Seminar DCS

Col de Porte

9-10 June 2008

Day 1 : Monday 9 June 2008

- **9h-9h30 : Welcome**
- 9h30-10h30 : Thanh-Hung NGUYEN,
  Compositional verification for component-based systems and application
- 10h30-11h30 : Simon BLIUDZE,
  A notion of expressiveness for component-based systems
- 11h30-12h30 : Laurent MOUNIER,
  Modelling and analysis of WSNs
- **12h30-14h : Lunch**
- 14h-15h : Sylvain BOULME,
  Verification modulaire d'invariants
- 15h-16h : Radu IOSIF,
  What else is decidable about integer arrays?
- 16h-20h : Walk in the Chartreuse or Roumanie-France at 18h
- **20h : Diner**

Day 2 : Tuesday 10 June 2008

- 9h-10h : Yassine LAKHNECH,
  Towards a proof theory for cryptographic systems
- 10h-11h : Pascal LAFOURCADE,
  Neighbourhood problems in wireless communication
- **11h-11h30 : Pause**
- 11h30-12h30 : Jean-Franois MONIN, F91 en Coq
- **12h30-14h : Lunch**
- 14h-15h : Florent GARNIER,
  Terminaison en temps moyen fini de systmes de régles probabilistes
- 15h-15h30 : Jacques COMBAZ,
  A stochastic approach for fine grain QoS control
- 15h30-16h : Mohamad JABER,
  Using neural networks for quality management
- 16h-17h : Discussion

Neighbourhood problems in wireless communications

David Basin Srdjan Capkun Patrick Schaller
Pascal Lafourcade

Université de Grenoble, CNRS
VERIMAG

Col de Porte
June 10, 11, 2008

Wireless Everywhere

Recently

```
###################################################################
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)! It is also possible that the RSA host key has just been
 changed....
###################################################################
```

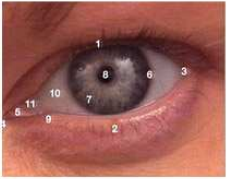
Recently

```
###################################################################
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)! It is also possible that the RSA host key has just been
 changed....
###################################################################
```

Due to a security flaw in a Debian package.

Might compromise the authentification mechanism of the system

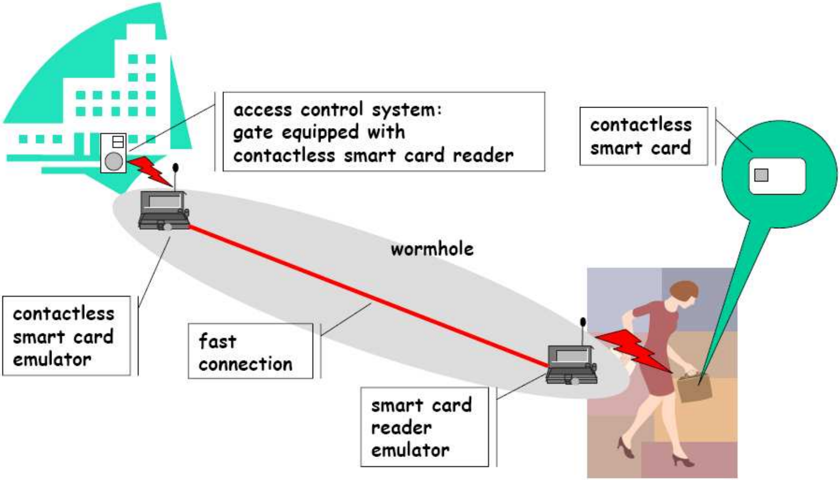
Mechanisms for Authentication

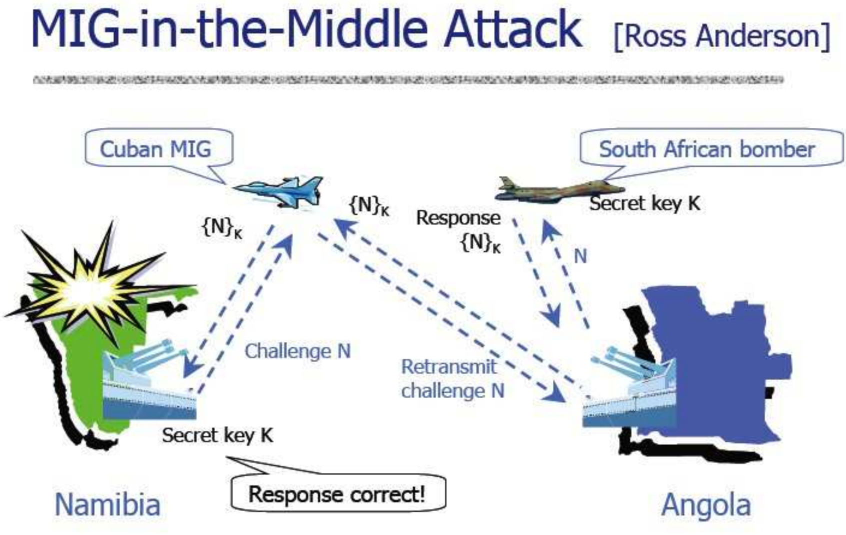


1. Something that you know
   E.g. a PIN or a password
2. Something that you have
   E.g. a smart-card
3. Something that you are
   Biometric characteristics like voice, fingerprints, eyes, ...
4. Where you are located
   E.g. in a secure building

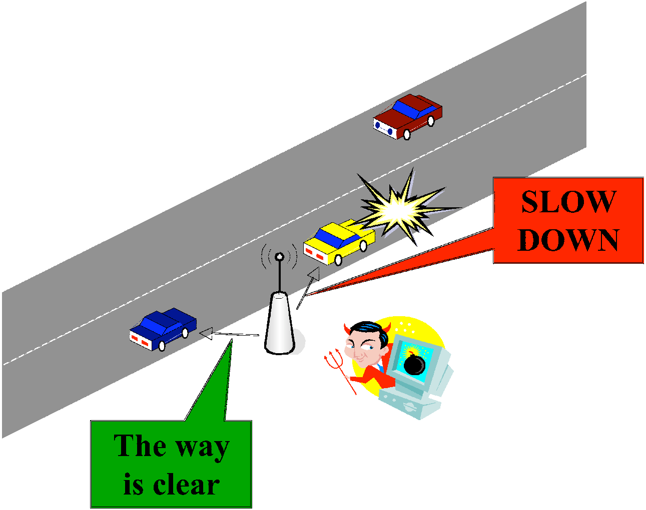
Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Authentication Problem: Wormhole Attack




MIG-in-the-Middle Attack [Ross Anderson]
Cuban MIG
South African bomber
$\{N\}_K$
$\{N\}_K$
Response $\{N\}_K$
Secret key K
N
Challenge N
Retransmit challenge N
Secret key K
Response correct!
Namibia
Angola

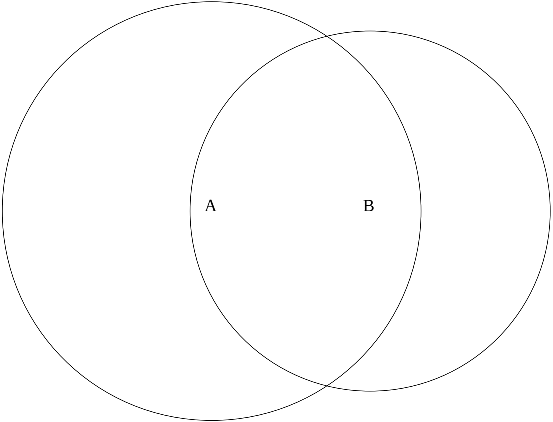
Vehicular Communicationn (Vanets)



Differents Authentication Notions due to Wireless

- **Entity Origin Authentication**: Sure to communicate with the good person (Usual achieved by Cryptographic Protocols)
- **Message Origin Authentication**: Sure the message has been generated by somebody (Signature)
- **Signal Origin Authentication**: Sure the signal has been forged by somebody

Signal Origin Authentication = Neighbourhood



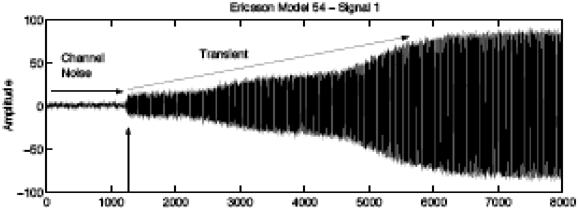
Guaranting that signal has been send by who is supposed to emit it.

Neighbourhood Discovery Protocol [Brands, Chaum'83]

P		**V**
$m_i \in_R \{0,1\}$		$\alpha_i \in_R \{0,1\}$
	$\xrightarrow{commit(m_1\|...\|m_k)}$	
	Start of rapid bit exchange	
	$\xleftarrow{\alpha_i}$	
$\beta_i \leftarrow \beta_i \oplus m_i$		
	$\xrightarrow{\beta_i}$	
	End of rapid bit exchange	
$m \leftarrow \alpha_1\|\beta_1\|\ldots\|\alpha_k\|\beta_k$		
	$\xrightarrow{(opencommit),sign(m)}$	
		Verify commit $m \leftarrow \alpha_1\|\beta_1\|\ldots\|\alpha_k\|\beta_k$ Verify $sign(m)$

Example: Radio Finger Printing [Capkun and al.'07]

Each Radio Device has is own Finger Printing



Using this physical properties ⇒ Signal Origin Authentication.

Outline

1. Introduction
2. Formal Analysis of Signal Origin Authentication
3. Conclusion

Outline

1. Introduction

2. Formal Analysis of Signal Origin Authentication

3. Conclusion

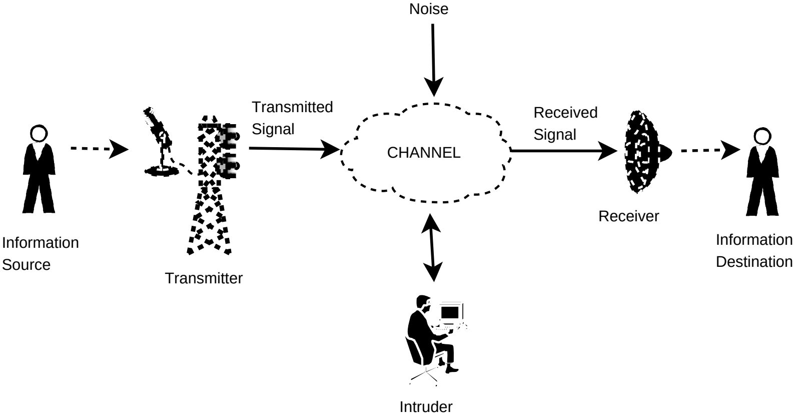
Our Goal

1. Nodes Characteristics
2. Communication Model
3. Formal definiton of neighbourhood
4. Intruder Model
5. Example: Finger Printing

Nodes Characteristics

- Signal (IF, Wave, ...)
- Range
- Power
- Antenna
- Transmiter
- Receiver
- (D)Encryption mechanisms

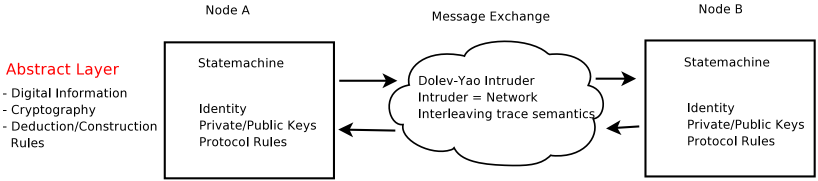
Communication Model (Shannon)



Two Layers

- Abstract Layer
- Physical Layer

Abstact Layer



Abstract Layer

- Digital Information
- Cryptography
- Deduction/Construction Rules

Node A

Statemachine

Identity
Private/Public Keys
Protocol Rules

Message Exchange

Dolev-Yao Intruder
Intruder = Network
Interleaving trace semantics

Node B

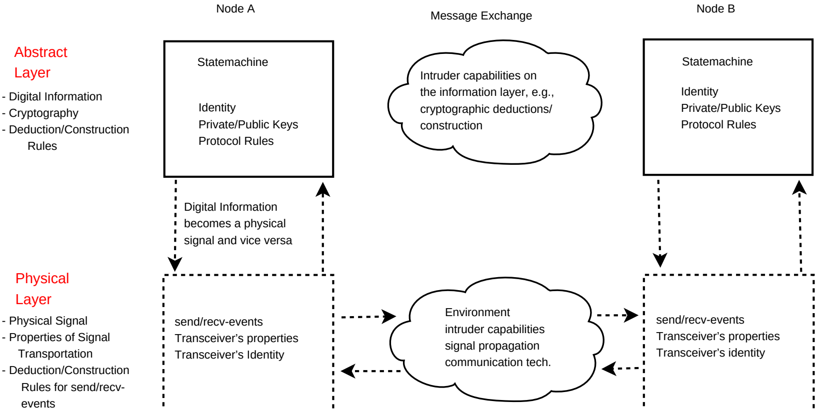
Statemachine

Identity
Private/Public Keys
Protocol Rules

Abstact Layer: Needham-Schroeder Example

$$
\begin{aligned}
A \rightarrow B: &\quad \{N_A.A\}_{K_B} \\
B \rightarrow A: &\quad \{N_A.N_B\}_{K_A} \\
A \rightarrow B: &\quad \{N_B\}_{K_B}
\end{aligned}
$$

Physical Layer



Node A

Message Exchange

Node B

Abstract Layer

- Digital Information
- Cryptography
- Deduction/Construction Rules

Statemachine

Identity
Private/Public Keys
Protocol Rules

Intruder capabilities on the information layer, e.g., cryptographic deductions/ construction

Statemachine

Identity
Private/Public Keys
Protocol Rules

Digital Information becomes a physical signal and vice versa

Physical Layer

- Physical Signal
- Properties of Signal Transportation
- Deduction/Construction Rules for send/recv-events

send/recv-events
Transceiver's properties
Transceiver's Identity

Environment
intruder capabilities
signal propagation
communication tech.

send/recv-events
Transceiver's properties
Transceiver's identity

Events

- $send_{\phi}(T_A, P_{T_A}, m)$
- $send_{\alpha}(A, m)$
- $recv_{\phi}(R_A, P_{R_A}, m)$
- $recv_{\alpha}(A, m)$

Communication Rules on Needham-Schroeder Example

$$\begin{array}{ll} A \to B: & \{N_A.A\}_{K_B} \\ B \to A: & \{N_A.N_B\}_{K_A} \\ A \to B: & \{N_B\}_{K_B} \end{array}$$

$$(P_0)\frac{}{\langle\rangle \in S} \qquad (P_1)\frac{tr \in S}{tr.send_\alpha(A, \{N_A.A\}_{K_B}) \in S}$$

$$(P_2)\frac{tr \in S \qquad recv_\alpha(B, \{N_A.A\}_{K_B}) \in tr}{tr.send_\alpha(B, \{N_A.N_B\}_{K_A}) \in S}$$

$$(P_3)\frac{\begin{array}{c} tr \in S \qquad send_\alpha(A, \{N_A, A\}_{K_B}) \in tr \\ recv_\alpha(A, \{N_A.N_B\}_{K_A}) \in tr \end{array}}{tr.send_\alpha(A, \{N_B\}_{K_B}) \in S}$$

Physical Rules

$$(Phy)\frac{tr \in S \qquad send_{\phi}(T_A, P_{T_A}, m) \in tr \qquad (T_A, R_B) \in \mathcal{N}}{tr.recv_{\phi}(R_B, P_{R_B}(P_{T_A}), m) \in S}$$

Connecting Rules

$$(Con_0)\frac{tr \in S \qquad send_\alpha(A, m) \in tr}{tr.send_\phi(T_A, P_{T_A}, m) \in S}$$

$$(Con_1)\frac{tr \in S \qquad recv_\phi(R_A, P_{R_A}, m) \in tr}{tr.recv_\alpha(A, m) \in S}$$

There exists a rule that inserts a flag $END(R_A, T_B)$ into a trace, indicating that the protocol has been successfully executed between the corresponding nodes A and B.

Rules for Intruder Capabilites

- $IK(<>) = IK_0$
- $IK(recv_\alpha(X, m).tr) = \{m\} \cup IK(tr)$
- $IK(send_\phi(T_A, P_{T_A}, m).tr) = IK(tr)$
- $IK(recv_\phi(R_A, P_{R_A}, m).tr) = IK(tr)$
- $IK(send_\alpha(A, m).tr) = IK(tr)$

Dolev-Yao intruder (Encryption, decryption, pairing, projections)

$$(insert)\frac{tr \in S \qquad m \in \widehat{IK(tr)}}{tr.send_\alpha(I, m) \in S}$$

Intruder is the neihgbour of all honest nodes.

$$\forall X, (I, X) \in \mathcal{N}, (X, I) \in \mathcal{N}$$

Notations

Definfition

Let $\mathcal{P}$ be a set of rules describing a protocol, $\mathcal{N}$ the direct communication relationand $\mathcal{I}$ the set of rules defining the intruder. $\mathcal{S}_{ind}(\mathcal{N}, \mathcal{I}, \mathcal{P})$ is the set of all possible traces.

We denote by $tr(i)$ the $(i+1)$th event of a trace tr.

Example

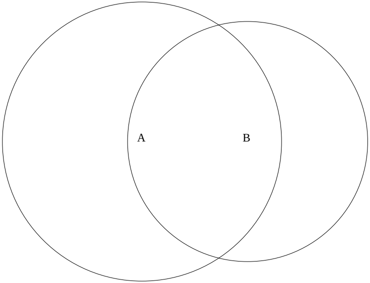
Let $tr = send_\alpha(A, m_1).send_\phi(T_A, P_{T_A}, m_2)$, then $|tr| = 2$, $tr(0) = send_\alpha(A, m_1)$ and $tr(1) = send_\phi(T_A, P_{T_A}, m_2)$.

Neighbourhood = Signal Origin Authentication

Definfition

A node A is neighbour to node B if there exists a **direct communication from** B **to** A**.**

- No Symetric
- No replay, relay
- No adversary between



Formal Signal Origin Authentication

Definition

Let T_A be a transmitter, R_B a receiver and S a set of traces. R_B *has a signal orgin authentication of* T_A *in* S, denoted by $Ng(T_A, R_B, S)$ iff there exists a trace $tr \in S$, a fresh message m with respect to tr, and indices i and j, with $0 \leq i < j < |tr|$, such that

1. $tr(i) = send_\phi(T_A, P_{T_A}, m)$,
2. $tr(j) = recv_\phi(R_B, P_{R_B}, m)$, and
3. for all k, $i < k < j$, there does not exist a $C \neq A$ such that $tr(k) = send_\phi(T_C, P_{T_C}, m)$.

Signal Origin Authentication

Definition

The protocol $\mathcal{P}$ is said to correctly verify signal origin authentication if and only if for all pairs of participating nodes A and B the following is true: $\exists tr \in \mathcal{S}_{ind}(\mathcal{N}, \mathcal{I}, \mathcal{P})$:

$$END(R_A, T_B) \in tr \Rightarrow Ng(T_B, R_A, \mathcal{S}_{ind}(\mathcal{N}, \mathcal{I}, \mathcal{P})).$$

Example: Finger Printing

$$(P_0)\frac{}{\langle\rangle \in S}$$

$$(P_1)\frac{t \in S}{t.send_\alpha(A, m) \in S}$$

$$(END)\frac{\begin{array}{c} tr \in S \\ recv_\phi(R_B, P_{R_B}(P_{T_A}), m) \in tr \qquad F_{T_A} \in P_{R_B}(P_{T_A}) \end{array}}{tr.END(R_B, T_A) \in S}$$

Outline

Summary

- Nodes Characteristics
- Communication Model
- Formal definiton of neighbourhood
- Intruder Model
- Example: Finger Printing

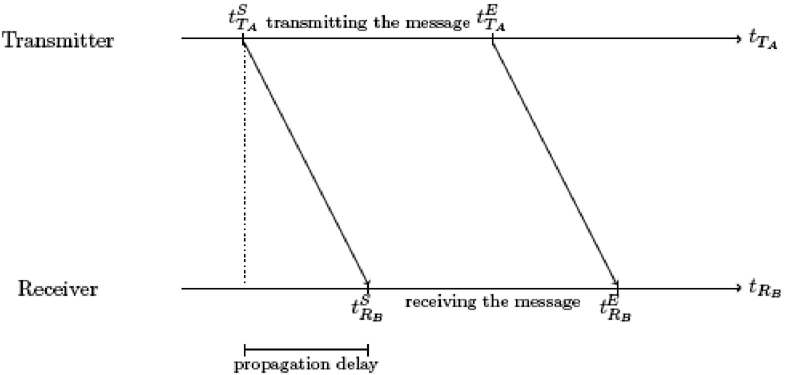
Challenges

- Refinement of Intruder Capabilities
- Refinement of Nodes properties
- New Modeling for Communication (Broadcast, range ,...)
- Time Modeling (location)
- Mobility of the nodes

Example using Time: Authenticated Ranging Protocol

A(lice)		**B(ob)**
Choose a nonce N_A		
$t^S_{T_A}$	$\xrightarrow{N_A, A}$	$t^E_{R_B}$
$t^E_{R_A}$	$\xleftarrow{t^E_{R_B}, t^S_{T_B}, N_A, B, Mac_{K_{AB}}(t^E_{R_B}, t^S_{T_B}, N_A, B)}$	$t^S_{T_B}$
if $\tau \leq T_{max}$ then A concludes B is his neighbor		

Time Propagation



Time-based Neighbourhood Property

Definition

Let T_A be a transmitter, R_B be a receiver, and S a set of traces. R_B *is a neighbor of* T_A *at* $t^E_{R_B}$ *in* S, denoted $Ng^t(T_A, R_B, t^E_{R_B}, S)$, if and only if there exists a trace $tr \in S$, a fresh ("unpredictable") message m in the trace tr, event indices i, j, where $0 \leq i < j < |tr|$, $t^E_{T_A}$ such that:

1. $tr(i) = send_\phi(T_A, t^S_{T_A}, t^E_{T_A}, P_{T_A}, m)$,
2. $tr(j) = recv_\phi(R_B, t^S_{R_B}, t^E_{R_B}, P_{R_B}, m)$, and
3. for all k, where $i < k < j$, and for all T_C, $t^E_{T_C}$, and $t^S_{T_C}$, with $C \neq A$, there does not exist $tr(k) = send_\phi(T_C, t^S_{T_C}, t^E_{T_C}, P_C, m)$.

Time-based Neighbourhood Property

Definition

A protocol given by the rule set $\mathcal{P}$ verifies the neighborhood property that A concludes that B is his neighbor at time $t^{E}_{R_A}$ if and only if $\exists tr \in S(\mathcal{N}^t, I, \mathcal{P})$,

$$End(R_A, T_B, t^{E}_{R_A}) \in tr \Rightarrow Ng^t(T_B, R_A, t^{E}_{R_A}, S(\mathcal{N}^t, I, \mathcal{P}))$$

Thank you for your attention.

Questions ?