6-25-2016

Demo: Wanda, Securely Introducing Mobile Devices

Timothy J. Pierson
Dartmouth College

Xiaohui Liang
Dartmouth College

Ronald Peterson
Dartmouth College

David Kotz
Dartmouth College

Demo: Wanda, Securely Introducing Mobile Devices

Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, David Kotz
Department of Computer Science, Dartmouth College
Hanover, New Hampshire, USA
{tjp,xiaohui.liang,rapjr,kotz}@cs.dartmouth.edu

ABSTRACT

Nearly every setting is increasingly populated with wireless and mobile devices – whether appliances in a home, medical devices in a health clinic, sensors in an industrial setting, or devices in an office or school. There are three fundamental operations when bringing a new device into any of these settings: (1) to configure the device to join the wireless local-area network, (2) to partner the device with other nearby devices so they can work together, and (3) to configure the device so it connects to the relevant individual or organizational account in the cloud. The challenge is to accomplish all three goals *simply*, securely, and consistent with user intent. We developed Wanda – a 'magic wand' that accomplishes all three of the above goals – and will demonstrate a prototype implementation.

1. INTRODUCTION

Some predict the Internet of Things (IoT) will make billions of everyday objects "smart" by adding wireless communication capabilities. The dream is that networks of these newly connection-enabled devices will give us greater insight into the behavior of complex systems than previously possible. The reality, however, is that configuring and managing billions of devices will be difficult.

The first major challenge in configuring a new IoT device is to connect it to the local-area network. We expect few IoT sensors, at least those for home, business, or clinical use, will not come with cellular or other long-range connections to the Internet; they will have lower-power short-range radios such as Wi-Fi. And yet, people still find it challenging to connect new devices – particularly those with no keyboard or display! – to secure Wi-Fi networks.

We will demonstrate **Wanda** [1], our approach to enabling everyday people to easily (and securely) associate Wi-Fi devices with their home or office Wi-Fi network. Wanda uses a small hardware device called the 'Wand' that has two antennas separated by one-half wavelength and uses radio strength as a communication channel to simply, securely, and consistent with user intent, impart information onto devices. (See Figure 1.) Our initial focus has been on connecting devices, but the Wand could be used to impart *any* type of information onto a nearby device. Wanda is more than just a solution for pairing devices or connecting to access points.

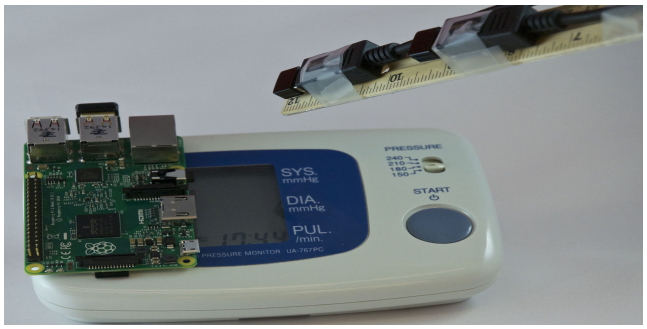

Figure 1: Wanda prototype used with a commercial blood-pressure device, extended to support Wi-Fi and Wanda. Some cables removed for clarity.

Unlike many other approaches, Wanda does not require any specialized hardware (or any hardware changes) in the new devices, does not require any pre-shared secrets, and does not require complex algorithms or complicated cryptography libraries. Furthermore, Wanda does not require the devices to be adjacent, or even movable – useful for large appliances as well as small mobile devices.

Wanda is a novel approach for imparting information onto a target device, even though the target device has never been seen before, nor have any secrets been pre-shared. Wanda makes four **contributions**:

1. a consistent, fast, easy, and secure method to impart any kind of information onto commodity wireless devices, regardless of device type or manufacturer, without hardware modifications to the device;
2. protocols for imparting information onto new devices (such as a Wi-Fi SSID and password), introducing two devices so they can establish a secure and user-intended connection, and imparting cloud identity and credentials into a new device;
3. a prototype implementation and experimental evaluation; and
4. a security analysis of the system.

2. ACKNOWLEDGEMENTS

This research is supported by NSF award number CNS-1329686. The views and conclusions in this document are those of the authors and may not necessarily represent the official policies of NSF.

3. REFERENCES

[1] T. J. Pierson, X. Liang, R. Peterson, and D. Kotz. Wanda: securely introducing mobile devices. In *IEEE International Conference on Computer Communications (INFOCOM)*, April 2016.

MobiSys '16 Companion, June 25–30, 2016, Singapore.

ACM ISBN 978-1-4503-4416-6/16/06..

DOI: http://dx.doi.org/10.1145/2938559.2938581