Wifi Security

Aggelos Kiayias

WEP

- WEP = “wired equivalent privacy”
- Sender : A device with wireless capability.
- Receiver : Access point.
- A shared secret-key is used for encryption and integrity.

WEP communication

- Sending a message *m* : involves computing a checksum *t* on *m*, select an IV *r*, generate a key-stream s=*RC4(r,k)*, and compute c = (*m*||*t*) *xor s*. Transmit *r*||*c*
- Receiving a message : parse input as *r*||*c*, compute, *s*=*RC4(r,k)*, *m*||*t* = *c xor s*, test checksum t, output *m*.

RC4

Array S has a permutation on 256 elements, selected by the key.

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

Attacks

- Fluhrer, Martin, Shamir (2001). 4M-5M packets needed.
- KoreK (2004). 700K packets needed.
- Tews, Weinmann, Pyshkin, (2007) 35K-40K packets.

http://dl.aircrack-ng.org/breakingwepandwpa.pdf

WPS protocol

- “Wi-fi protected setup.”
- protocol for automated configuration of wireless networks.
- Attack from Brute forcing Wi-Fi Protected Setup, Stefan Viehböck

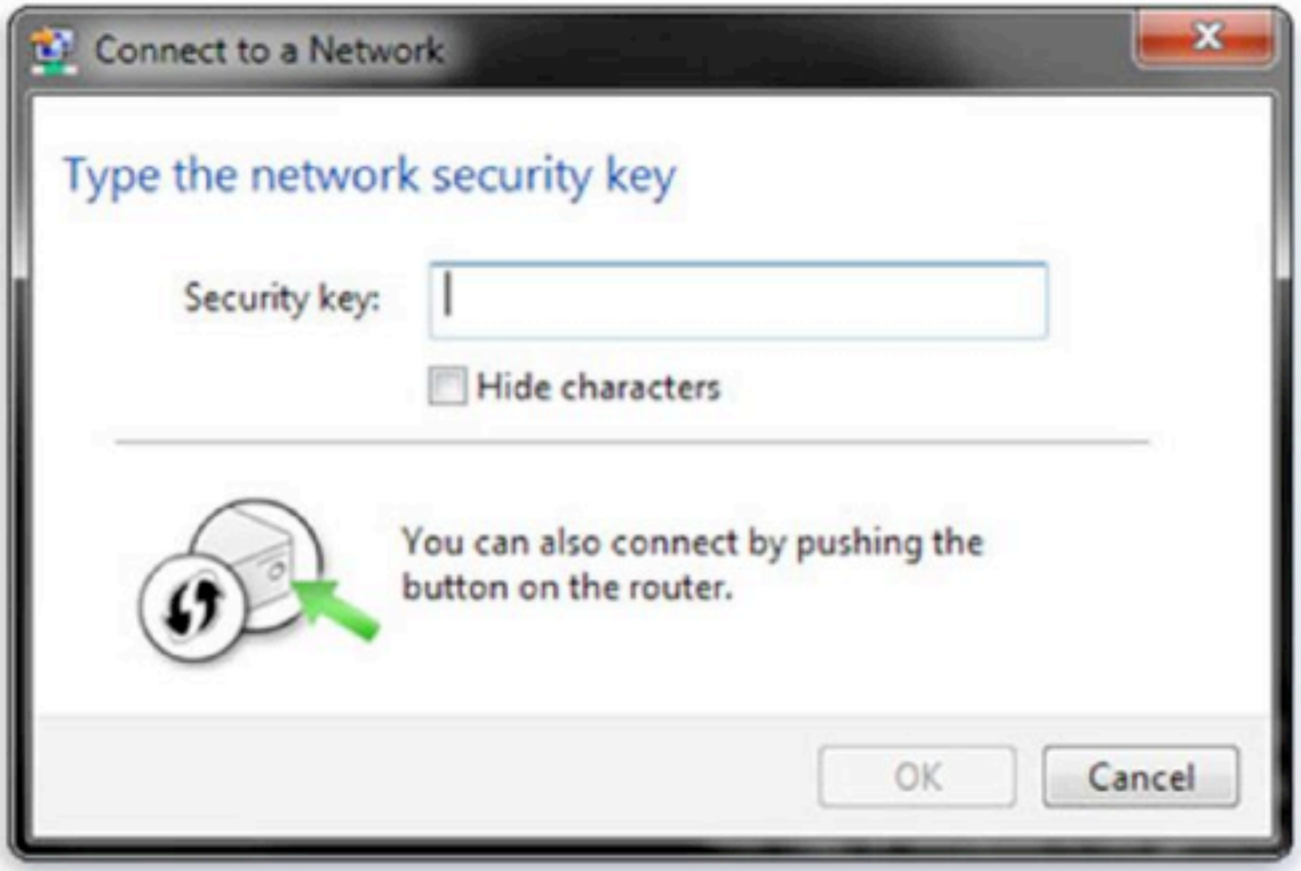
http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

WPS terminology

- Enrollee : wireless device that does not have settings for the wireless network.
- Registrar: provides wireless settings to enrollee.
- Access point: provides normal wireless network hosting.

Method 1

- User pushes a button on the access point.



Connect to a Network

Type the network security key

Security key:

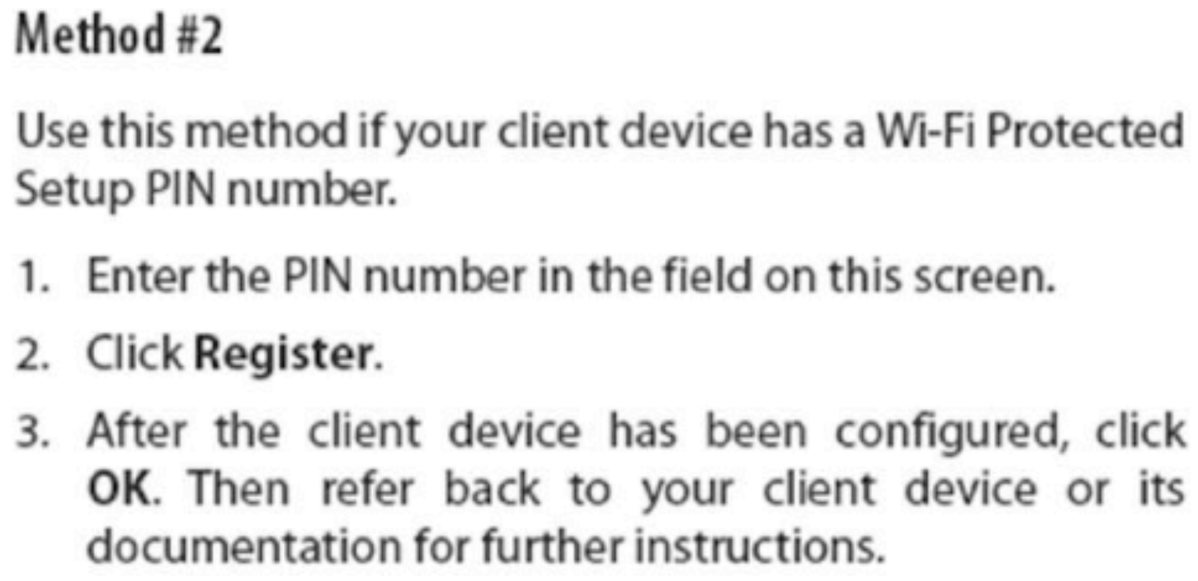
□ Hide characters

You can also connect by pushing the button on the router.

Firgure 1: activated "virtual Push Button" (Windows acts as enrollee) (Windows 7)

Method 2

- The user has to enter a PIN into the interface of the access point.

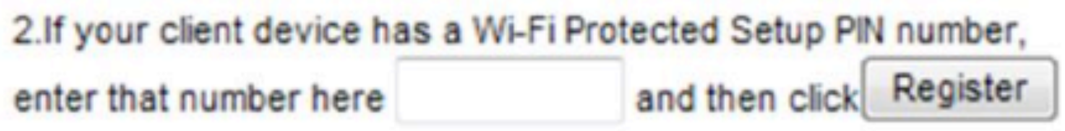


Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number in the field on this screen.
2. Click **Register**.
3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

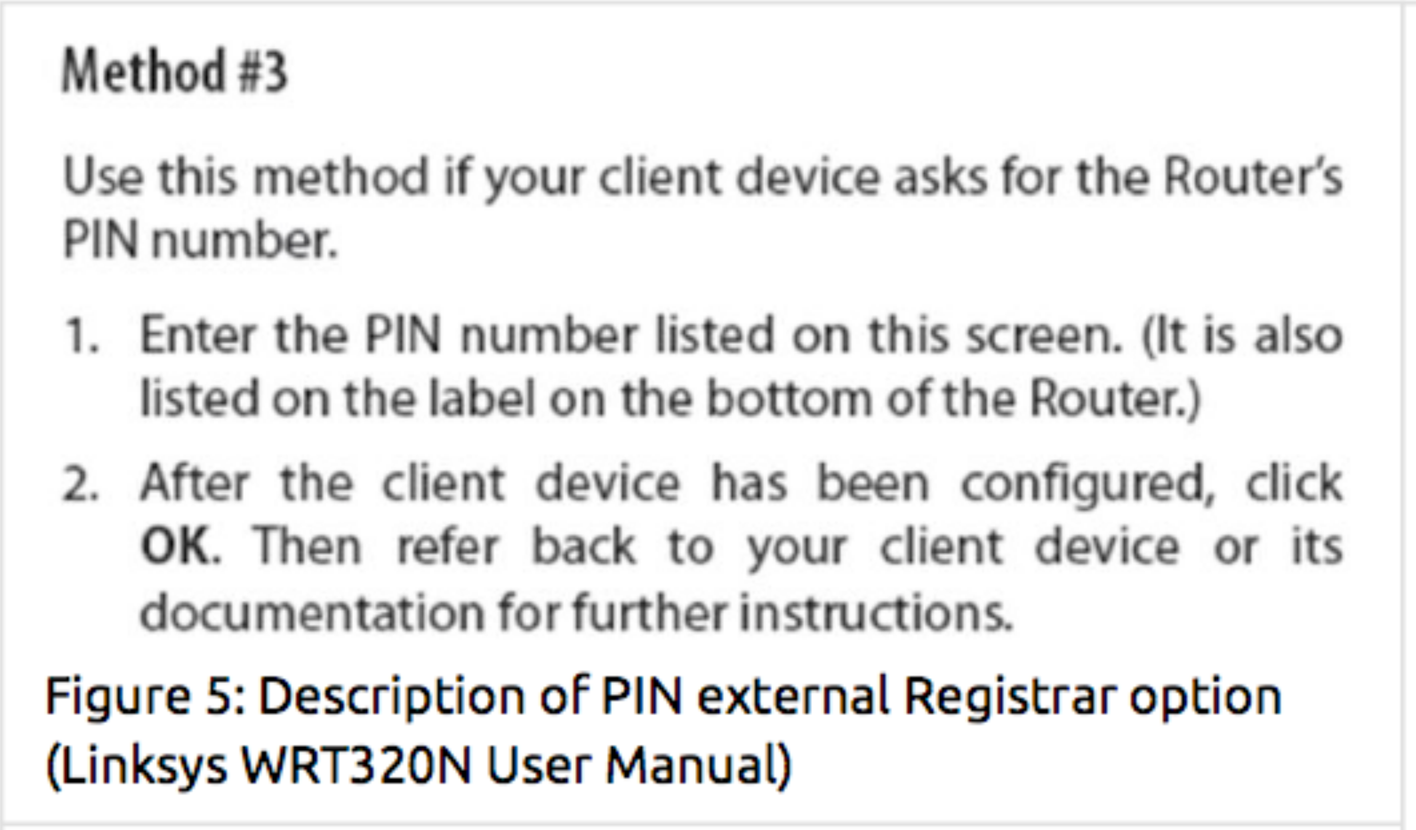
Figure 3: Description of PIN internal Registrar option (Linksys WRT320N User Manual)



2.If your client device has a Wi-Fi Protected Setup PIN number, enter that number here ______ and then click Register

Figure 4: PIN field – Router is Registrar (Linksys WRT320N Web Interface)

Method 3

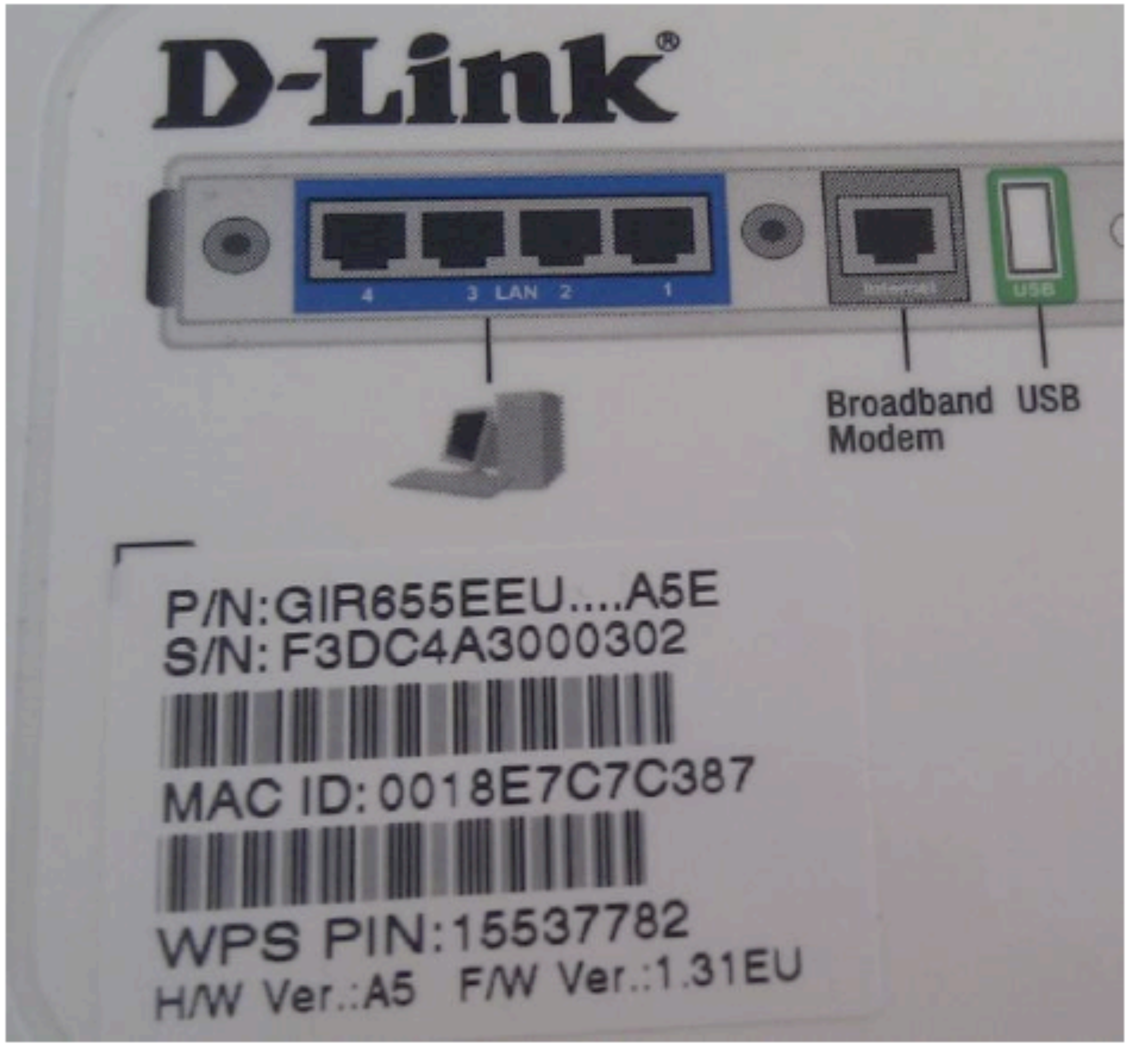


Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

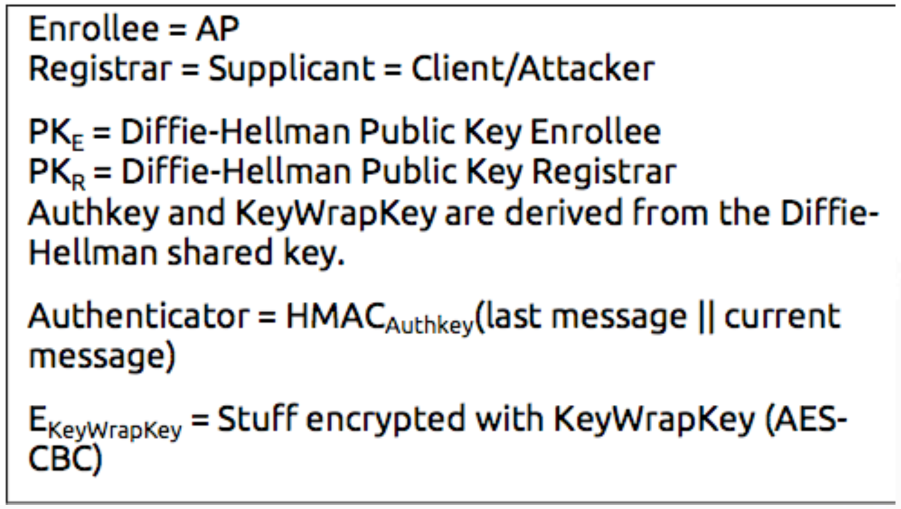
Figure 5: Description of PIN external Registrar option (Linksys WRT320N User Manual)



Potential issue

- Method 3 might be vulnerable.
- it requires no authentication whatsoever beyond the PIN (the other two : 1. require physical access, 2. web-interface access).
- The device plays the role of the registrar in the WPS protocol.

Protocol Description

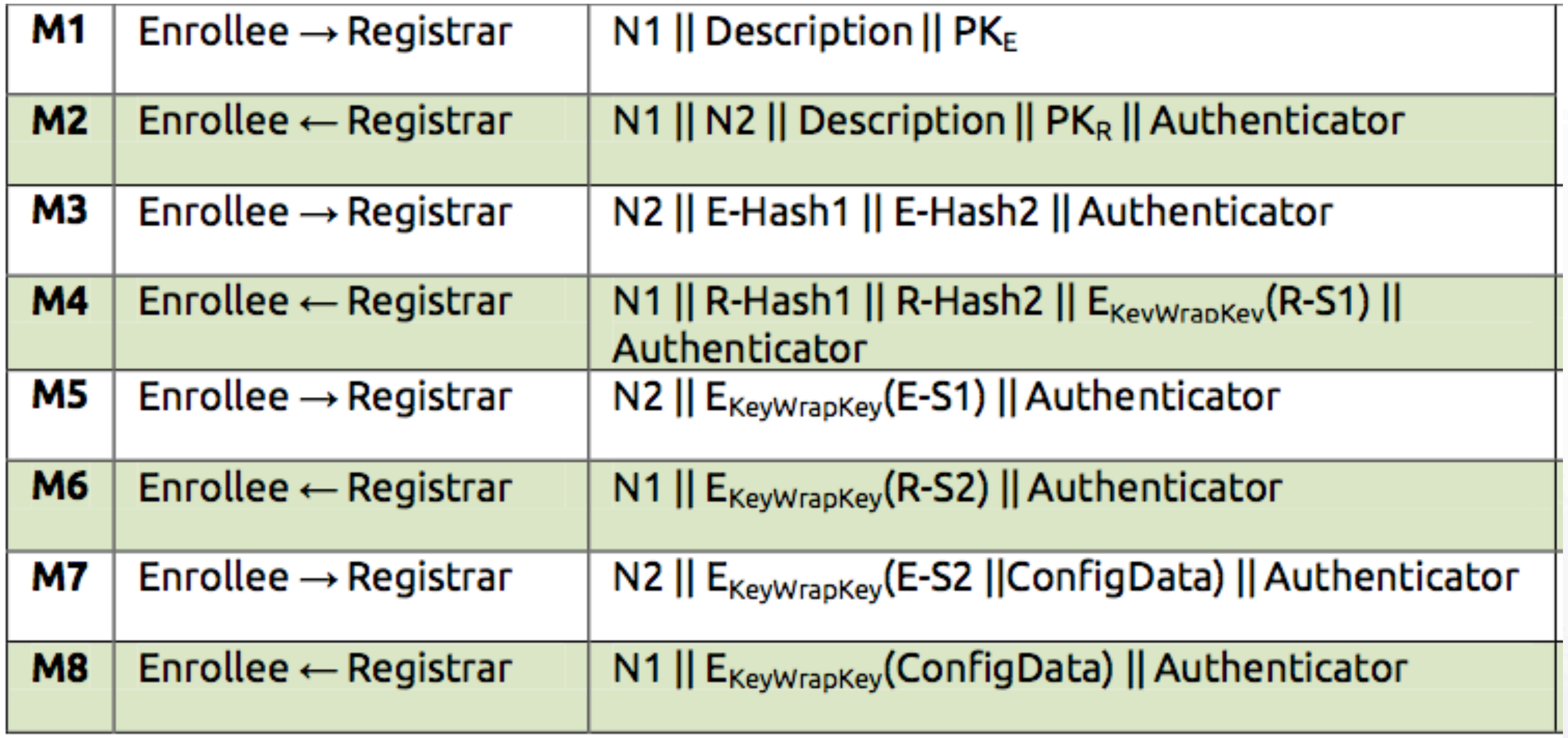


Enrollee = AP
Registrar = Supplicant = Client/Attacker

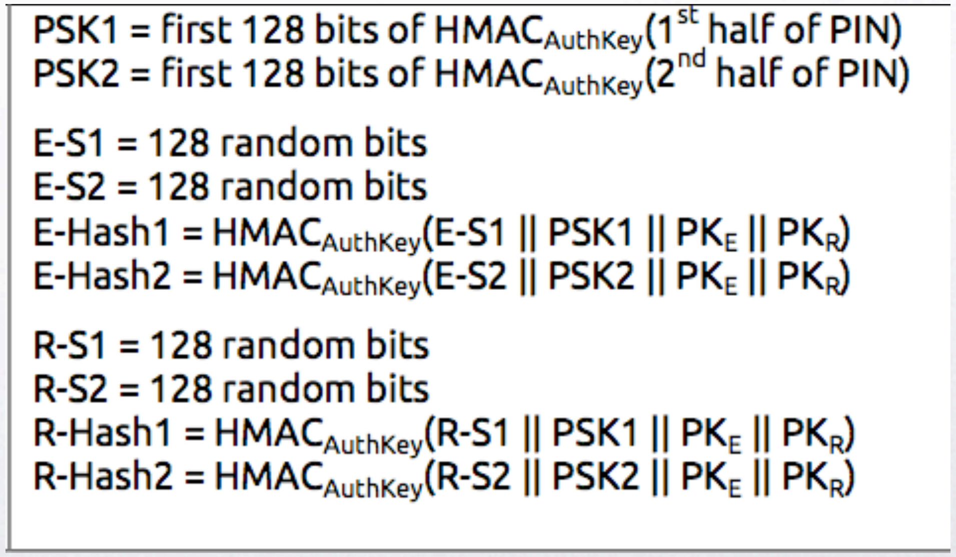
PK_E = Diffie-Hellman Public Key Enrollee
PK_R = Diffie-Hellman Public Key Registrar
Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.

Authenticator = $HMAC_{Authkey}$(last message || current message)

$E_{KeyWrapKey}$ = Stuff encrypted with KeyWrapKey (AES-CBC)



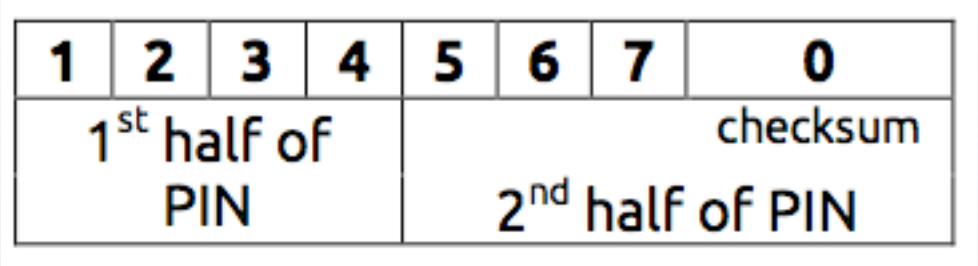
M1	Enrollee → Registrar	N1 || Description || PK_E
M2	Enrollee ← Registrar	N1 || N2 || Description || PK_R || Authenticator
M3	Enrollee → Registrar	N2 || E-Hash1 || E-Hash2 || Authenticator
M4	Enrollee ← Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KeyWrapKey}$(R-S1) || Authenticator
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator



PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of PIN)
PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)

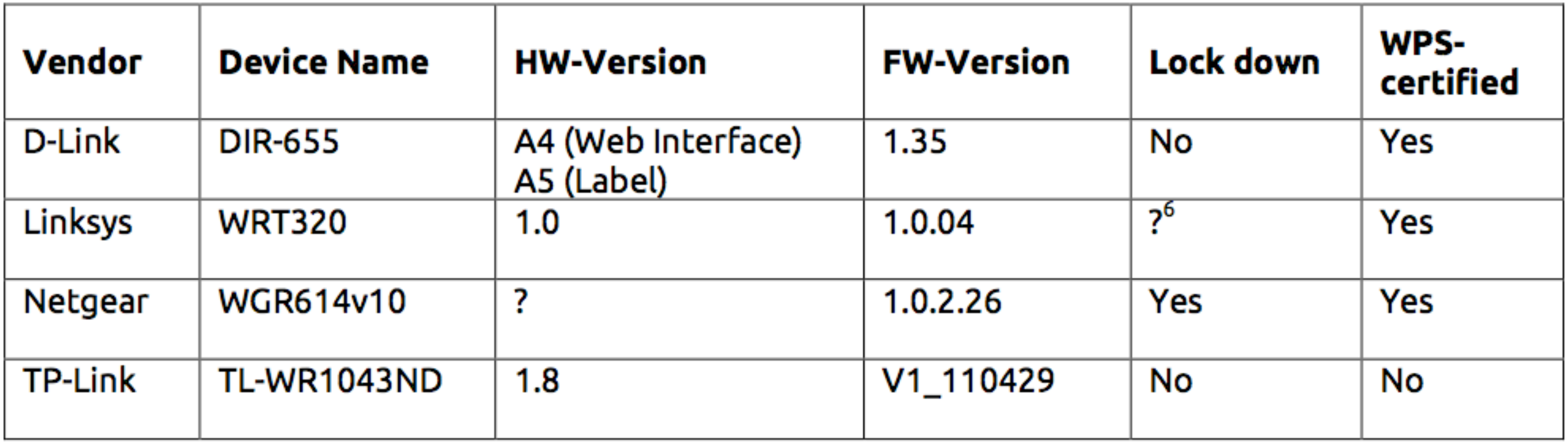
E-S1 = 128 random bits
E-S2 = 128 random bits
E-Hash1 = $HMAC_{AuthKey}$(E-S1 || PSK1 || PK_E || PK_R)
E-Hash2 = $HMAC_{AuthKey}$(E-S2 || PSK2 || PK_E || PK_R)

R-S1 = 128 random bits
R-S2 = 128 random bits
R-Hash1 = $HMAC_{AuthKey}$(R-S1 || PSK1 || PK_E || PK_R)
R-Hash2 = $HMAC_{AuthKey}$(R-S2 || PSK2 || PK_E || PK_R)

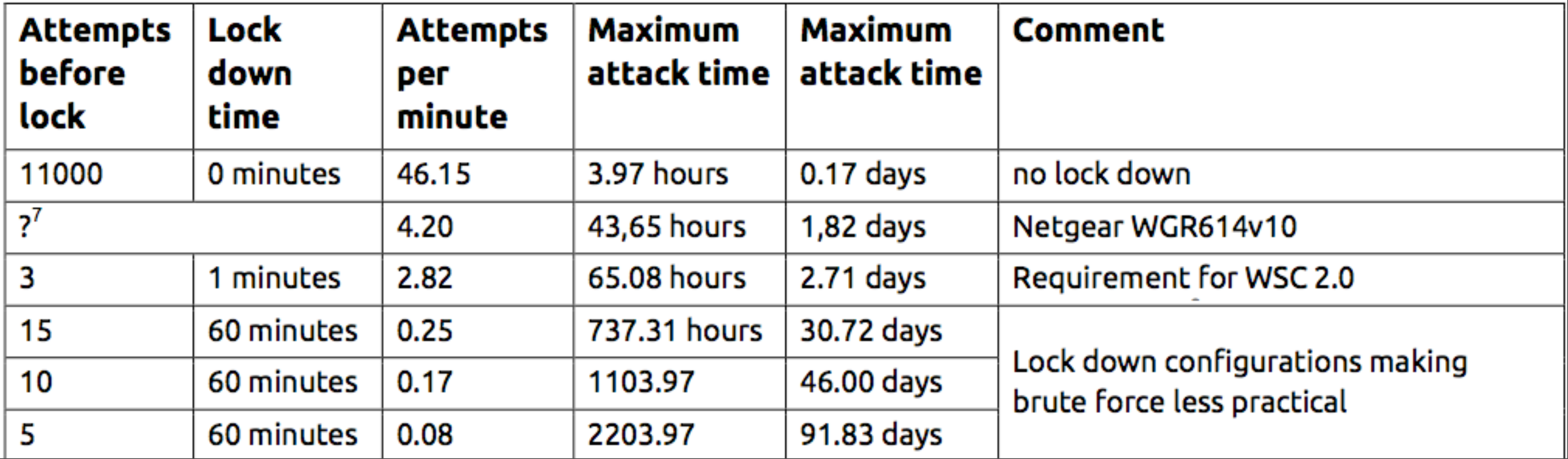


1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

Results



Vendor	Device Name	HW-Version	FW-Version	Lock down	WPS-certified
D-Link	DIR-655	A4 (Web Interface) A5 (Label)	1.35	No	Yes
Linksys	WRT320	1.0	1.0.04	?[6]	Yes
Netgear	WGR614v10	?	1.0.2.26	Yes	Yes
TP-Link	TL-WR1043ND	1.8	V1_110429	No	No



Attempts before lock	Lock down time	Attempts per minute	Maximum attack time	Maximum attack time	Comment
11000	0 minutes	46.15	3.97 hours	0.17 days	no lock down
?[7]		4.20	43,65 hours	1,82 days	Netgear WGR614v10
3	1 minutes	2.82	65.08 hours	2.71 days	Requirement for WSC 2.0
15	60 minutes	0.25	737.31 hours	30.72 days	Lock down configurations making brute force less practical
10	60 minutes	0.17	1103.97	46.00 days	
5	60 minutes	0.08	2203.97	91.83 days	