Bluetooth Wireless Privacy

Robert H. Warren
David R Cheriton School of Computer Science,
University of Waterloo
rhwarren@uwaterloo.ca

Gregory M. Zaverucha
David R. Cheriton School of Computer Science, University of Waterloo
gzaveruc@uwaterloo.ca

Abstract

In this poster we investigate privacy issues of portable devices using the Bluetooth wireless communication standard. Existing safeguards in some devices do little to protect the owners' privacy. Many do not protect against hotlisting, tracking and profiling attacks. We present empirical data on the weakness of Bluetooth wireless devices to this class of attacks as collected from a number of different devices. We find that wireless devices are easily tracked with low-cost attacks. The resulting information can be used for profiling individuals and groups according to behavior patterns.

Dataset creation

In order to gain a better understanding of the privacy issues involved, we constructed an experiment where a Bluetooth access point was placed near a doorway of a corridor. The access point continuously broadcasted discovery requests over the next 3 months to nearby Bluetooth devices. Whenever a device would come into range of the access point, its name and capabilities would be recorded as well as the time and date of the observation.

While the name of a Bluetooth device can and is often changed by users for privacy or vanity reasons, the devices have a unique hardware address identifier. Using this address as a identifier enabled us to track the devices and individuals even when they changed their device names over a period of time.

This approach is known to under report the number of Bluetooth devices since the owner of the device must set his devices to a discoverable mode in order for it to answer to requests. However, we felt that other, more aggressive, methods of data collection would be inappropriate and invasive. Therefore this research presents a lower bound of the type and amount of information that is potentially being leaked by Bluetooth devices.

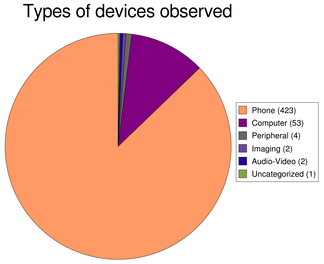
Information Available

Bluetooth devices volunteer the following information to anyone who asks, including **btscanner.** , a free software package designed to extract information from Bluetooth devices, without connecting to them.

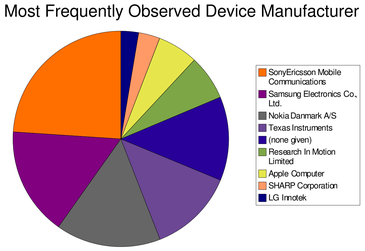
- Unique hardware address (MAC)
- Organizationally Unique Identifier (company that made the device)
- Name (set by the device owner, e.g. “Greg's phone”)
- Class of device (Phone, computer, headset ...)
- Services supported (networking, object transfer, telephony...)
- Manufacturer
- HCI version and features (Host Controller Interface)

Device Types

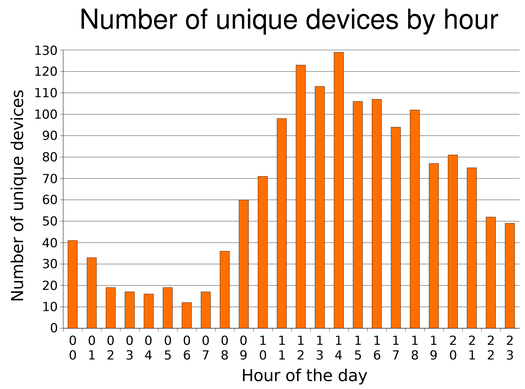
Types of devices observed



Most Frequently Observed Device Manufacturer



Activity by Time

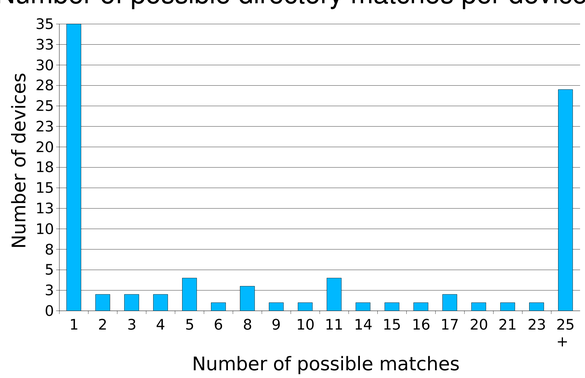


Linking Owners

We attempted to identify the owners of the devices by making the assumption that they were a part of the University population and not one time visitors. By this assumption, their personal details would be part of the online University directory (uwdir). We searched uwdir for whatever string was reported by the devices. After a careful human review of the results, we plotted a graph of the number of individuals that a particular device could be be assigned to. As uwdir has a built-in limit of 25 results per query, strings that matched more than 25 hits are lumped into their own category.

What we found interesting about the use of this method is that in many cases, people make use of nicknames for privacy or vanity reasons. However, they tend to make repeated use of the same nicknames across databases, nullifying any privacy advantage that this behavior could provide. Hence, where someone may have labeled his cellphone as belonging to 'greatguy43', he will also have marked his University directory entry with the nick names 'greatguy43'. In some cases, this information enabled us to link devices to their owners even when no name was provided.

Number of possible directory matches per device



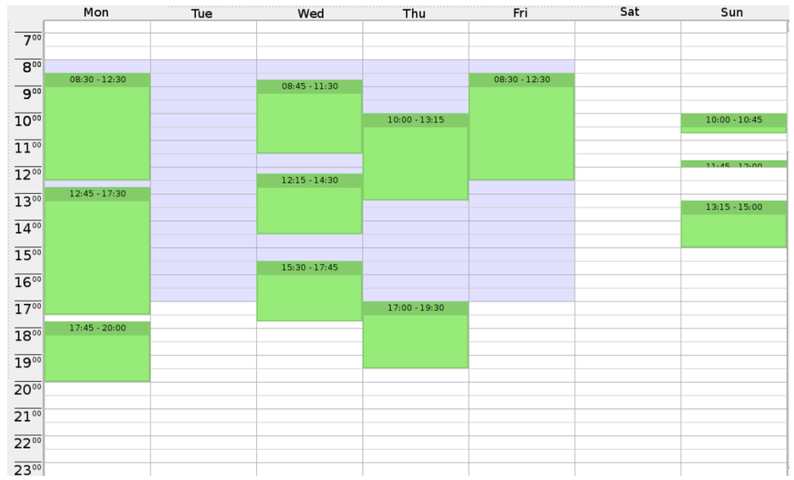
Tracking

Since every device has a unique identifier, tracking is not difficult. Using the time and date in the logs kept by **btscanner** each time a device is seen, we can track when a device is near an access point. When the device is a mobile phone kept in the owner's pocket, we effectively track the owner of the device.

If the person walks past the scanner to enter/exit the building we can we can (heuristically) know what hours they are in the building (see example below). Over time, a profile can be constructed. Multiple access points and integration with CCTV systems can significantly increase the amount and quality of tracking data (with a modest budget and slightly more effort).

Tracking Example

To illustrate that tracking a device is feasible using a single access point we reconstruct a schedule from the logs of the device. Log entries were paired up as (time in, time out) for a given week. For privacy reasons, we *did not* attempt to identify the device owner.



Conclusion & Recommendations

In this low-cost experiment, **information about 485 devices** was collected, and 35 users could be uniquely identified. **Tracking is possible**, even with a single access point as demonstrated above. Combination with other “guerrilla surveillance” techniques and additional information (such as uwdir) can greatly increase the reach of tracking and profiling attacks.

Recommendations:

- **Users**: If you have a cellphone or laptop, **disable Bluetooth** when you aren't using it

Device manufacturers:

- do not enable Bluetooth by default
- make it easy for users to enable/disable
- when enabled, restrict information to authenticated devices