NC STATE UNIVERSITY Computer Science

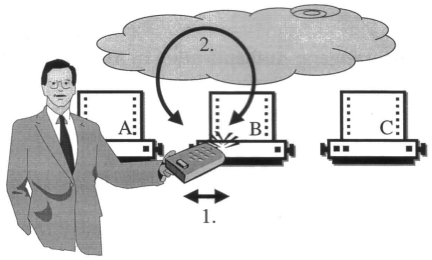
Talking to Strangers

Authentication in Ad-Hoc Wireless Networks

Outline

- Introduction
- Related Works
- Preliminaries
- Two-Party Protocols
- Group Key Exchange Protocols
- Conclusion and Future Work

Introduction



- Problem
  - Securely and Authentically Communicate with *the* Device
- Certificate Authority?
  - Public Key Infrastructure – Impractical & Expensive
  - Finding the Device Name – Not Reliable
  - Universal Naming Scheme – Not User-Friendly

Related Work

- Out-of-Band Authentication
  - Phone, Mail, Face-to-Face
- Bluetooth and WEP
  - PIN and Link Layer Security
- Resurrecting Duckling Security Model
  - Master/Slave (Mother/Duckling)

Preliminaries

- Location-Limited Channels
- Public Key Cryptography
- Pre-Authentication

Location-Limited Channels

- Used for Pre-Authentication
- Properties
  - Support Demonstrative Identification
    - Based on Physical Context
  - Authenticity
    - Protect from Potential Active Attackers
  - No Secrecy
    - Resistant to Eavesdropping
- Physical Media:
  - Contact, Infrared, Sound, etc.

Public Key Cryptography

- Remove Secrecy Requirement
  - Secure Against Passive Attacks
  - Active Attacks Are Easily Detectable
- Use of Hash Functions

Pre-Authentication

- Initial Step
  - Over Location-Limited Channels
- General Methods/Any Key Exchange Protocol
  - e.g. Exchange Public Keys
- Use Hash For Efficiency
  - e.g. Exchange Digest of Public Keys

Two-Party Protocols

- Basic Protocol
  - Public Key Operations at Both Ends
- Single Public Key Protocol
  - Public Key Operations at Single End
- Interactive Guy Fawkes Protocol
  - Hash Functions
  - Integrity, But No Secrecy

Basic Protocol

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

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

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

1. $A \rightarrow B$: TLS_CLIENT_HELLO

...and so on.

The various symbols denote:

$addr_A$, $addr_B$:	A's (resp. B's) address in wireless space, provided strictly for convenience
PK_A, PK_B :	the public key belonging to A (resp. B), either a long-lived key or an ephemeral key used only in this exchange
$h(PK_A)$:	a commitment to PK_A, *e.g.,* a one-way hash of an encoding of the key

Single Public Key Protocol

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

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

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

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

...and so on.

Symbols as above, with the following additions:

S_B :	a secret belonging to B
$h(S_B)$:	a commitment to S_B, *e.g.*, a one-way hash of the secret
$E_{PK_A}(S_B)$:	the encryption of S_B under PK_A

Interactive Guy Fawkes Protocol

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

Round 0:	1.	$A \rightarrow B$:	$a_1 = h(\underline{A_1}, h(X_2), X_1)$, $h(X_1)$
	2.	$B \rightarrow A$:	$b_1 = h(\underline{B_1}, h(Y_2), Y_1)$, $h(Y_1)$
	3.	$A \rightarrow B$:	$h(b_1, X_1)$
	4.	$B \rightarrow A$:	$h(a_1, Y_1)$

Authentication continues over the wireless channel:

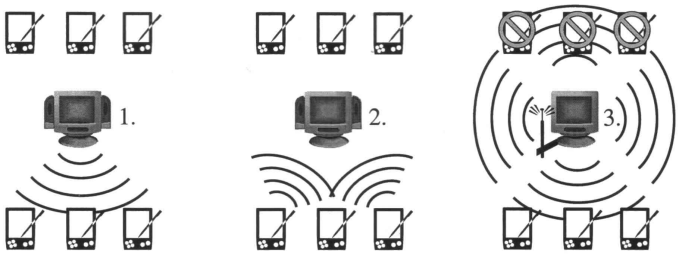
Round 1:	1.	$A \rightarrow B$:	$\underline{A_1}$, $h(X_2)$, X_1, $a_2 = h(A_2, h(X_3), X_2)$
	2.	$B \rightarrow A$:	$\underline{B_1}$, $h(Y_2)$, Y_1, $b_2 = h(\underline{B_2}, h(Y_3), Y_2)$
	3.	$A \rightarrow B$:	$h(b_2, X_2)$
	4.	$B \rightarrow A$:	$h(a_2, Y_2)$
Round 2:	5.	$A \rightarrow B$:	A_2, $h(X_3)$, X_2, $a_3 = h(A_3, h(X_4), X_3)$
	6.	$B \rightarrow A$:	$\underline{B_2}$, $h(Y_3)$, Y_2, $b_3 = h(B_3, h(Y_4), Y_3)$
	7.	$A \rightarrow B$:	$h(b_3, X_3)$
	8.	$B \rightarrow A$:	$h(a_3, Y_3)$

...and so on.

The various symbols denote:

X_i, Y_i :	randomly generated data, used as authenticators
$h(Z_1, \ldots, Z_n)$:	a one-way hash on the concatenation of values $Z_1, \ldots, Z_n$
A_i, B_i :	Meaningless random message from A (resp. B) at round i
$\underline{A_i}, \underline{B_i}$:	Meaninful message from A (resp. B) at round i
a_i, b_i :	the commitment from A (resp.B) for round i

Group Key Exchange Protocols



- Centrally Managed Groups
- Unmanaged Groups

Centrally Managed Groups

First, the key manager broadcasts its pre-authentication data over the location-limited channel:

1. $KM \xrightarrow{b}$ group : $addr_{KM}$, $h(PK_{KM})$

Then, group members send their pre-authentication data:

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

...

The protocol continues over the wireless channel with any standard point-to-point key exchange protocol, *e.g.*:

1. $A \rightarrow KM$: *TLS_CLIENT_HELLO*
2. $B \rightarrow KM$: *TLS_CLIENT_HELLO*

...and so on; once connection is established the KM gives the appropriate multicast keys to every group member.

The various symbols denote:

$addr_A$, $addr_{KM}$:	A's (resp. KM's) address in wireless space, provided strictly for convenience
PK_A, PK_{KM} :	the public key belonging to A (resp. B), either a long-lived key or an ephemeral key used only in this exchange
$h(PK_A)$:	a commitment to PK_A, *e.g.*, a one-way hash of an encoding of the key
$\xrightarrow{b}$:	message broadcast

Centrally Managed Groups - Problems

- Single Point of Attack
- Compatibility with Trusted GM
- GM Leaving the Group

Unmanaged Groups

Each member broadcasts its pre-authentication data over the location-limited channel:

1. $A \xrightarrow{b}$ group : $addr_A, h(PK_A)$
2. $B \xrightarrow{b}$ group : $addr_B, h(PK_B)$

...

Participants exchange authenticated Diffie-Hellman public values over the wireless channel:

1. $A \xrightarrow{b}$ group : A, PK_A
2. $B \xrightarrow{b}$ group : B, PK_B

...

Participants continue with their chosen protocol to derive a shared secret key K:

1. $A \rightarrow B$: $PROTOCOL\_MSG\_1_{A,B}$
1. $B \rightarrow C$: $PROTOCOL\_MSG\_1_{B,C}$

...

The various symbols are as in Figure 6; the public keys PK_A, *etc.* are Diffie-Hellman public values.

Conclusions

- Use of Location-Limited Channels
- Novel Location-Limited Channels
- Concrete Pre-Authentication Protocols
- Group Communication
- No Reliance on PKI

Future Works

- Physical Media for Location-Limited Channels
  - Discover New Media
  - Determine Optimal Media
    - For Two-Party
    - For Group
- Determine Any Vulnerabilities & Fixes
- Further Implementation Development
  - Constructing Contact-Mediated Interface
  - Expand to Group Authentication w/ Audio

Questions & Comments