SUIB: Browsing local web resources in a secure usable manner

IoT device configuration as a special case

Primary contributions
Jan Geertsma (Signify)
Christian Amsüss
Micheal Richardson
Nick Allott
THE PROBLEM

Browsers cannot connect securely (and useably) to local “intranet” resources
Learn about the BT Hub Manager

Alongside the launch of our new BT Smart Hub 2, we've redesigned the Hub Manager. It's now even easier to manage the Hub's settings and to get the best wi-fi set-up. It's also easy to see the Hub Manager across all devices.

How to open the Hub Manager

1. Open a new web browser
2. Type 192.168.1.254 into the address bar

3. This will open the Hub Manager
1. Overview

When your Vodafone Mobile Wi-Fi Router is switched on and you are connected to its Wi-Fi network, you can view the status of your Router by opening the Mobile Wi-Fi Web application in your web browser. Enter http://VodafoneMobile.wifi in your browser to open the app.

The Web app view that is opened first will look similar to the picture below, displaying the status of your mobile broadband and Wi-Fi networks.
How to view your IP camera remotely via a web browser

User Application Requirement

This Article Applies to: 

Note: The steps below assume you already have your IP camera installed and connected to a router with Internet access. HTTP://192.168.1.101 represents the IP address of the camera being accessed.

Step 1
Find your camera's IP address. If you don't know its IP address, click here.

Step 2
Open a web browser and type the IP address. Enter your login information.
Xfinity Wireless Gateway Admin Tool

A lot of people like using My Account, xFi, and X1. But if you’re more advanced, you might also want to try the Xfinity Admin Tool.

1. Connect a computer, tablet or phone to your network. You can either use WiFi or hook up an Ethernet cable to your Gateway.
2. Open a web browser and go to the Admin Tool (http://10.0.0.1). This is the Wireless Gateway’s administration site. The default settings to open the Admin Tool are:
   - **Username:** admin
   - **Password:** password (case sensitive)
Internal name and Reserved IP addresses

- mdns .local
  - Not secure
  - philips-hue.local/

- private ip-address
  - https://10.0.0.74

- ipv6 linked-scope
  - [fe80::eel5:fafe:fe10:be76]
WHY IS IT THIS WAY

Usable or Secure – Pick one…..
"Attackers might be trying to steal"
5 Communicate securely
5.1 No universal default passwords

Provision 5.1-1 Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

NOTE 1: There are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged according to NIST Special Publication 800-63B [i.3]. Using passwords for machine to machine authentication is generally not appropriate.

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

EXAMPLE 1: During initialization a device generates certificates that are used to authenticate a user to the device via an associated service like a mobile application.

To increase security, multi-factor authentication, such as use of a password plus OTP procedure, can be used to better protect the device or an associated service. Device security can further be strengthened by having unique and immutable identities.

Provision 5.1-2 Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

EXAMPLE 2: Pre-installed passwords are sufficiently randomized.

As a counter-example, passwords with incremental counters (such as "password1", "password2" and so on) are easily guessable. Further, using a password that is related in an obvious way to public information (sent over the air or within a network), such as MAC address or Wi-Fi® SSID, can allow for password retrieval using automated means.

Provision 5.1-3 Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

Provision 5.1-4 Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
Insecure Transport

Description

Using HTTPS is best practice

uncommon problem that the configuration of the application fails to enforce the use of SSL on pages that contain sensitive data.

There are three common ways for SSL to be bypassed:

- A user manually enters the URL and types “HTTP” rather than “HTTPS”.
- Attackers intentionally send a user to an insecure URL.
- A programmer erroneously creates a relative link to a page in the application, failing to switch from HTTP to HTTPS. (This is particularly easy to do when the link moves between public and secured areas on a web site.)

Examples

- Login pages are not SSL protected
- A publicly accessible page contains a relative link to a protected page which forgets to switch to SSL.
Sol #8 Build an IoT App

- IoT Browser
- Enroll devices
1. **It's not scalable:** every new IoT device type, or device ecosystem, needs its own management application.

2. **Burden on end user:** that's many applications that the user might have to install. If I have 10 different IoT device manufacturers on my internal network, that means 10 different management applications.

3. **Usability:** it means we have added a new precondition to each IoT device/router installation – that is the need for yet another application.

4. **Cost to manufacture:** it adds cost and complexity for the manufacturer. A new application needs not only to be developed, but maintained indefinitely.

5. **Obsolescence and support costs:** applications need to be maintained indefinitely; operating systems updates increasingly render applications obsolete, meaning new versions have to be created, putting burden on user and manufacturer alike.

6. **Increases the attack surface:** although this solution solves the bootstrap encryption problem, we have increased the attack surfaces for the local IoT ecosystem, by adding an arbitrary number of end applications, where each application-device pairing is free to choose its own mechanism of negotiation for a secure administration channel.

7. **Control point:** by delegating management to an application, we are entirely dependent on the near-duopoly of application store providers (Google and Apple) to act as distributors of these applications. Given that both Apple and Google have clear commercial intent and ambition to be major players in the IoT space, there is a clear potential commercial conflict of interest here.

8. **Vendor lock-in and dependency:** openness, interoperability and security are fundamentals that should be core to new internet innovations. IoT should be no different.
THE FIX?

Where we have got to so far
CERTIFICATES IN THE WILD

0. No certificate (null) (USABLE)
1. Non device unique - self-signed certificate (NU-S/S)
2. Non device unique - untrusted root-signed certificate (NU-U/S)
3. Device unique - self-signed certificate (U-S/S)
4. Device unique - untrusted root-signed certificate (U-U/S)
5. Device unique - locally-signed certificate (U-L/S)
6. Device unique - CA root signed certificate (U-CA/S) (USABLE)

7. Non Certificate based trust?
SO WHY BOTHER?

- Bring secure connections to the home
- Simple and Secure
- It has to work for grandma
- It will work for small businesses and factories
- TLS PKI could complement or replace passwords

Think holistically: Create a technical landscape
SOL #6 DEVICE DNS NAME

https://support.plex.tv/articles/206225077-how-to-use-secure-server-connections/
Device DNS NAME: Christian Amsüss  

https://github.com/chrysn/provisioning-demo

- IOT Device
  1: Create key pair
  2: Create common name
  3: Register wildcard but device specific record on the DNS
  4: Generate CSR (using \(^*\).[dev-id].devices.vendor.example)
  5: Send CSR
  6: Return certificate
  7: Return to device
  8: Install certificate on local webserver

- DNS Server
  - DNS bind protection issues

- CA Processor

- CA Issuer

---

DNS bind protection issues
SOL #1 CHANGE THE WARNING

- Change browser warning message
- It won’t fix anything, but not exaggerating either

You are visiting a device for which the certificate can’t be verified
SOL #4 LOCAL GATEWAY PKI

- Sign it with your own signatures, gestures, button presses
- But what is the address you are signing?

- How to bring uniqueness to your network?
- How to prevent misuse?
MASA: Where a vendor can keep inventory

IDEvID: factory certificate
IEEE 802.1AR Certificate can bootstrap security

JOIN Proxy / EST How to obtain a certificate

Domain Registrar PKI RA

RFC8995
BRISKI

e.g., RFC 7030

"Domain" Components
NEXT STEPS ..?

- Publishing current progress in next few weeks
- Moving to open working model (GitHub open repo)
- Needling gov agencies
- Progressing the implementation experiments
- Strongly Suspect:
  - We need a enhanced browser
  - Better addressing paradigm
  - Different trust models (user vs manufacture)
- Ideas ... ????
QUESTIONS
OVERFLOW

Other bits....
Sol #5 Extend BRSKI

- Matter and FIDO Device Onboarding refer to BRSKI
- Maybe extend BRSKI for Consumer IoT?
- Use IEEE 802.1AR to bootstrap trust in your own home
Sol #7 IoT Infrastructure

- Global unique domain name for local context
- Dedicated IoT Certification Authority

- .iot is too close to .io
- .dev is too to developer
- .m2m / .home / .thing / .private / .here / .this
Solutions

Change one of the dimensions

Browser

Address

Certificate
Bringing it all together

- Context matters!
- Simple to change the warning message
- Difficult to attach a meaningful domain name to the device
- Difficult to validate the device is really yours
- Difficult to establish trust relationship
- Must work with other organisations
Quick History

- ITU X.500 1988
- Netscape SSLv2 1995
- Netscape SSLv3 1996
- IETF TLSv1.0 1999
- IETF TLSv1.1 2006
- IETF TLSv1.2 2008
- IETF TLSv1.3 RFC 8446 2018
Where does the trust come from?

Root CA's
- Mozilla CA
- Windows Root CA
- Google Root
- Apple Root

Browsers
- Mozilla Firefox
- Microsoft EDGE
- Google Chrome
- Apple Safari

Mobile
- Mozilla Firefox
- Microsoft EDGE
- Google Chrome Mobile
- Apple Safari
Sol #2 Treat local differently

- Change browser to be network aware
- Internal and External context matters

You are visiting a device for which the certificate can’t be verified. This device is located in your own network. Do you want to continue?
Sol #3 CA/Browser Forum Ballot

- Propose change of rule 7.1.4.2.1
- For .local certificates there is not unique address.

- EV Certificates describe the rules for .onion
- Darkweb gets signed certificates because the owner can validate the unique address.
OTOPS Agenda
IETF 112 [virtual] Madrid
Friday, November 12, 2021
16:00-17:00 (UTC)

Meetecho: https://meetings.conf.meetecho.com/ietf112/?group=iotops&short=&item=1
Jabber: iotops@jabber.ietf.org
Notes: https://notes.ietf.org/notes-ietf-112-iotops

Chairs: Alexey Melnikov and Henk Birkholz

16:00   Administrivia
        (5 min; chairs)

16:05   IoT Authentication in Next Generation Networks
        (5 mins; Behcet Sarikaya)

16:10   IoTSF ManuSecured SUIB: Browsing local web resources, in a secure usable manner:
        examining IoT device configuration as a special case
        (15 min; Michael Richardson)

16:25   Framework For Integrated Industrial Networks
        https://datatracker.ietf.org/doc/draft-iotops-km-iiot-frwk/
        (10+5 min; Kiran Makhijani)

16:40   Midlife Crisis (of an IoT Device)
        (10+10 min; Eliot Lear)