The Internet of Things: Risks in the Connected Home

Research Paper

Bitdefender

Contents

Author

Alexandra Gheorghe

February 2016

Executive summary

Four billion internet-connected devices promise to take our homes to an unprecedented level of comfort.[1] But this new digital convenience takes its toll on private lives. As we have seen in the early stages of IoT development, gadgets designed for our home can talk with each other, yet they risk being overheard when communicating sensitive data.

Bitdefender believes the IoT can reach its full potential only if interactions between users, devices, applications and the cloud are authentic and secure.

In this light, researchers from Bitdefender Labs examined four Internet-connected consumer devices and found several common vulnerabilities. The analysis reveals that current authentication mechanisms of internet-connected devices can easily be bypassed to expose smart households and their inhabitants to privacy theft.

Connectivity between IoT devices

We investigated a random selection of popular and affordable consumer IoT devices to understand the security stance of each. The team scrutinized the way each device connects to the Internet and to the cloud, as well as the communication between the device and corresponding mobile application.

First and foremost, it's important to understand that Internet-facing devices use multiple models of communication. Some use **device-to-device communication**[2], with devices communicating with each other directly via protocols like Bluetooth, Z-Wave or ZigBee. Residential IoT devices like light bulbs, switches, thermostats and door locks normally connect this way to send small amounts of information to each other.

In a **device-to-cloud communication model,** the IoT device connects directly to an Internet cloud service (an application service provider) to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. Popular consumer IoT devices such as the Nest thermostat and Samsung Smart TVs[3] are known to use this communication pattern.

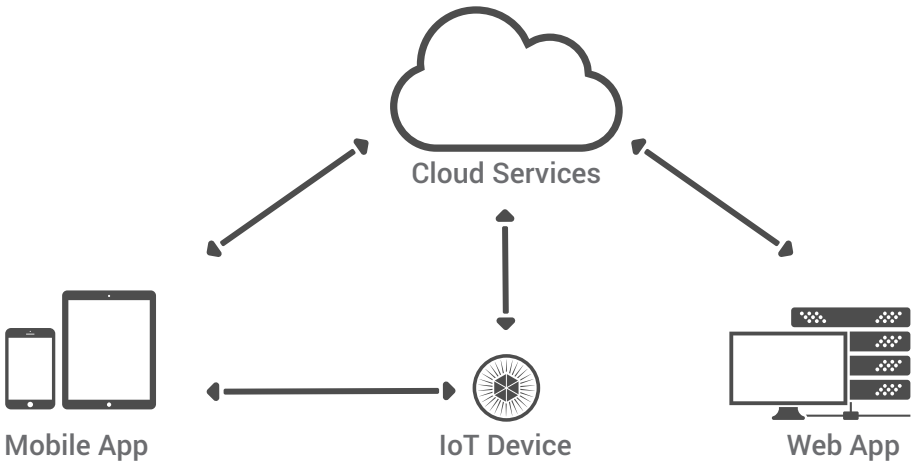

Fig.1 Communication in an IoT landscape

Most consumer devices rely on the **device-to-gateway plan**. The smartphone acts as the middleware for interaction between the Internet and "things".

Hubs also fill this role - dozens of vendors have created smart home-automation hubs that promise to serve as one-stop shops to control home thermostats, lights, door locks, windows shades, intercoms, monitor cameras, security systems and more. They act as local gateways between individual IoT devices and a cloud service.

All four devices from the aforementioned analysis use **a smartphone app as a means of remote control.**

1 http://www.gartner.com/newsroom/id/3165317
2 https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf
3 http://www.samsung.com/sg/info/privacy/smarttv.html

Unique security challenges in the IoT landscape

The disruptive nature of the Internet of Things raises its own security challenges. For instance, constrained in memory and computer resources, IoT devices can't always support complex and evolving security algorithms. Another setback is that IoT products don't include long-term support or automatic firmware updates despite being created with longevity in mind. Smart meters, for example, can last more than 40 years. Another handicap is that most devices are, to the end user, like black boxes – few people know how everything works.

But some of the most ardent security questions concern data confidentiality, authentication and access control:

- What is the role of data encryption in IoT?
- Which technologies can be adapted for the Internet of Things, despite constraints on cost, size and processing speed?
- Are the devices secure enough for consumer use?

Unfortunately, these questions are yet to be answered and solutions are still works in progress. Some vendors, like Philips and Apple, have created a locked-in ecosystem in view of better security. However, at this stage in IoT development, interoperability, although clunky, proprietary, resource-intensive, and largely controlled by vendors – is very important. So, most vendors leave their platforms open-source and, consequently, more exposed to code manipulation.

Privacy Expectations

The Internet of Things has the potential to infringe on basic human rights and Internet principles by collecting data with an unprecedented level of detail. We can learn more about someone than ever, based on the person's intentional disclosure of eating habits, location, lifestyle, etc. as well as via metadata. And although fragmented data sources seem harmless, by aggregating them, cyber-criminals can create an invasive digital portrait of a person. The IoT expands the reach of surveillance and tracking, leaving users with few or no options to customize privacy settings or control what happens to their data.

One aspect that interests us in particular is the concept of **privacy by design.**

- How can we encourage IoT device manufacturers to integrate privacy principles into every phase of the design?
- How do we reconcile functionality and privacy requirements?
- Should devices be designed to collect data by default?

Research findings

The researchers have chosen devices meeting this criteria:

a. Customer-focused

b. Affordable (under 100 US dollars)

c. Real-world impact

Methodology

We have installed and configured the devices as per documentation. In a test environment, Bitdefender's research team monitored and tried to capture all communications between each device, app, the cloud and the Internet.

The devices were purchased and tested between September-October 2015.

WeMo Switch

The Wi-Fi enabled WeMo Switch lets users turn electronic devices on or off from anywhere. It uses an existing home Wi-Fi network to control TVs, lamps, stereos, heaters, fans and more.

Biggest issue: Vulnerable protocols

Bitdefender Labs researchers found that the UPnP compatible switch communicates with its smartphone app without authentication. When the hotspot is configured, everything is transmitted in plain text except for the password. However, this is encrypted with an easily breakable 128-bit AES algorithm.

The Wi-Fi password is encrypted with a key AES derived from the MAC address and the device ID. Since the device ID and MAC address are transmitted prior to the encrypted password we have all the elements for decryption.

Stream Content

```
POST /upnp/control/metainfo1 HTTP/1.0
Content-Type: text/xml; charset="utf-8"
HOST: 10.22.22.1
Content-Length: 281
SOAPACTION: "urn:Belkin:service:metainfo:1#GetMetaInfo"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
schemas.xmlsoap.org/soap/encoding/">
   <s:Body>
      <u:GetMetaInfo xmlns:u="urn:Belkin:service:metainfo:1"></u:GetMetaInfo>
   </s:Body>
</s:Envelope>
HTTP/1.0 200 OK
CONTENT-LENGTH: 373
CONTENT-TYPE: text/xml; charset="utf-8"
DATE: Sat, 01 Jan 2000 00:03:09 GMT
EXT:
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
schemas.xmlsoap.org/soap/encoding/"><s:Body>
<u:GetMetaInfoResponse xmlns:u="urn:Belkin:service:metainfo:1">
<MetaInfo>[redacted]|Plugin Device|WeMo_WW_2.00.8095.PVT-OWRT-InsightV2|
WeMo.Insight.4E4|Insight</MetaInfo>
</u:GetMetaInfoResponse>
</s:Body> </s:Envelope>
```

Fig. 2. Device MAC and SSID

Stream Content

```
POST /upnp/control/smartsetup1 HTTP/1.0
Content-Type: text/xml; charset="utf-8"
HOST: 10.22.22.1
Content-Length: 897
SOAPACTION: "urn:Belkin:service:smartsetup:1#PairAndRegister"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
schemas.xmlsoap.org/soap/encoding/">
   <s:Body>
      <u:PairAndRegister xmlns:u="urn:Belkin:service:smartsetup:1">
         <PairingData>&lt;PairingData&gt;&lt;ssid&gt;&lt;![CDATA[dd-wrt]]&gt;&lt;/
ssid&gt;&lt;auth&gt;WPA2PSK&lt;/auth&gt;&lt;password&gt;[illegible]==
1901&lt;/password&gt;&lt;encrypt&gt;TKIP&lt;/encrypt&gt;&lt;channel&gt;1&lt;/
channel&gt;&lt;/PairingData&gt;</PairingData>
         <RegistrationData>&lt;RegistrationData&gt;&lt;DeviceId&gt;[illegible]/
DeviceId&gt;&lt;DeviceName&gt;&lt;![CDATA[Samsung GT-I8160]]&gt;&lt;/
DeviceName&gt;&lt;smartprivateKey&gt;&lt;/
smartprivateKey&gt;&lt;ReUnionKey&gt;[illegible]/ReUnionKey&gt;&lt;/
RegistrationData&gt;</RegistrationData>
      </u:PairAndRegister>
   </s:Body>
</s:Envelope>
HTTP/1.0 200 OK
CONTENT-LENGTH: 300
CONTENT-TYPE: text/xml; charset="utf-8"
DATE: Fri, 25 Sep 2015 13:48:48 GMT
EXT:
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
schemas.xmlsoap.org/soap/encoding/"><s:Body>
<u:PairAndRegisterResponse xmlns:u="urn:Belkin:service:smartsetup:1">
<PairingStatus>Connecting</PairingStatus>
</u:PairAndRegisterResponse>
</s:Body> </s:Envelope>
```

Fig. 3. Capturing password and SSID to decrypt encryption key

Using the decryption code from the application, our researchers managed to reverse engineer the password. They gained access to the device and were able to perform various tasks.

Status: not fixed

Lifx Bulb

Lifx Bulb is a smart LED with Wi-Fi radios built in. Fully compatible with Nest, it allows users to adjust colors according to weather, mood or music.

Biggest issue: Insufficient authorization and authentication

The smart bulb carries a design vulnerability that allows hackers to intercept credentials of the user's Wi-Fi network.

During normal setup, the device creates a hotspot. This is used by the Android app to manage initial configuration of the device. During setup, the device asks for the username and password of the home network. Once the credentials are entered, the bulb connects to the Internet and the hotspot is closed.

An attacker can switch on/off the device 5 times (1-2 second intervals) to reset the configuration state and force the creation of a new hotspot. He can do so by manipulating the physical switches, which could be located outside the home perimeter. Once the user sees the bulb is not working, he will try to re-register it in the application.

Meanwhile the attacker creates an identical fake hotspot.

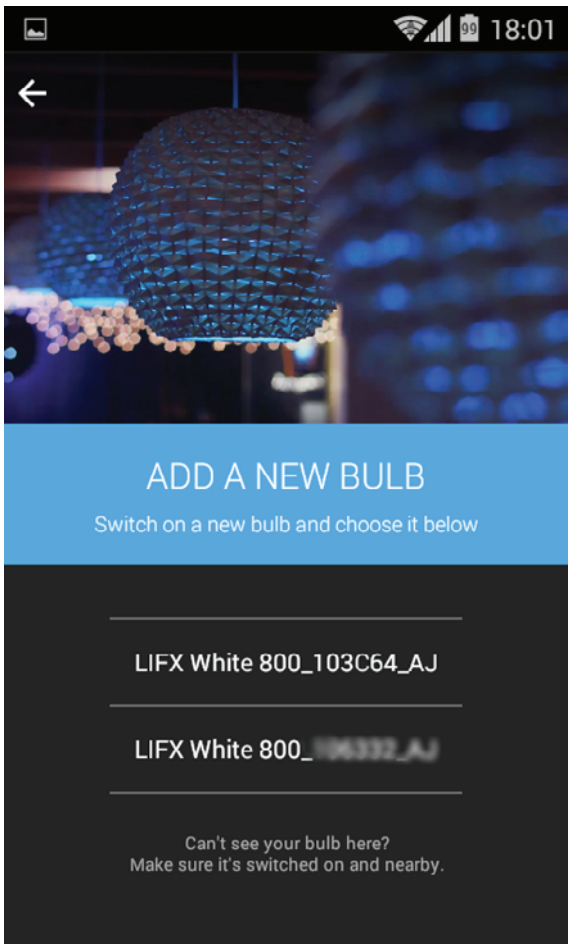

Fig. 4. Fake hotspot ranks first among other networks

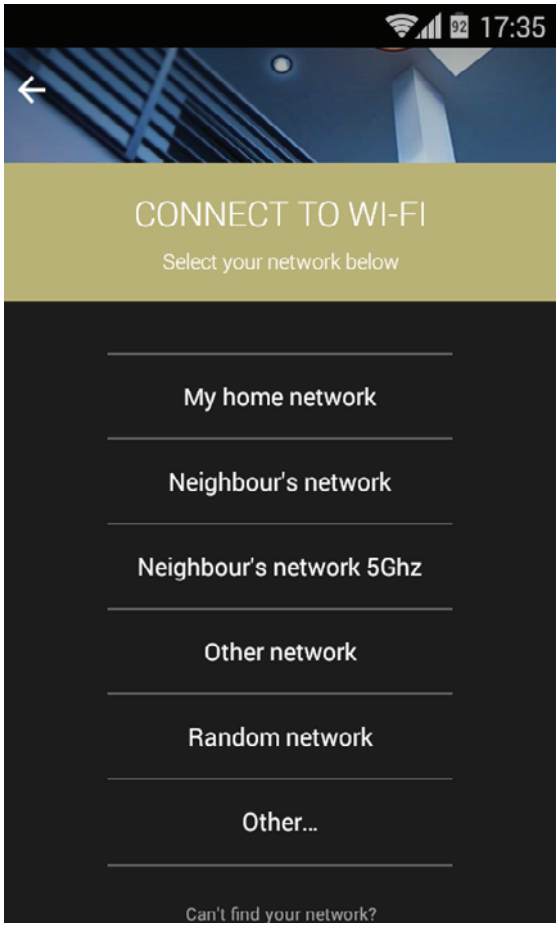

Fig. 5. App selects fake hotspot from other visible networks

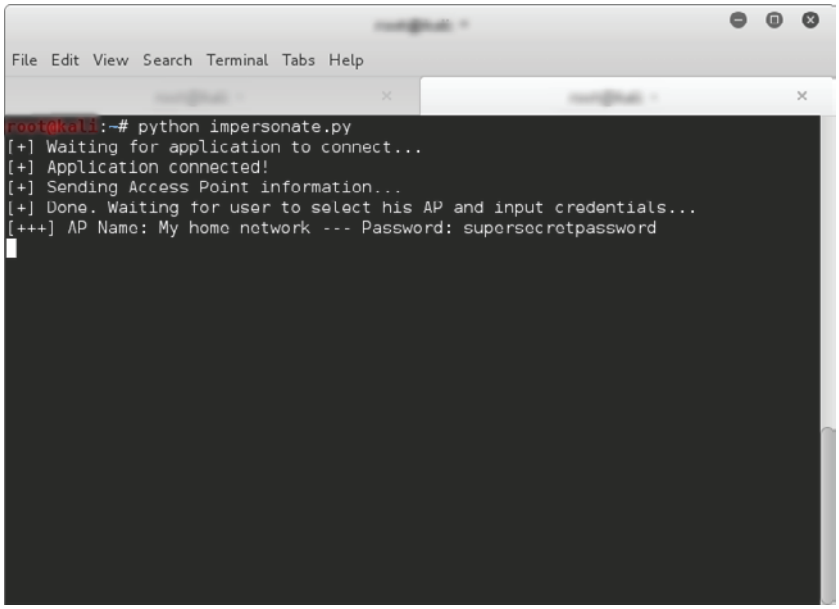

Fig. 6. Attackers' script during configuration service

By manipulating the device's MAC and SSiD, the fake hotspot appeared on top of the list along with the authentic one. It managed to fool the Android app looking to establish a connection. The connection succeeded and our researchers managed to grab the username and password of the user's Wi-Fi network.

The attack is still possible on the application's latest version, 3.3.0.1.

Status: not fixed

LinkHub

The starter kit includes two GE Link light bulbs and a hub. The hub allows the user to remotely operate individual lights or groups, sync them with other smart products, and automate lighting to fit the user's schedule.

Biggest issue: Lack of transport encryption when configuring through hotspot

The two lightbulbs and the smart adaptor can be controlled via an Android app. Initial setup of the smart adaptor creates a temporary hotspot, which lacks authentication mechanisms and the data is transmitted through it in plain text. By using the same interception maneuver as above, researchers managed to capture network credentials.

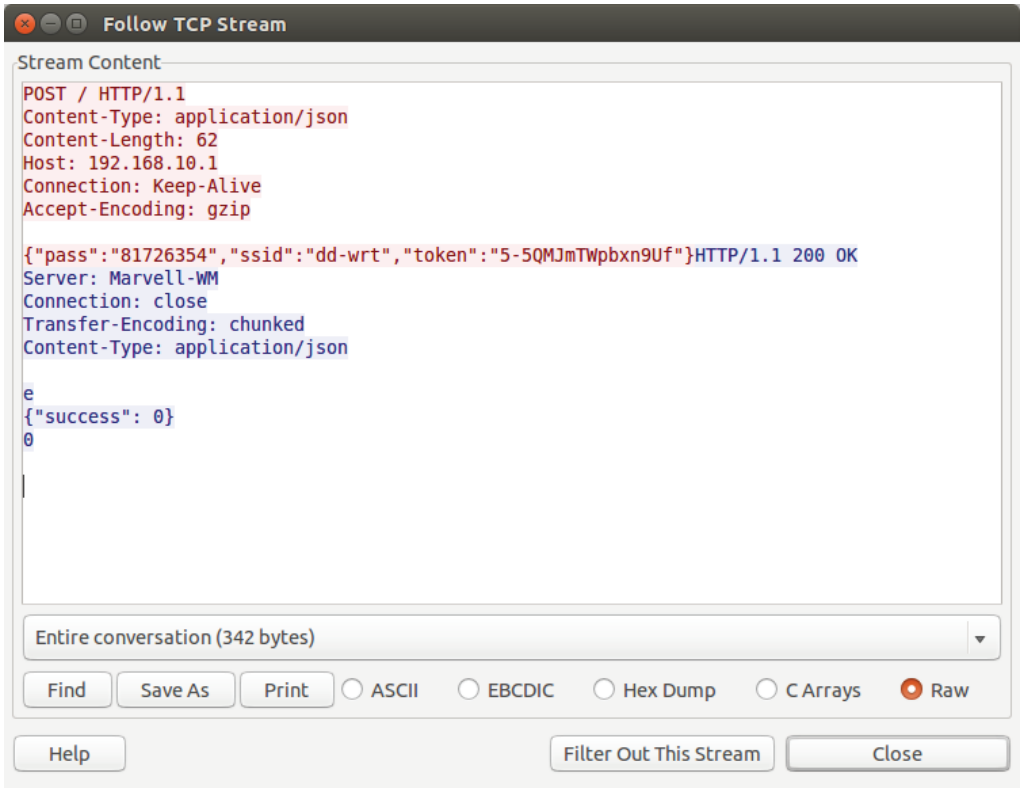

Fig. 7. Attacker sniffing packets during configuration

Sending data in clear text is a rookie mistake. However, while today's encryption protocols are robust, they require high compute platforms, a resource that may not exist in all IoT-attached devices. But this is in no way an excuse to avoid encryption.

Status: not fixed

MUZO Cobblestone Wi-Fi Audio Receiver

Muzo Cobblestone is a Wi-Fi audio receiver that allows users to stream music services to a sound system from smartphones and tablet.

Biggest issue: Unencrypted hotspot

The music player follows the same setup routine – it creates a hotspot. This time, the hotspot remains active indefinitely after configuration.

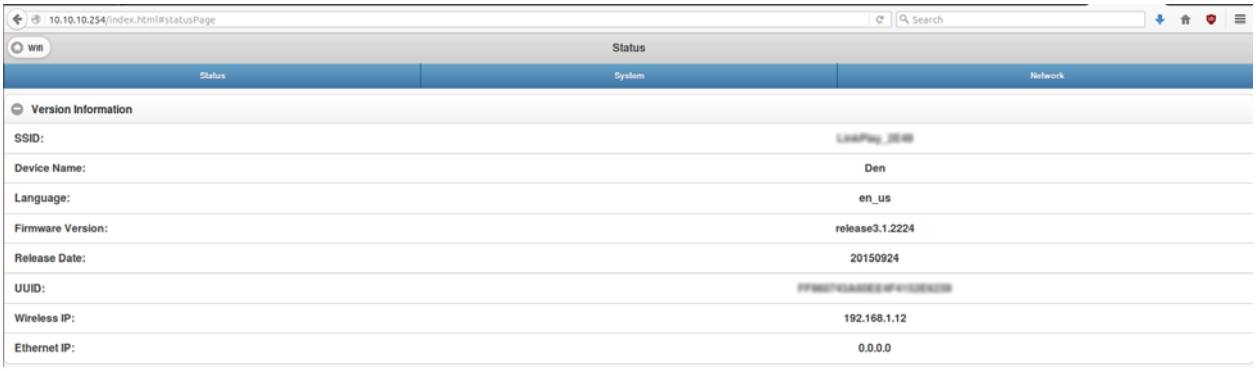

Fig. 8. Device information from the configuration page of the system

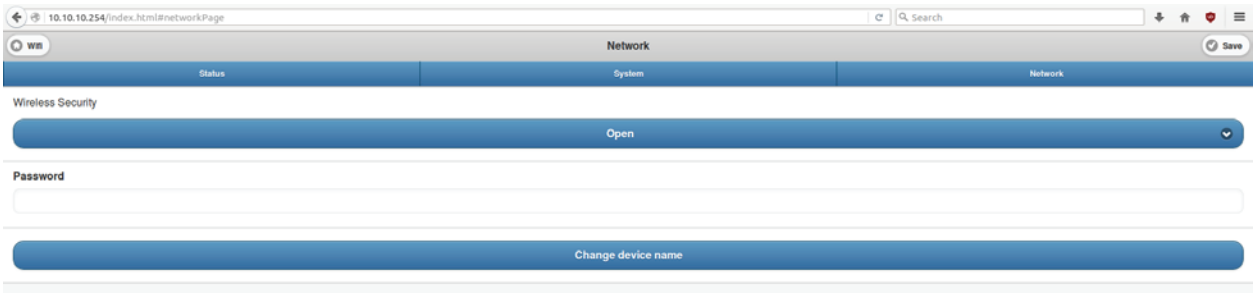

Fig. 9. Access point password can be changed

The access point can be protected by setting a password from the configuration page, but nothing notifies the user about this possibility, nor of the existence of the configuration page. There is no attention or notification in the Android application.

The device comes embedded with a Telnet service that allows users to access the device remotely.

Telnet is an old and simple-to-use network protocol that allows a user on one computer/device to log into another computer/device in the same network. One of the biggest problems with Telnet is that it's always active on the device.

Telnet ranks 6th among the 10 most-used services, according to Shodan (March 2015).

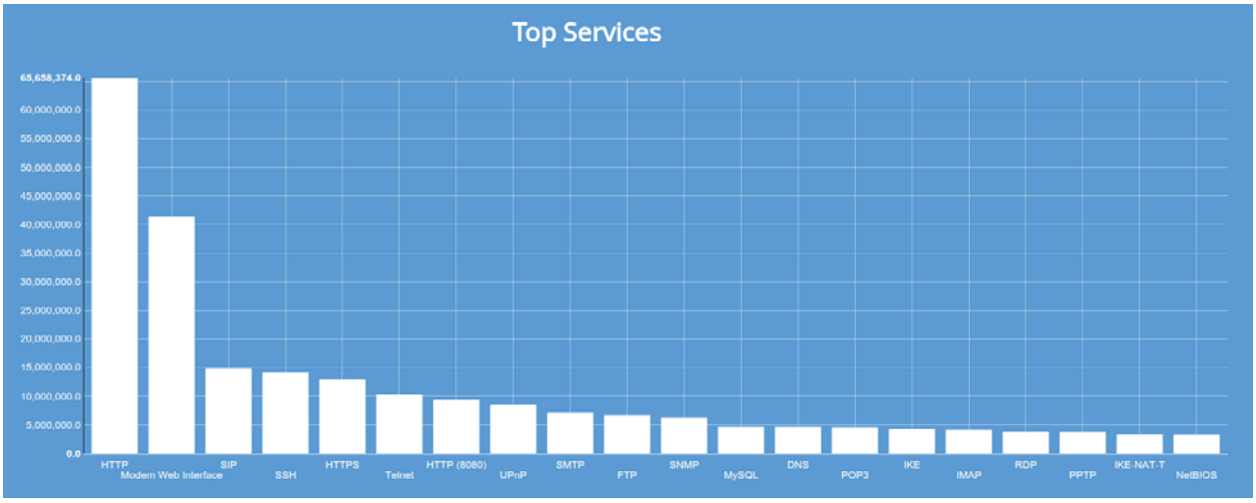

Fig. 10. Top 10 most used services in March 2015

Our researchers tried basic password brute-forcing and observed that the initial credentials of the service were admin/ admin.

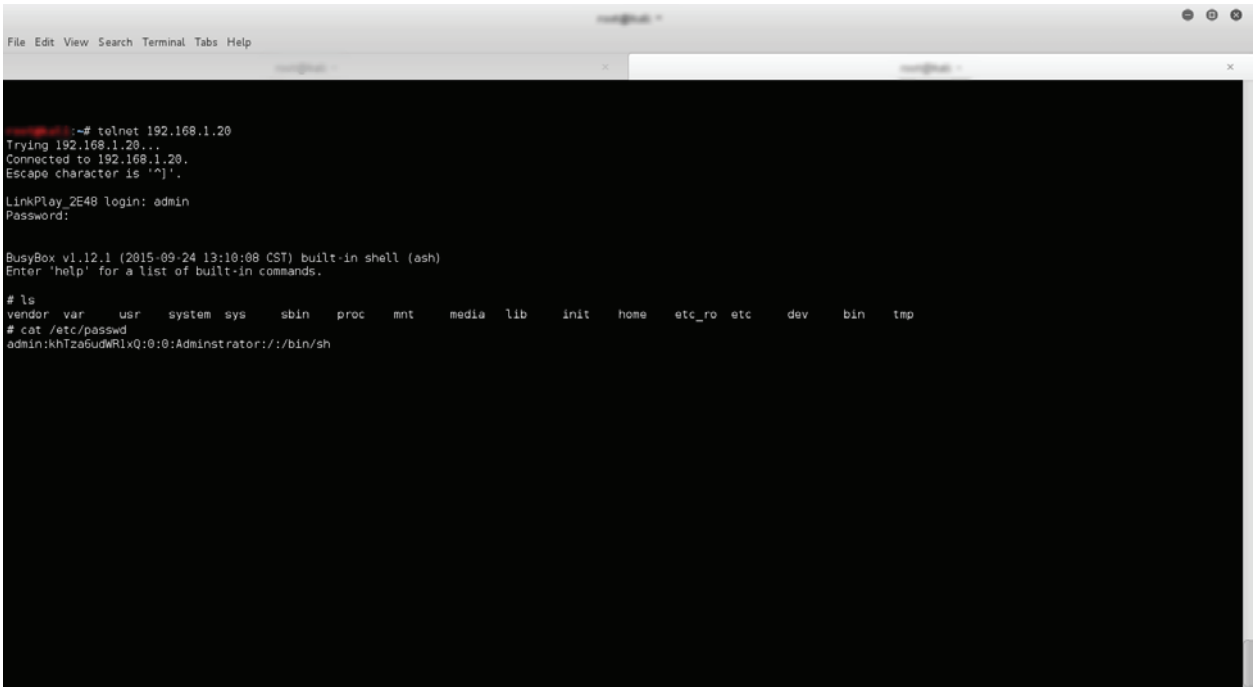

Fig 11. Telnet service stores default credentials

Since the device is connected both to its hotspot and to the home Wi-Fi, it's fairly easy to find and grab the files were Wi-Fi credentials are stored.

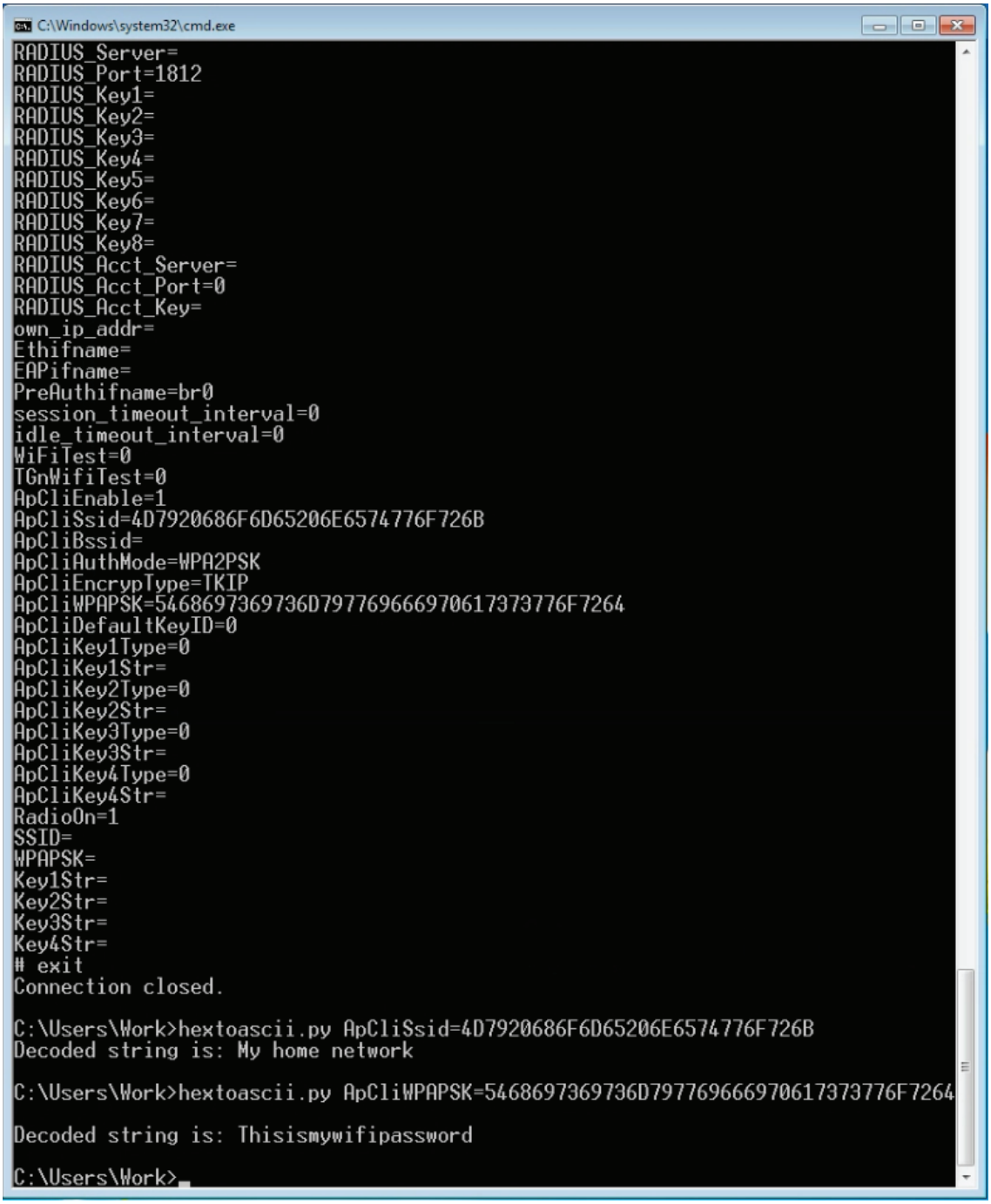

Fig. 12. Attackers steal Wi-Fi password after configuration

A fundamental element in securing an IoT infrastructure concerns device identity and mechanisms to authenticate it. These devices are pushed to market rapidly, without strong authentication mechanisms. Data disclosures show many IoT devices are secured with basic passwords like “1234” or require no passwords at all. This leaves them vulnerable to brute-force attacks and intrusion. Although threats in the IoT environment might be similar to those in the traditional IT environments, the overall impact differs significantly.

Status: partially fixed. After the most recent firmware update, the access point is no longer active after configuration, but the Telnet service is.

Future security priorities

This research reminds us of the imperative to embed a proper security architecture in the lifecycle of devices.

As security becomes more entwined with the physical world, protection against physical manipulation needs to be addressed, too. Mobile devices can be stolen. If someone successfully hacks into the memory of an IoT device and reads the encryption key, every identical device that is or has been shipped becomes vulnerable. This is a real problem for both consumers and the industry as a whole.

The IoT opens a completely new dimension to security – it is where the Internet meets the physical world. If projections of a hyper-connected world become reality and manufacturers don't bake security into their products, consequences can become life-threatening.

To prevent this, IoT security needs an integrated home cybersecurity approach. That means shifting from device-oriented security to a solution able to protect an unlimited number of gadgets by intercepting attacks at their core: the network. Bitdefender BOX is a forward-thinking, powerful piece of hardware that acts as an antivirus for networks and provides advanced malware protection for all connected devices.

Responsible disclosure

Bitdefender practiced reasonable disclosures with the vendors of the aforementioned IoT equipment. So, as a matter of course, the vulnerabilities were reported in accordance to Bitdefender's vulnerability disclosure policy. According to this policy, vendors are officially informed of the findings and encouraged to solve the bugs/flaws in their products. 30 days after the initial reporting, the findings are published.

The analysis has been performed by Bitdefender researchers Dragos Gavrilut, Radu Basaraba and George Cabau.

About Bitdefender

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/ .

B

B

Publication Date: February 2016

BD-NGZ-Mar.08.2016-Tk#: 86847