User-Assisted Secure Association of Wireless Devices*

Nitesh Saxena
Polytechnic Institute of NYU
(*formerly* Polytechnic University)

Joint work with:

Ramnath Prasad, Arun Kumar, Borhan Uddin, Jonathan Voris (NYU-Poly)
Stanislaw Jarecki, Gene Tsudik, Ersin Uzun (UC Irvine)
N. Asokan (Nokia Research)

*Funded by NSF Cybertrust

The Problem: "Pairing"

Audio; Visual; Tactile

Goal: To bootstrap secure communication between Alice's and Bob's devices when they have

- no prior context
- no common trusted CA or TTP

Idea: make use of a physical channel between devices

- with least involvement from Alice and Bob

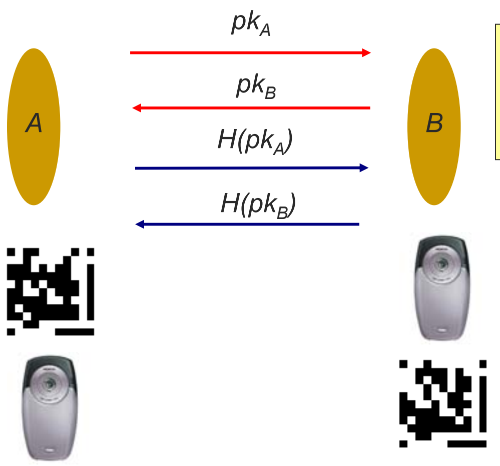
Examples (single user setting)

- Pairing a bluetooth cell phone with a headset
- Pairing a WiFi laptop with an access point

Seeing-is-Believing (McCune et al. [Oakland'05])

- Protocol (Balfanz, et al. [NDSS'02])

⟷ Insecure Channel
⟷ Authenticated Channel



pk_A

pk_B

$H(pk_A)$

$H(pk_B)$

A

B

- Secure if
  - H(.) weak CR
- 80-bit for permanent
- 48-bit for ephemeral

Rohs, Gfeller
[PervComp'04]

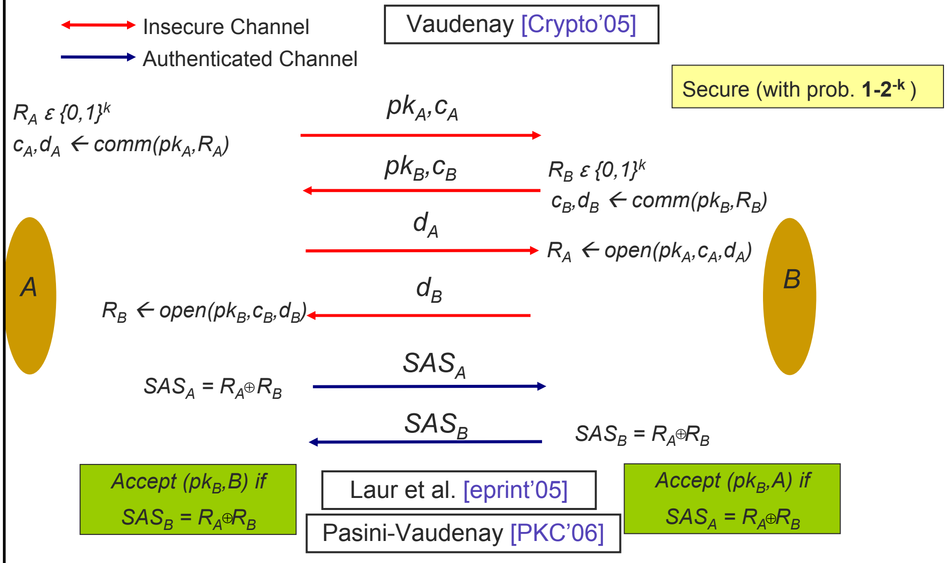
Challenges

- OOB channels are low-bandwidth!
- One of the device might not have a receiver!
- Neither has a receiver and only one has a good quality transmitter
  - (Non-)Universality!
- Protocols might be slow – multiple executions!
- Multiple devices – scalability!

Challenges

- OOB channels are low-bandwidth!
- One of the device might not have a receiver!
- Neither has a receiver and only one has a good quality transmitter
  - (Non-)Universality!
- Protocols might be slow – multiple executions!
- Multiple devices -- scalability

Protocol: **S**hort **A**uthenticated **S**trings (SAS)



Insecure Channel

Authenticated Channel

Vaudenay [Crypto'05]

Secure (with prob. **$1-2^{-k}$**)

R_A ε $\{0,1\}^k$

$c_A, d_A \leftarrow comm(pk_A, R_A)$

pk_A, c_A

pk_B, c_B

R_B ε $\{0,1\}^k$

$c_B, d_B \leftarrow comm(pk_B, R_B)$

d_A

$R_A \leftarrow open(pk_A, c_A, d_A)$

d_B

$R_B \leftarrow open(pk_B, c_B, d_B)$

SAS_A

$SAS_A = R_A \oplus R_B$

SAS_B

$SAS_B = R_A \oplus R_B$

Accept (pk_B, B) if $SAS_B = R_A \oplus R_B$

Accept (pk_B, A) if $SAS_A = R_A \oplus R_B$

Laur et al. [eprint'05]

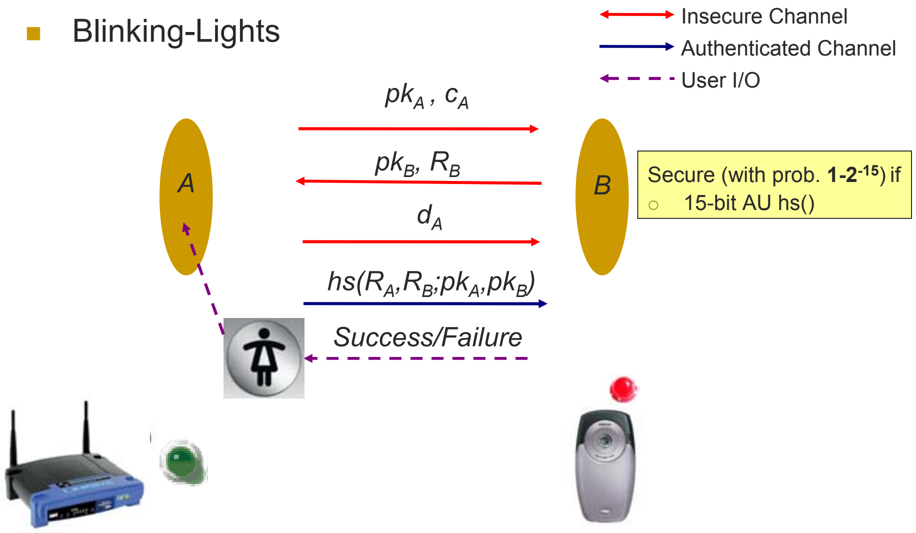
Pasini-Vaudenay [PKC'06]

Challenges

- OOB channels are low-bandwidth!
- One of the devices might not have a receiver!
  - e.g., keyboard-desktop; AP-phone
- Neither has a receiver and only one has a good quality transmitter
  - (Non-)Universality!
- Protocols might be slow – multiple executions!
- Multiple devices -- scalability

Unidirectional SAS (Saxena et al. [S&P'06])

- Blinking-Lights



Secure (with prob. **$1\text{-}2^{-15}$**) if
- 15-bit AU hs()

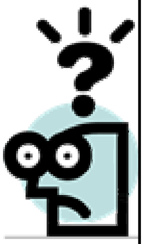
Multiple Blinking LEDs (Saxena-Uddin [ICICS'08])

Challenges

- OOB channels are low-bandwidth!
- One of the device might not have a receiver!
- Neither has a receiver and only one has a good quality transmitter
  - e.g., AP-laptop/PDA
- Protocols might be slow – multiple executions!
- Multiple devices -- scalability

Drawbacks with Prior Research

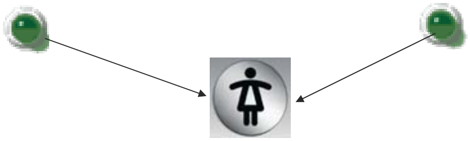
- Geared for specific pairing scenario
- None are universally applicable
  - Require hardware and interfaces not common across all devices
- User doesn't know what method to use on what pair of devices ➔ confusion!



- We believe: universality would immensely improve security as well as usability

A Universal Pairing Method

- Prasad-Saxena [ACNS'08]
- Use existing SAS protocols
- The strings transmitted by both devices over physical channel should be
  - the same, if everything is fine
  - different, if there is an attack/fault
- Both devices encode these strings using a pattern of
  - Synchronized **beeping/blinking**
  - The user acts as a reader and verifies if the two patterns are same or not

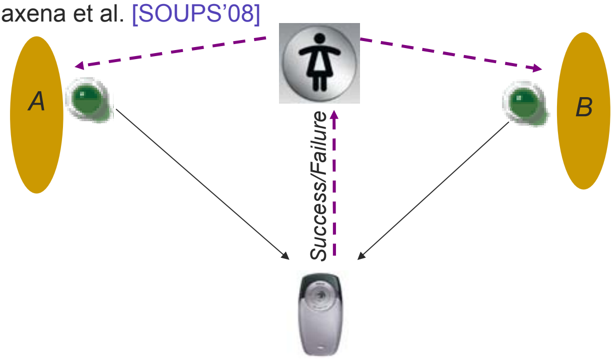


Is This Usable?

- Our test results are promising
  - Users can verify both good test cases and bad ones
- **Blink-Blink** the easiest
  - Very low errors (less than 5%)
  - Execution time ~22s
- Then, **Beep-Blink**
  - Very low errors with a learning instance (less than 5%)
  - Execution time ~15s
- **Beep-Beep** turns out error-prone

Further Improvement: Auxiliary Device

- Saxena et al. [SOUPS’08]



- Auxiliary device needs a camera and/or microphone – a smart phone
- Does not need to be trusted with cryptographic data
- Does not need to communicate with the devices

Further Improvement: Auxiliary Device

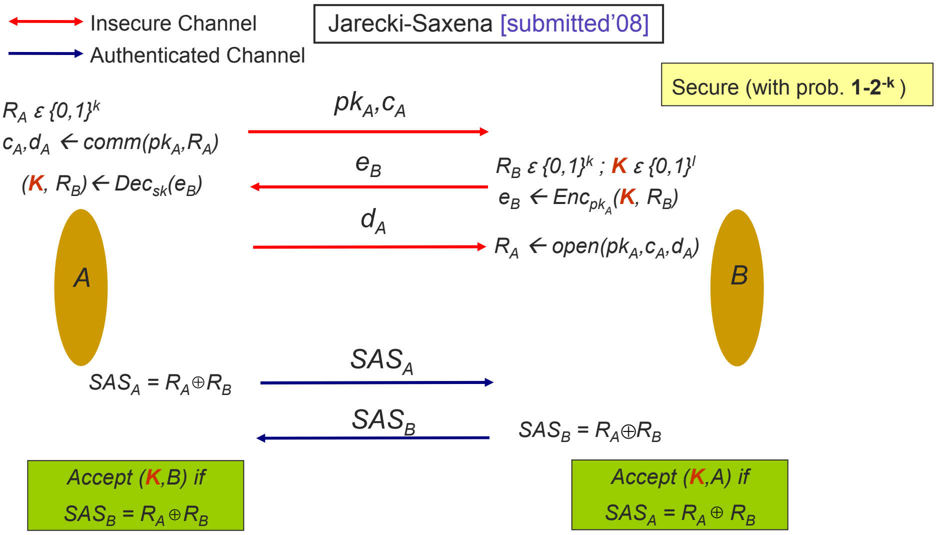
- **Blink-Blink**
  - ~14s (compared to 22s of manual scheme)
- **Beep-Blink**
  - Approximately takes as long as the same as manual scheme
  - No learning needed

- In both cases,
  - False negatives are eliminated
  - False positives are reduced
- It was preferred by most users

Challenges

- OOB channels are low-bandwidth!
- One of the device might not have a receiver!
- Neither has a receiver and only one has a good quality transmitter
  - (Non-)Universality!
- Protocols can be slow – multiple executions!
  - Key Re-use
- Multiple devices -- scalability

Encryption-based SAS protocol with **Key Re-use**



Insecure Channel

Authenticated Channel

Jarecki-Saxena [submitted'08]

Secure (with prob. **$1\text{-}2^{-k}$**)

R_A ε $\{0,1\}^k$

$c_A,d_A \leftarrow comm(pk_A,R_A)$

$(\mathbf{K}, R_B) \leftarrow Dec_{sk}(e_B)$

A

pk_A,c_A

e_B

d_A

R_B ε $\{0,1\}^k$; $\mathbf{K}$ ε $\{0,1\}^l$

$e_B \leftarrow Enc_{pk_A}(\mathbf{K}, R_B)$

$R_A \leftarrow open(pk_A,c_A,d_A)$

B

$SAS_A = R_A \oplus R_B$

SAS_A

SAS_B

$SAS_B = R_A \oplus R_B$

Accept ($\mathbf{K}$,B) if $SAS_B = R_A \oplus R_B$

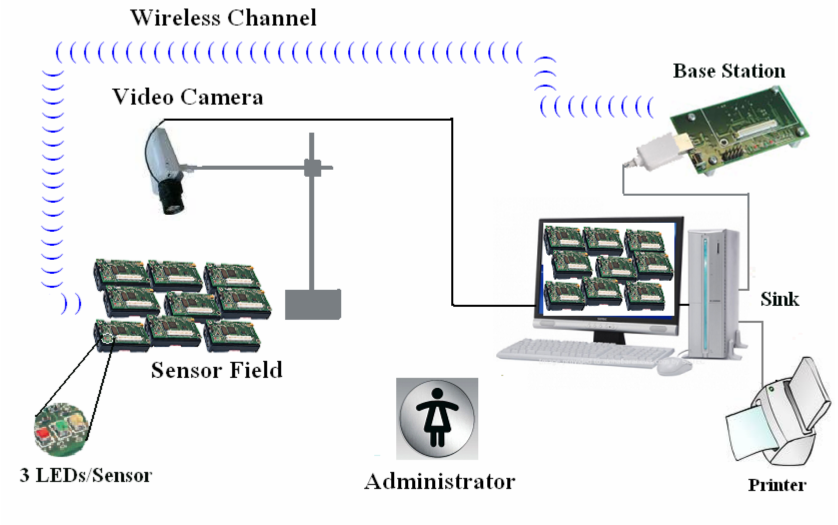
Accept ($\mathbf{K}$,A) if $SAS_A = R_A \oplus R_B$

Challenges

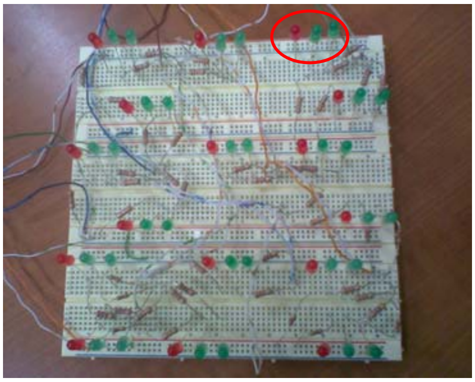
- OOB channels are low-bandwidth!
- One of the device might not have a receiver!
- Neither has a receiver and only one has a good quality transmitter
  - (Non-)Universality!
- [Usability!]
- Protocols might be slow – multiple executions!
- Multiple devices – scalability
  - Bootstrapping key pre-distribution on sensors

Sensor Network Initialization

Saxena-Uddin [Submitted'08]

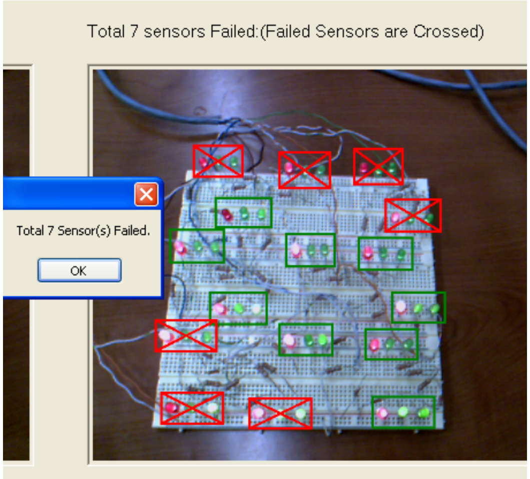


Sensor Network Initialization



16 sensors with three LEDs each

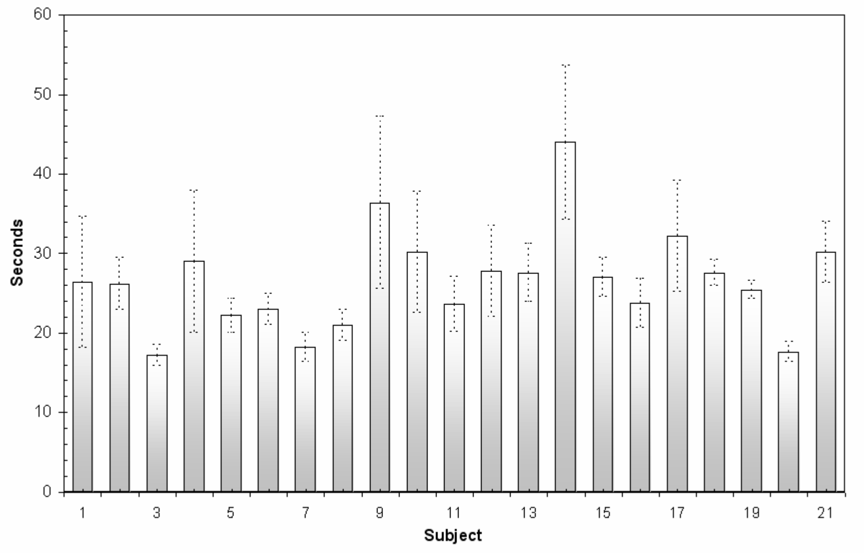
Sensor Network Initialization



Total 7 sensors Failed:(Failed Sensors are Crossed)

Total 7 Sensor(s) Failed.

Sensor Network Initialization



Future Work

- "Two-user" setting
- Group-setting
- Pairing RFIDs
- More usability tests

Papers: http://cis.poly.edu/~nsaxena

Thanks!