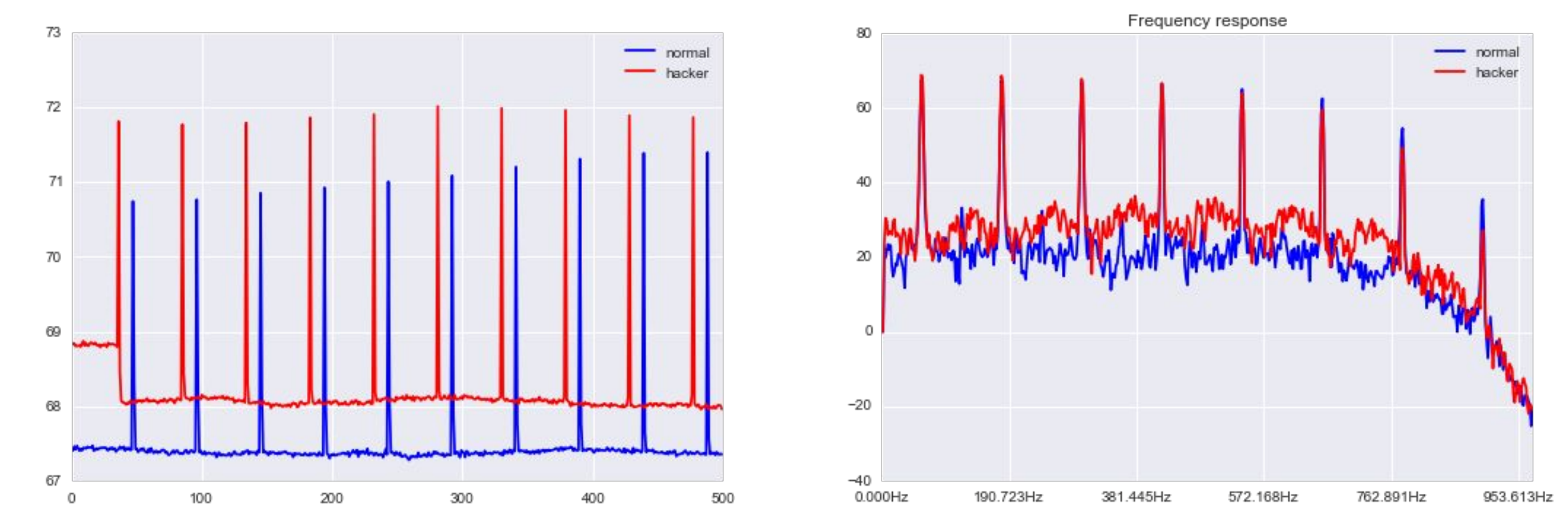
The monitoring system based on work by Clark et al. [4] uses a Hall Effect sensor on the AC power line to non-intrusively monitor the power consumption of the device under test. The high-precision readings are forwarded to a cloud-based analytics system. We investigated large-volume and syringe-type infusion pumps for abnormal infusion rates. We also investigated network-based intrusions and measured our ability to detect abnormal infusion rates and unexpected software execution.

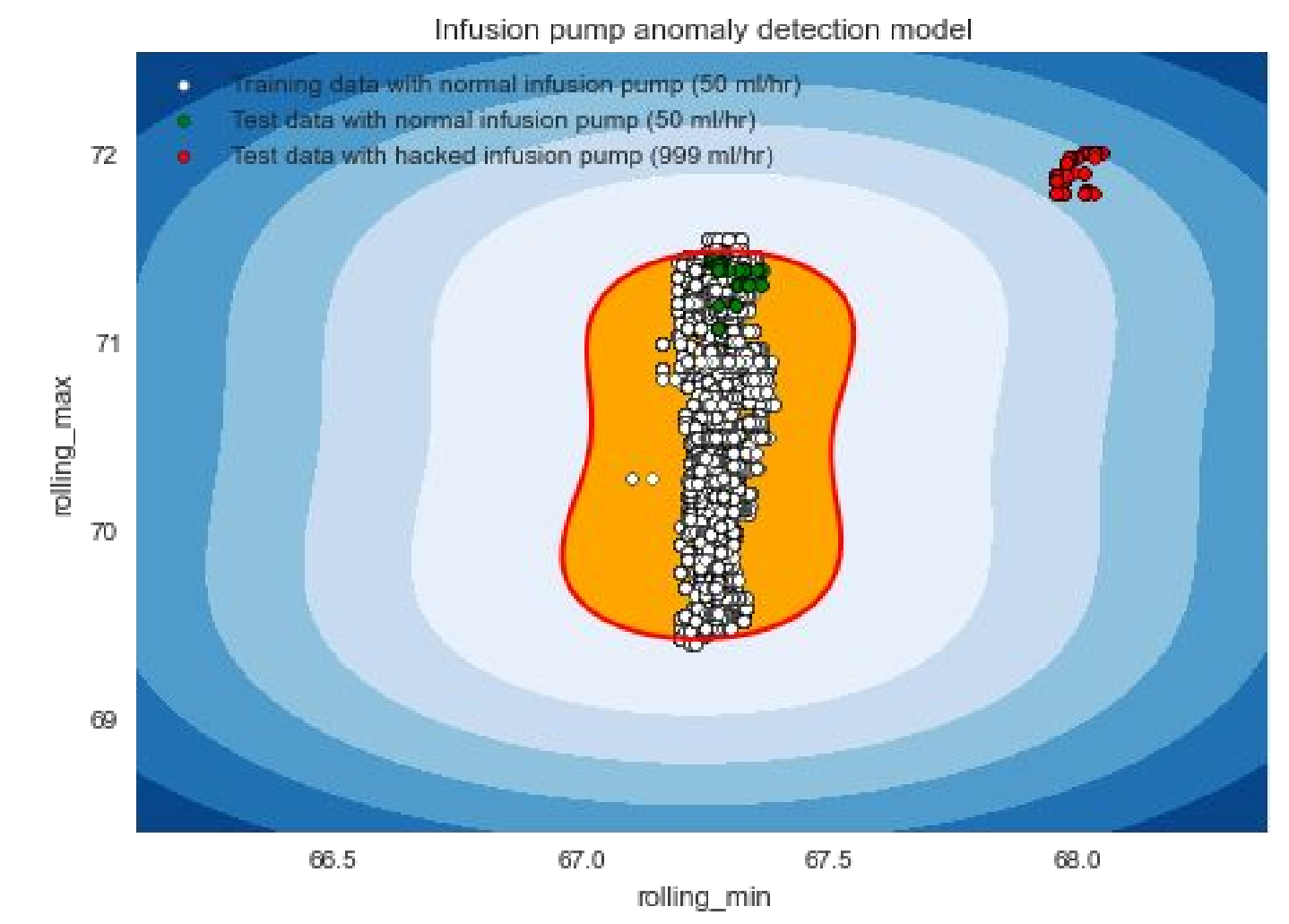
Device connected to AC monitoring system

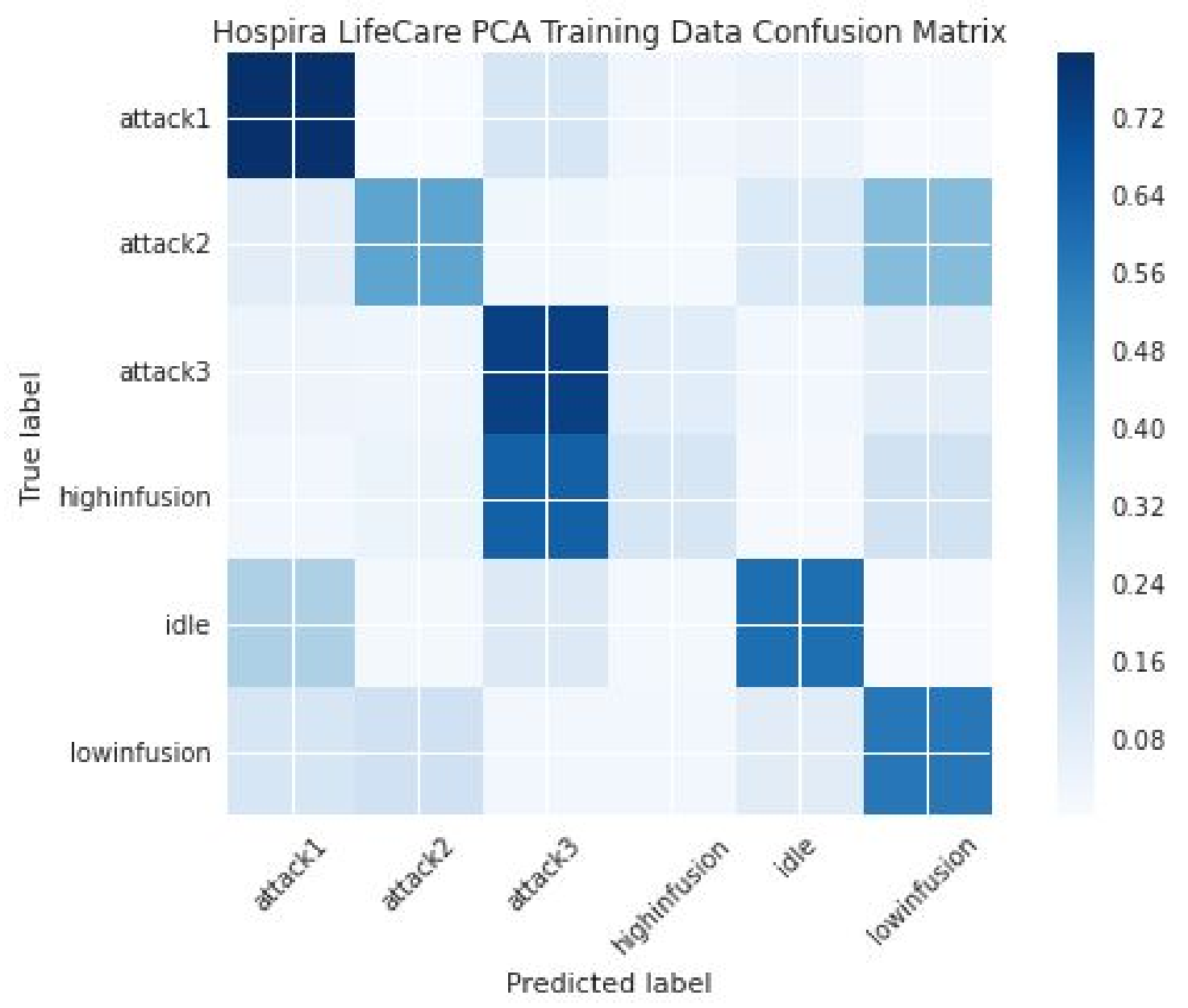
Results

By analyzing only the alternating current (AC) power consumption at the wall outlet, we were able to train a machine learning module on normal and attack scenarios. We could detect cyber-physical intrusions leading to overdosage of drugs on large-volume and syringe-type infusion pumps. The **precision and recall were over 95%** for both types of pumps.

Detecting cyber-physical attacks via AC Power Analysis





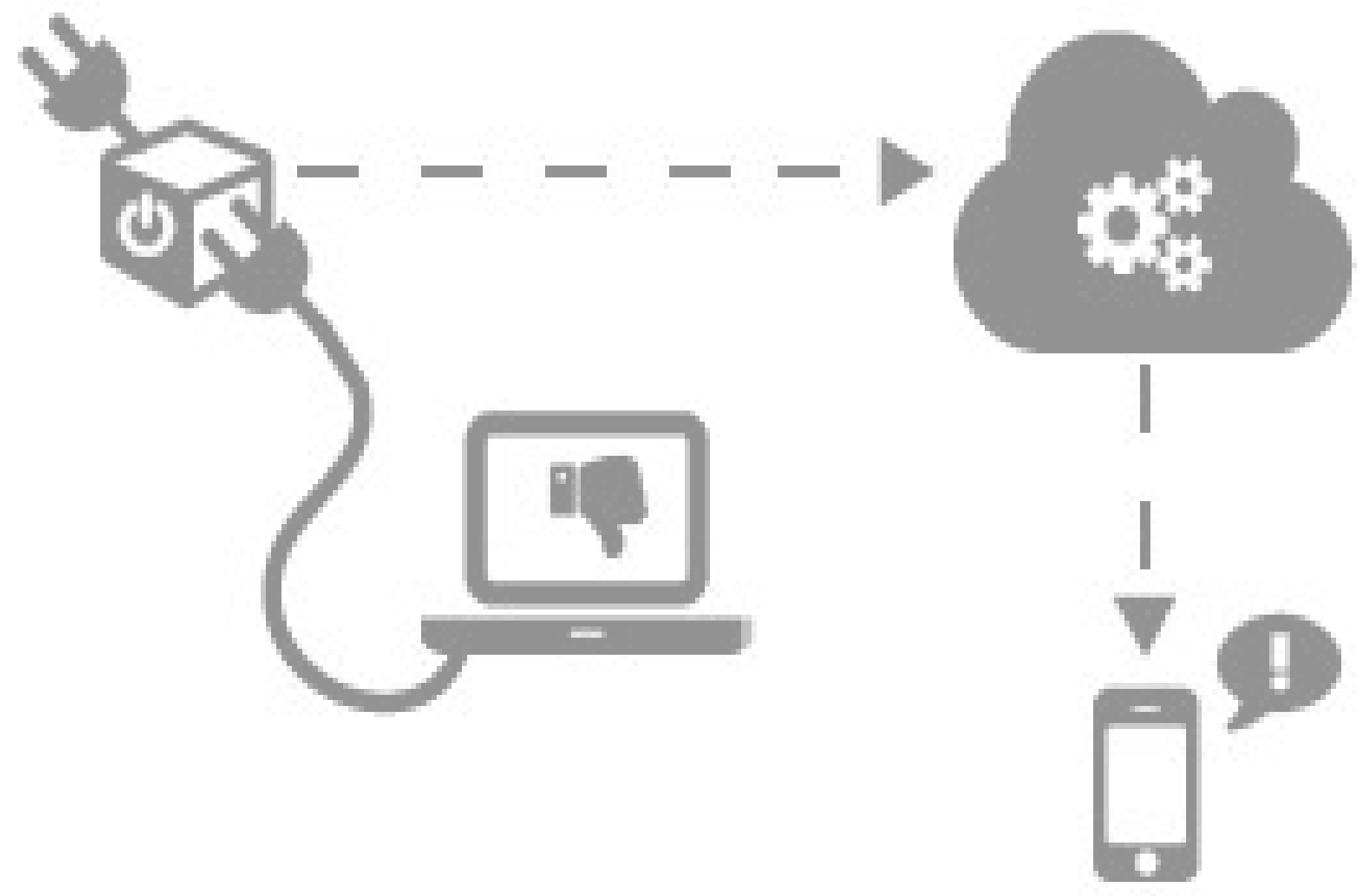


We extended the technique to detect network-based intrusions that do not change actuations. With the features being more subtle, the precision and recall drop to 70% in our initial experiments. Detection of attacks without causing actuation was still possible as indicated by the confusion matrix to the left.

Conclusions

Our results demonstrate that commercially available infusion pumps' patterns of AC power consumption are correlated with their infusion rates, suggesting that monitoring power at fine granularity is a potentially viable approach to postmarket security maintenance for these medical devices. We are also able to detect abnormal software execution with an attacker doing a complete compromise of the pump, while the pump was operating.

Postmarket strategies constitute a critical component of **defense in depth** to decrease the attack surface of healthcare delivery organizations with a wide variety of software. To further improve the visibility of postmarket devices, healthcare delivery organizations can schedule periodic network scans to discover vulnerabilities and misconfigurations on their networks. If done safely, those scans can offer a good complement to the monitoring system discussed.



Bibliography

1. The Linux Foundation, http://www.linuxfoundation.org/, Accessed April 2016
2. Vincent Maraia. 2005. "The Build Master: Microsoft's Software Configuration Management Best Practices." Addison-Wesley Professional.
3. U.S. National Institute of Standards and Technology, "National Vulnerability Database," 2016, https://nvd.nist.gov. Accessed April 2016
4. Clark, S. S., Ransford, B., Rahmati, A., Guineau, S., Sorber, J., Fu, K., Xu, W., 2013 "WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices." USENIX Workshop on Health Information Technologies, August 2013.

Acknowledgement

This material is based upon work supported by the National Science Foundation under the SBIR Grant No. 1448440.