Wireless Vulnerabilities

(Music)

Mobility products have significantly increased in the workplace over the last decade.

But while they have improved the efficiency and convenience of everyday work environments they have also increased the likelihood of information falling into the wrong hands.

There are several way to gain access to a wireless device.

The easiest way is to get physical access to the device.

However, there are several attack vectors that have existed for some time, including public device
hacks, rooting, or jailbreaks, which work remotely through a malicious web page or file.

Through social engineering techniques, a user can be tricked into connecting

something malicious, allowing an attacker access to the device.

The following demonstrations show attacks taken from the Internet.

The devices were broken into using publicly available
jailbreak attacks, which can attack any smart phone, tablet, or Bluetooth device.

Once a wireless device has been broken into, many different applications can be installed.

Once such application that can be installed is an SSH server.

With this installed on a device, an attacker can
gain access and control it through the Internet from anywhere.

With iOS devices, there is a known root password that is pre-installed on every device.

That known password makes it easier to access a device after it has been hacked into.

For most of these demonstrations,
we will be controlling the devices mainly through an SSH connection.

Control of the device is not just limited to control over software.

It is also possible to control the hardware of the device.

In the following demonstration, you can see how a picture can be taken with an iPhone
and then pulled back to a control computer.

This same attack can be performed on any camera-enabled phone.

The following is a demonstration of how a device can be instructed to sound like it is ringing.

Control of the device vibration is also possible.

Manipulating a text-to-voice program on a device could be used to confuse a user.

This is more relevant as people use such devices for turn-by-turn navigation while driving.

(computer voice) "Rerouting. Make next left onto main street.

Once on a device, an attacker can continue to fool
a user into potentially revealing more information.

In the following demonstration, the attacker pops up a simple message

asking the user to input their password again.

The inputted password is then transmitted back to the attacker.

Most devices, including phones, tablets, and
>Bluetooth headsets contain a microphone.

Using these devices to record the room audio is a relatively easy thing to do.

Recordings can be started based on calendar events or time,
allowing for devices to record while not connected to the Internet.

This audio can be transmitted immediately or stored for later transmission
when an Internet connection is restored, or in the middle of the night.

(recorded audio)

Programs already exist that allow for device screens
to be manipulated and viewed remotely by another computer.

Once installed, an attacker can watch what a user is doing or even go into the device
to see what information might be present.

An attacker might then manipulate the data without the user knowing.

While an attacker is going through data on a device,

he might find a file or picture of interest.

An attacker can easily pull that file off the device and send back to their computer for later use.

Most Bluetooth headsets use a PIN of 0000.

Programs can take advantage of that.

Once connected, a conversation can be recorded or played back in real time.

The standard range for Bluetooth is 30 feet,

but adding antennas can extend the range upwards of 1 mile.

Devices such as smart phones and tablets are essentially computers.

They can be hacked like a computer, and current security mitigations for wireless devices are not up to the same level as desktops and laptops.

Classified and other sensitive information

should not be present on wireless devices until a time when they have been approved for that data.