IoT Henry and Sally pairing protocol

Using existent standards for an user-friendly and more secure Internet of Things pairing system

© 2015, Roberto A. Foglietta <me@roberto.foglietta.name>

Revision 0.7.6, 13th december 2015, CC BY-SA 4.0

1. ABSTRACT

Internet of Things (IoT) market requires that micro devices like sensors with a limited computation capacity and power source would be able to negotiate with an access point (AP) their entrance in a Personal Area Network (PAN). Adding such devices into a PAN should be an user-friendly action for final customers. Moreover pairing system should be secure enough for the targeting market.

This pairing concept is based on sharing a cryptographically strong shared secret like a RSA public key (or anything equivalent) between two devices. Shared secret is used to let the two devices identify themselves and establish a trusted connection. A couple of NFC cards are used to inform the access point about incoming device set of permissions required and to acquire its credentials. Using a set of clearance levels, an ACL table and an API set, the configuration procedure could handle any kind of devices that support a standard encrypted connection like SSL or SSH tunnel and VPN setup.

1.1. INTRODUCTION

Security is a process, not a product. So far, absolute security does not exist even if deployed by design. Security and simplicity usually do not fit together but are at opposite in balance between them. It is quite difficult to imagine something simpler than pressing a button on each devices, e.g. on AP and new client, or pressing a button on AP and switch-on the new device immediately after. The two ways are not equivalent in terms of hardware requirements (a button on device also, even a switch on/off one), technical specifications (first hand-shake time frame) hence in terms of security (available time window for delivering an attack). Using a set of NFC cards (or any contact-less card with similar data capacity) is possible to attribute to any device a specific level of trust and related capabilities (guest, parent control, IoT device, administration, etc.). Moreover this helps in reducing the range in which the attacker should stay within to be considered a threat.

2. USERS AND THREATS

Attackers could be differentiate in two profiles:

A1 - casual attacker with limited resource, a personal motivation but with a possible great amount of spare time to invest in;

A2 - professional attacker high skilled, founded and motivated, relatively time constrained.

Counter measures will works for A1 may not work for protecting the system from A2 and viceversa. More over the professional attacker once defeat the system could publish a description of the security breach, a proof-of-concept or a complete tool to empower causal attackers to an higher level of threat. Design and safe factory configuration could mitigate risks but may not protect any single installation. Moreover safe configuration usually are not out-of-box user-friendly ready.

Profile A1 did not mean necessarily they are less dangerous. An A1 that could access locally would have a bigger chance to successfully attack the system than an A2 from remote. So far, A1 should not considered a merely less dangerous A2 subset. Social engineering should also included into the scene but from an OEM perspective this does not really matter as long as the solution is not insanely designed or factory configured.

Users as well could be diversified into two groups:

U1 - private facility conductor for personal or SoHo IoT usage

U2 - industry 4.0 or any other professional related infrastructure

Relation like U1, A1 and U2, A2 are not exhaustive because any very important person (VIP U1) could be object of A2 activities. Any kind of private or commercial espionage activity (A2) could be focused on a personal home network (U1) in order to easily gain an access to data transfers related to a work laptop (U2) and mobile or wearable devices add complexity in this picture.

A virus spread among smart-phones will be able to access PANs in which has been previously authenticate and attacks others PANs around. All data collected, even if not enough to successfully break into a PAN system, included brute force attempts, georeferential coordinates, PAN ID and devices list could be shared with others infected devices in order to carry on a massive and distributed attack. Factory ill or vulnerable devices may play their role, as well.

Fortunately, only U1 need a very easy way to pairing devices in their PAN because they do not have skills, time or resources to face a more secure but more complex pairing method. Others (U2) could relay on a professional installation service which bring to them a higher security standards in order to properly face A2 threats in terms of system architecture and system administration procedure.

So far previously solutions and standards were focusing on serving U1 and protecting them from A1, mainly. However solution could well enough designed to be used by U2 and able to be resilient to A2 threats as long as professional installation, configuration and securing policy has been implemented. Resilience (elasticity) differs from resistance (hardness) because is does not fail if a single step or component fail but still maintain a certain level of protection.

2.1. VULNERABILITIES

Widely available pairing methods demonstrated to be weak and progressively less adapt for the role has been designed initially. In particular some flaws have been found, impacting the security at protocol or design level and they are not anymore viable secure enough solution used as-is.

- Viehböck, Stefan (2011-12-26). "Brute forcing Wi-Fi Protected Setup" (PDF). Retrieved 2011-12-30. Allar, Jared (2011-12-27).
- "Vulnerability Note VU#723755 - WiFi Protected Setup PIN brute force vulnerability". Vulnerability Notes Database. US CERT. Retrieved 2011-12-31.
- "Windows Connect Now–NET (WCN-NET) Specifications". Microsoft Corporation. 2006-12-08. Retrieved 2011-12-30.

- Dennis Fisher (2011-12-29). "Attack Tool Released for WPS PIN Vulnerability". Retrieved 2011-12-31. This is a capability that we at TNS have been testing, perfecting and using for nearly a year.
- Slavin, Brad (January 18, 2013). "Wi-Fi Security – The Rise and Fall of WPS". Netstumbler.com. RetrievedDecember 17, 2013.

Original source: Wikipedia - https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup#Vulnerabilities

3. GOALS

In order to design an innovative and more secure pairing method for PAN devices, some of well-known assumptions may be challenged or totally abandoned. Design and delivering a new hardware subsystem may as well contribute to setup a new standard. Combination of existing standards may drive to a faster time to market solution.

3.1. APPROACHES

The are several possible approaches:

A - embrace a standard and using it as-is
B - enhance a standard maintaining back-compatibility
C - combining existing standards in an innovative way
D - proposing a totally new standard

Under security point of view option C and D do not fully satisfying higher security expectation as long as others less secure way to pairing are available, like fall back mode or back compatibility mode. So far, an option for disabling the previous less secure way of pairing is strictly necessary, preferably activated by default factory configuration.

(C) = (D) ∪ subset (A ∪ B)
secure (C, D) ∩ (A, B) = void ( )
secure ((C, D) ∩ subset (A, B)) ≠ void ( )

What is the subset (A, B) that has a not void intersection with (C, D) and still secure?

3.2. STATE OF ART

Following standards and protocols are widely available and in-deep documented

1. Wi-Fi Direct
https://en.wikipedia.org/wiki/Wi-Fi_Direct

2. Wi-Fi Protected Setup
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

3. Devices pairing using Wi-Fi Direct and NFC directive
https://msdn.microsoft.com/en-us/library/windows/hardware/dn481543(v=vs.85).aspx

4. Near Field Communication (and passive stickers)
https://en.wikipedia.org/wiki/Near_field_communication

5. MAC Address (unicity, hard cabled, privacy)
https://en.wikipedia.org/wiki/MAC_address#Spying

6. Bluetooth pairing and bonding
https://en.wikipedia.org/wiki/Bluetooth#Pairing_and_bonding

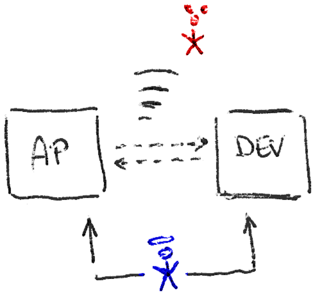
7. Certificate Authority
https://en.wikipedia.org/wiki/Certificate_authority#Security

Standards are so important just because they are standards, well-known, wide-spread around, inter-operative. However others technologies change and evolve in time and some assumption could fail to be acceptable anymore.
For example MAC address unicity could be useful in order to grant or deny network activities to certain devices but its unicity exposes consumers to others risks, in particular about privacy. So far, any unique identification number – despite if they are hard coded or not into read-only registry by factory setup – inherently contains the same shortcomings for consumers. For this reason MAC address randomization has been introduced into the market breaking the unicity assumption. In any case many network cards were allowing users to change their MAC address or part of. This shows that even a small number of devices implemented slightly away from a standard could be used to empower attackers or generate ill-behaving activities that could be exploited.

4. ANALYSIS

Design matters and implementation matters, as well. Pairing process usually are relaying over user triggering events that open a time window in which untrusted device would be accepted as trusted in a hand-shake procedure, this is sometime combined with a secret shared by user between the two parties.

Certification authorities relief the end user to be the one who authorize the trust of chain among parties but require a Internet connection which is not always granted being available on a local PAN. Another successful authentication mechanism is based on key and lock, as long as key and lock could not be easily tampered and key could not easily copied.

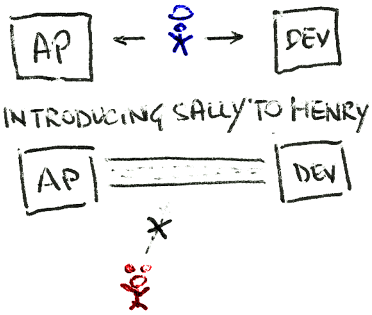


Typical and most effective attacks are base on ear-dropping and man-in-the-middle combined with brute force techniques empowered by optimized algorithms, great calculation capacity availability, off-line computed dictionaries or rainbow tables and vulnerable implementations that leaks informations or greatly reduce the combinatorial domain.

4.1. THE IDEA

The importance of being Sally.

Henry would like to know Sally but he knows that to acquire from her a certain degree of trust, he has to be introduced to her by a common trusted friend. This is the trust-of-chain basic concept and the implementation relays on unique humans ability to recognize faces which is difficult to tamper.



Forget biometrics because are sensitive data complex to deal. For personal IoT and SoHo use, they could be replaced with something like contact-less business cards which contains all data to identify and authorize the desired device. The owner present himself to the AP by the chosen card then introduce the new device to the AP presenting the device card and switch-on it.

Another typical human characteristic involved in granting trust to someone else is that process is not a single act but a step-by-step path escalating higher level of trust. At any step and at any time the level of trust could be reverted back or completely denied. So far, NFC colored cards are not the only part of the system that is designed to manage different levels of trust, but the pairing protocol itself.

NFC cards are cheap to create, easy to read and accessible only locally within 5 cm (without the usage of special and costly devices). Today they could store up to 8.192 bytes of data that are enough to store credentials, device and producer identification, required network permissions and describe a list of features exported by the device.

5. HENRY AND SALLY PAIRING

The AP works as ADSL modem, Wi-Fi (IEEE 802.11), may have low power wireless communication (6LoWPAN, Z-WAVE or ZIGBEE) access point and bluetooth tethering capabilities.

At the beginning, it is supposed that all devices could be paired with Sally introduction system based on NFC cards. Others devices like laptops, smart phones and tablets which did not have their own NFC cards will be paired with a secure back-compatibility way named Henry.

5.1. SALLY CONCEPT

Sally pairing protocol is based on colors in order to quickly familiarize the end user with security levels simplifying the concept by the use of colors. The related card will report the English name of color or the first letter of the color in black ink on white background for color impaired people. More over in the same B/N box will be displayed the number related to that level, number could be presented as roman number or dice stamp embossed onto the card. Number or dice stamp will help not English speaker and embossed number or stamp will help vision impaired people.

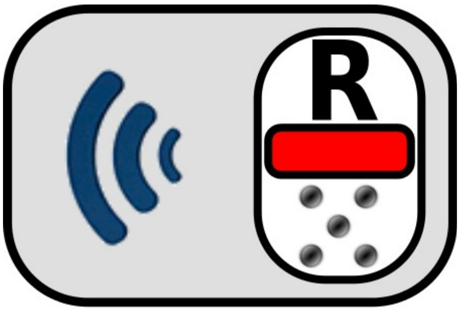
Standardization of color scale and card presentation is mandatory to set up a common knowledge about how Sally protocol could be used. In each country, all around the globe, everybody will be able to use the same system to do the same things.

5.1.1. Sally concept for Access Point

The AP box is delivered to the end user with several NFC cards in a special radio protected box which avoid in warehouse massive NFC data collection:

- 1. WHITE: guest device, parental control, back-compatibility, no VPN, PAN trough AP only
- 2. GREEN: local PAN device without any Internet connection, accessible only by AP
- 3. YELLOW: like GREEN with the ability to communicate with others local devices
- 4. ORANGE: like YELLOW with the ability to communicate over Internet
- 5. RED: full access to Internet and local PAN devices directly
- 6. BLACK: like RED with AP administration authorization

The AP manual will report the warnings related of using BLACK card only for AP administration purposes and that IoT PAN devices should not be paired using RED or BLACK cards (unsafe).



5.1.2. Sally concept for devices

Each device enabled for Sally pairing protocol will be delivered by OEM producer with a NFC card and the manual will instruct the user which level of security each feature will require. So far, the end user could decide to have limited features set in order to maximize security or full features set.

If a device supports different users or profiles (e.g. guest, parent controlled, standard users, administrator, etc.) then the procedure should repeated for any profile. The AP administration web interface could be used to assign clearance levels to any device and any profiles.

5.1.3. Sally pairing procedure

Pairing procedure does two mainly tasks: let the new device found the wireless network and setup a VPN in a secure way despite the medium may be not completely trustful by itself.

Descriptive example.

The end user wish to pair a new device to the AP with a certain level of trust. User presses the pairing button. A blinking led will inform the pairing procedure has been started. It should be completed within a certain time frame outside of which the NFC reader will be disabled in order to avoid NFC data collection (like e.g. credit card). A colored NFC card and the new device NFC card will be presented to the AP at the same time (within the timeout). If the AP will read multiple colored card codes or multiple device card codes will drop the procedure. The manual will inform the user that others NFC cards should be kept far away the AP during pairing procedure. Within a limited time frame the paired device will be able to establish a connection with the AP and exchanges credentials in order to complete the authentication procedure. At the end of that time frame the pairing procedure will be aborted and it should be repeated.

Example of table of interactions in chronological order.

END USER	ACCESS POINT	DEVICE
Pairing button pressed	WPS	WPS or ON
	Led starts to fast blinking	
NFC colored and device cards are presented to AP		It founds the network but medium is still insecure
	Led starts to slow blinking	
	It starts the VPN configuration via an encrypted tunnel	It receives VPN configuration and credentials to log in
	It insert the device into its inner ACL table	
	Led stops blinking	

Normal working led color is green. During configuration the blinking led will be yellow and return green at the end. If configuration procedure will be aborted or unsuccessful the led will change color, still or blinking red, for few seconds before returning green.

5.1.4. Sally configuration procedure

The AP offers a wireless communication channel as usual. Any device could connect to the AP by WPS procedure (or another hand-shake protocol equivalent). This connectivity would not give any access to any resources apart those are strictly necessary to complete the VPN configuration process. Even if not any encryption is used for the medium, the configuration procedure is safe because is based on data transferred by NFC card, out-of-band. If configuration will not be completed within a limited timeout, then it will be aborted.

List of mandatory data the AP need or useful to retrieve from the NFC device card:

- networking mac address or equivalent device network identification
- list of available procedures for configuring the device, the first is the preferred
- if it exists, a custom configuration procedure should report actions in terms of a set of API
- a shared secret like a RSA public key or anything equivalent
- list of capabilities and related ACLs required with their level of clearance
- some of these capabilities and related ACLs could be optional

End user should be able to reset to factory configuration the device in order to pairing with another network or because a major network change.

Any NFC device card could contains several public keys. The device may use one taken randomly each system reboot. For a limited timeout after the reboot, device will offer the configuration service or trying to access the configuration service.

5.1.5. Sally configuration procedure examples

Example n° 1 – AP takes the initiative

> The AP received and stored in its not-volatile internal memory the pairing mac address (or any other equivalent device ID related to the networking interface), credentials to remotely and securely access to device, some information about configuration procedure. The device has micro SSH server (or equivalent cryptographic service, like SFTP) and its port number is stored into NFC data. The AP accesses into device via encrypted connection and write in its not-volatile internal memory the credentials needed to open a VPN (or any other encrypted communication channel supported) and data usefully to route data packets and to export its capabilities like in any RESTfull system.

- Man in the middle attack: the AP has the public key of the new device read from NFC card. Because of this, the AP could verify the real identity of the device preventing the attack from someone pretending to be the waiting device. Attacker could impersonate the AP and trying to access to the waiting device but it has not the device public key shared only by NFC. So far, attacker cannot put a valid signature on the device challenge response.

Example n° 2 – Device takes the initiative

> The AP received and stored in its not volatile internal memory the pairing mac address (or any other equivalent device ID related to the networking interface), a shared secret from device (like RSA public key or equivalent). The AP offers to the device (any other devices with different mac address and IP will be blocked on that port for that time). The configuration service port is indicated into NFC data among those (port-range) allowed for the configuration procedure. Otherwise, another configuration procedure will be choose from the list. The device browse the AP resource page and download its public key then open a connection to the AP on a specific port for configuration. The AP sends to the device data encrypted with its private key and with the device public key. The device will be able to decrypt such data because it has the public key from the AP (attacker may have as well) and its own private key complementary to the one shared via NFC with the AP (attacker has not). Data sent will contains all parameters and credential necessary for open a VPN (or any other encrypted communication channel supported) and to route data packets and to export its capabilities like in any RESTfull system.

- Man in the middle attack: attacker could impersonate an incoming device but because it has not new device private key, it cannot put a valid signature on the challenge sent by the AP. The attacker could impersonate the AP but because it has not the device public key, it cannot put a valid signature on the configuration dataset and device will not accept any invalid or encrypted data.

Denial of Service: it slows down or forces the procedure to fail. Repetition of the pairing procedure increases the chances for the attacker to try the MITM attack.

Others limitations: devices build on single task, single thread, CPU would not be able to run a service in parallel at boot time but configuration service may starts only if encrypted network access failed and in any case, it will terminate within a limited timeout.

5.2. HENRY CONCEPT

Henry procedure aims to bring Sally advantage to devices with does not come with NFC presentation card out of box using different medium and approach. Once Harry procedure has been completed the Sally one could take place. Back compatibility introduce an extended set of vulnerabilities which could be faced using the same principles behind firearm security systems design.

Sally protocol relays in information about device that AP will receive from out-of-band medium in order to complete the pairing procedure. While Henry protocol relays on AP giving information to the device in order to complete the pairing procedure.

The main issue is that any wide range wireless medium is inherently insecure if device could not trust AP and AP does not know how to reach the device and trust it. Thus, the man-in-the-middle attack is the main threat and the solution itself. In fact the entire procedure is nothing else that a scaling level of trust like an attacker would do but trusted parties do that with an advantage to the attacker, in a such limited time frame that attacker would not compete, or could not compete easily enough.

Henry off-of-band data transfer could happen via many ways. Some of them have an intrinsic level of security like 3G, USB, Ethernet or NFC cards writer and have a decreasing level of user friendless. Others like bluetooth, WPS, shared PIN or password belong to those subset of solution that demonstrated to be vulnerable and could not be trusted nor used as-is like in the past.

Sally procedure is the main point of strength which brings the security usually related to enterprise networks to the end user without the pain of dealing with such technologies. However, designing and implementing a secure and user-friendly Henry procedure is the key of a fast adoption of AP which implement Sally procedure as well.

5.2.1. Henry via 3G connection

Any tablet and mobile phone which has an 3G connectivity could retrieve the application from its own store. At the first run, the application will register the device to the OEM web server via a secured SSL transaction, then will open a registration procedure to the local AP and finally will inform the user to press the pairing button. The AP will retrieve information about local incoming device comparing it with the registered ones into the OEM web server and via OEM web server will signal the application to inform the user to present the NFC card related to the trust level which should be transferred to the new device.

5.2.2. Henry via USB flash drive

User connect any USB flash drive into the AP, presses the pairing button and presents to the AP the NFC card related to the trust level which should be transferred to the new device. The AP writes on that USB a self-starting software that will take care of everything else.

5.2.3. Henry via Ethernet

User could connect any laptop or desktop via an Ethernet cable to the AP, presses the pairing button and presents to the AP the NFC card related to the trust level which should be transferred to the new device. This allows him to land to an AP internal page from which he could download all the software that will take care of everything else.

5.2.4. Henry software support

Multiple operative systems should be supported but updates could be downloaded by the AP itself which by Internet is able to access with a secure SSL connection to the OEM website dedicated page. The same service colud be used to download the firmware upgrades and security fixes.

5.2.5. Henry via bluetooth

Those mobile devices that could not support any of the previous way of authentication will go for a standard bluetooth pairing which will grant to them a temporarily and very limited clearance (less than GUEST/WHITE level of trust) in order to do initiate the procedure described for 3G connected devices.

5.2.6. Henry via WPS (or unencrypted Wi-Fi)

Those devices that support standard WPS could retrieve from the AP a temporarily and very limited clearance (less than GUEST/WHITE level of trust) in order to do initiate the procedure described for 3G connected devices. If the AP would have a valid CA signed certificate, it could be trusted directly.

6. DISCLAIMER

6.1. This document completeness

Document is not yet finished and probably it will never be because no one single person could describe in full a standard like this. For this reason the document has been released with Creative Common license that allow anybody to modify the document for any purposes as long as it would distribute with the same license and report the original document and author.

6.3 Collaboration

I am keen to collaborate with anyone interested in improve and extend this document or implement a proof-of-concept or a working access point. Feel free to contact me at roberto.foglietta@gmail.com

6.2 This protocol naming

If you are not happy about Henry and Sally naming, you could read Hand & Shake instead.

7. LICENSE

This document is released under the Attribution-ShareAlike 4.0 International

7.1 Summary of license terms

You are free to:

- **Share —** copy and redistribute the material in any medium or format
- **Adapt —** remix, transform, and build upon the material

for any purpose, even commercially as long as report the original work license and author.

The licensor cannot revoke these freedoms as long as you follow the license terms.

7.1 Full license text

Please refer to the following link to retrieve the full license text

http://creativecommons.org/licenses/by-sa/4.0