Talking to Strangers: Authentication in Ad-Hoc Wireless Networks

Dirk Balfanz
D.K. Smetters
Paul Stewart
H. Chi Wong

Overview

- Introduction to the applicable areas
- Some terms to be used
- Interactive Guy Fawkes Protocol
- Conclusion

Introduction

Imagine a scenario where you enter an airport lounge and would like to use the wireless printer set up there by some company.

Your options would be to –

- Plug your mobile device to the printer using a cable (if possible)
- Use the power of wireless devices

3

Introduction

The paper is meant for the people who would like to use the latter option ☺

What needs to be done to use the available resource (printer in this case)?

- Need to somehow learn who to communicate with
- Exchange a key (in case encryption is required)

4

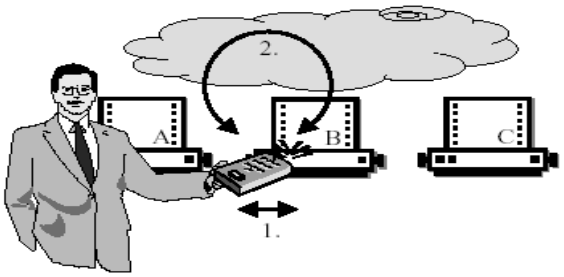
Introduction to 'The Scheme'

The stages to the proposed scheme are –

1. Pre-Authentication
2. Authentication over the Wireless Network
3. Communication

5

Terms to be used



The first stage is called *Pre-Authentication* – Here the person walks over to the device he wishes to communicate with and *touches* it.

Data is exchanged during this *touch*.
This physical contact is termed as a *Location Limited Channel .*

6

Moving on…

A contribution of this paper removes the requirement of the *pre-authentication data* to be *secret .* It doesn't need to be secret.

This is done by the use of verification data instead of identity-proving data.

7

… and on…

In a world where PKI was all set up we could use –

Pre-authentication, taking place over the location-limited channel:

1. $A \rightarrow B: \quad addr_A, h(PK_A)$
2. $B \rightarrow A: \quad addr_B, h(PK_B)$

Authentication continues over the wireless channel with any standard key exchange protocol, *e.g.*, SSL/TLS:

1. $A \rightarrow B: \quad TLS\_CLIENT\_HELLO$

...and so on.

8

... and on ...

NOTE – A device that does not receive pre-authentication data from its peer will be vulnerable to impersonation

The same scheme could be used for devices which do not wish to employ the overhead of PKI

They would use –

Pre-authentication, taking place over the location limited channel:

1. $A \rightarrow B: \quad addr_A,\ h(PK_A)$
2. $B \rightarrow A: \quad addr_B,\ h(S_B)$

Authentication continues over the wireless channel, *e.g.*:

1. $A \rightarrow B: \quad PK_A$
2. $B \rightarrow A: \quad E_{PK_A}(S_B)$

...and so on.

Interactive Guy Fawkes Protocol

This is a scheme that does not use PKI and so is efficient in usage. It does not carry the overhead of encryption / decryption using PKI

It does not provide privacy of data but does provide integrity protection and authentication

Interactive Guy Fawkes Protocol

The first stage is that of Pre-Authentication over a Location Limited Channel –

Pre-authentication, taking place over the location-limited channel:

Round 0:

1. $A \rightarrow B: \quad a_1 = h(\underline{A_1}, h(X_2), X_1),\ h(X_1)$
2. $B \rightarrow A: \quad b_1 = h(\underline{B_1}, h(Y_2), Y_1),\ h(Y_1)$
3. $A \rightarrow B: \quad h(b_1, X_1)$
4. $B \rightarrow A: \quad h(a_1, Y_1)$

Interactive Guy Fawkes Protocol

Then starts the Wireless communication (including the authentication at every stage) –

Round 0 occurs in the location limited channel (only here for reference)

Round 0:

1. $A \rightarrow B: \quad a_1 = h(\underline{A_1}, h(X_2), X_1),\ h(X_1)$
2. $B \rightarrow A: \quad b_1 = h(\underline{B_1}, h(Y_2), Y_1),\ h(Y_1)$
3. $A \rightarrow B: \quad h(b_1, X_1)$
4. $B \rightarrow A: \quad h(a_1, Y_1)$

Round 1:

1. $A \rightarrow B: \quad \underline{A_1},\ h(X_2),\ X_1,\ a_2 = h(A_2, h(X_3), X_2)$
2. $B \rightarrow A: \quad \underline{B_1},\ h(Y_2),\ Y_1,\ b_2 = h(\underline{B_2}, h(Y_3), Y_2)$
3. $A \rightarrow B: \quad h(b_2, X_2)$
4. $B \rightarrow A: \quad h(a_2, Y_2)$

Round 2:

5. $A \rightarrow B: \quad A_2,\ h(X_3),\ X_2,\ a_3 = h(A_3, h(X_4), X_3)$
6. $B \rightarrow A: \quad \underline{B_2},\ h(Y_3),\ Y_2,\ b_3 = h(B_3, h(Y_4), Y_3)$
7. $A \rightarrow B: \quad h(b_3, X_3)$
8. $B \rightarrow A: \quad h(a_3, Y_3)$

Round 3:

9. $A \rightarrow B: \quad A_3,\ h(X_4),\ X_3,\ a_4 = h(\underline{A_4}, h(X_5), X_4)$
10. $B \rightarrow A: \quad B_3,\ h(Y_4),\ Y_3,\ b_4 = h(B_4, h(Y_5), Y_4)$
11. $A \rightarrow B: \quad h(b_4, X_4)$
12. $B \rightarrow A: \quad h(a_4, Y_4)$

Interactive Guy Fawkes Protocol

The outcome of the protocol is an authenticated channel between two parties.

For secrecy the device should use the previous scheme where PKI was used.

This demands a computational overhead.

13

Conclusion

- A scheme was developed to authenticate data in situations without a demand for secrecy
- The reliance on PKI was dropped
- A scheme was suggested where the use of PKI could protect data from being exposed to third-parties

14