Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Embedding Security and Trust in Mobile Ad Hoc Networks

Mirosław Kutyłowski

Wrocław University of Technology
Institute of Mathematics and Computer Science

2nd International Conference on New Technologies, Mobility and Security (NTMS)
Tangier, 7.11.2008

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Agenda

- problems, risks and challenges
- recent ideas, techniques:
  - improving point-to-point connection against node capture
  - improving key predistribution against node capture
  - authentication for RFID-like devices

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Introduction

perspectives, key issues

Pervasive electronic systems

Tendency

- rapidly increasing use of electronic micro-controllers in industrial products due to
  - low manufacturing price
  - flexibility
  - dependability
- advantage of radio communication

New application areas

pharmacy, logistics, law enforcement, health protection, monitoring systems, ...

Challenges

Conflicting requirements

- price should be extremely low,
- sophisticated demands on functionality.

Mission Impossible?

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Challenges
communication problems

Communication limitations

- communication bandwidth limited
- communication volume limited due to energy use
- interferences
- diverse and uncoordinated systems

Challenges

energy supply problems

Battery operated devices

- single use devices,
- avoid any energy consuming activity,
- energy saving drives the hardware design

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Challenges

energy supply problems

Battery operated devices

- single use devices,
- avoid any energy consuming activity,
- energy saving drives the hardware design

Inductive circuits

- working as slaves only – a master device must activate them,
- a session may be interrupted at any time,
- no way to perform any activity independently.

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Challenges
computational power

Computational power limitations

- “outdated” technology:
  - low frequency, slow
  - low density - small number of gates, registers, ...
  - small word size (8bit processors!)
  - limited instruction set
  - ...
- but reliable in extreme conditions

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Privacy

Big Brother problems

- pervasive systems may provide a huge amount of information,
  it can be misused for:
  - criminal purposes
  - dishonest competition
  - terrorism
- legal requirement: each system MUST protect against unauthorized access to personal data

Developing Trust

How to trust a device?

(mutual) authentication necessary:
even in a small proximity, how do we know that we are talking to a certain device?

how do we know that we are in contact with an authorized device? recall the cases of fake ATMs!

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Emerging threats

New types of attacks

- passive attacks on communication: eavesdropping
- active attacks on communication: replay attacks, scrambling, . . .
- Sybian attacks (a device emulates many devices with many identities)
- capturing devices for cloning
- destroying devices (e.g. for batteries)

Solutions

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Key Evolution Technique

joint work with M.Ren, M.Klonowski, K.Rybarczyk, J.Jaworski, and J.Zhou, Tanmoy

ESORICS'2006, CANS'2007

Key evolution

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Scenario

- devices cannot use asymmetric cryptography
- unpredictable in advance which devices will establish a communication link,
- an eavesdropper may capture a device and retrieve its keys

  how to protect then the past communication (already recorded by the adversary)?

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key evolution
basic scenario

Establishing a session key between devices $\mathcal{A}$ and $\mathcal{B}$

- any available method can be used:
  - agree upon a key in a secure environment (in plaintext)
    like for Bluetooth
  - or something else
    like a key predistribution

Key evolution
change of the session key

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Idea

- change the key at random at each communication round
- do not increase communication volume

impossible?

Key evolution
change of the session key

Basic mechanism

Let K be the key currently shared by $\mathcal{A}$ and $\mathcal{B}$

1. if $\mathcal{A}$ wishes to send a message M to $\mathcal{B}$, then:
   - it flips a random bit of K, getting a modified key K'
   - it encrypts M with K':

     $$C := E_{K'}(M)$$

     and send C to $\mathcal{B}$
2. $\mathcal{B}$ works as follows:
   - it decrypts C with all keys obtained from K by flipping just one bit
   - until a reasonable plaintext is obtained
   - such a key is taken as the new shared key

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Key evolution

change of the session key -consistency issues

Problems

- $\mathcal{B}$ may fail to receive a message sent by $\mathcal{A}$
  but we have to retain the property that $\mathcal{A}$ and $\mathcal{B}$ have a shared key!
- one can design a protocol that works:
  with some procedural effort and a temporary change of a key until it becomes confirmed in some way

Key evolution
Properties of the basic scheme

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Advantages

- the changes are purely random
- if two devices exchange enough messages, then the key changes completely

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key evolution

Properties of the basic scheme

Advantages

- the changes are purely random
- if two devices exchange enough messages, then the key changes completely
- if an adversary captures $\mathcal{A}$ or $\mathcal{B}$, then he gets the current key, but cannot reverse the random process of flipping bits to learn old shared keys

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key evolution

Properties of the basic scheme

Advantages

- the changes are purely random
- if two devices exchange enough messages, then the key changes completely
- if an adversary captures $\mathcal{A}$ or $\mathcal{B}$, then he gets the current key, but cannot reverse the random process of flipping bits to learn old shared keys

Disadvantages

- if the adversary has recorded all communication, then reversing is easy
  - just by flipping single bits

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Forward secure version

scheme

Scheme

just like the basic scheme, but instead of flipping a random bit in K, device $\mathcal{A}$:

- chooses i at random,
- computes
$$K' := F(K, i)$$
where F is an one-way function.

one-way function

F is one-way, if computing $y := F(x)$ is easy, but finding x from y has negligible success probability

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Forward secure version

properties

Forward security

The adversary having all past transmission at hand cannot derive the past keys from the current one.

computing K from K' would mean reversing the one-way function

Practical meaning

if a transmission is confidential now, it will remain secure in the future even if one of the devices gets captured by an adversary

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Nontrivial issues

Potential dangers

- the changes are not now as random as before,
- *F* defines a random directed graph of outdegree 1,
- ... but random graphs have sometimes strange properties
  like short cycles

Proved properties

With very high probability:

- *F* has no property that would enable time-space trade-off attacks.
- every state of the key is reachable and the path is relatively short.

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Levels

joint work with J.Cichoń, J.Grząślewicz

unpublished work

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Predistribution
requirements

Goal

- preinstall keys on mobile devices so that they can establish secure links with symmetric methods

one shared key for all devices?

Key Predistribution

requirements

Goal

- preinstall keys on mobile devices so that they can establish secure links with symmetric methods

  one shared key for all devices?

- but make sure that compromising a few devices should not compromise the whole system

Key Predistribution
Solution

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Assignment

- there is a large pool of n keys $\mathcal{K}$
- before deployment a device gets keys from a random subset of $\mathcal{K}$ of cardinality k

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Predistribution
Solution

Key Assignment

- there is a large pool of n keys $\mathcal{K}$
- before deployment a device gets keys from a random subset of $\mathcal{K}$ of cardinality k

Establishing a Session Key

- devices A and B tell themselves the identifiers of the keys they posses
- A and B determine the keys, $k_1, \ldots, k_u$ which they share
- the session key is computed independently by A and B:

$$s_{AB} := H(k_1, \ldots, k_u, \text{public parameters})$$

Key Predistribution
Problems

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Attack scenario

- an adversary collects devices with the keys from the pool ...
- and retrieves the keys from these devices (even in a destructive way),

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Predistribution
Problems

Attack scenario

- an adversary collects devices with the keys from the pool ...
- and retrieves the keys from these devices (even in a destructive way),

Attack cost

observe that the number of keys k in a device must be fairly large compared to the size of the key pool n

(for $k \approx \sqrt{n}$ the probability to establish a connection reaches acceptable level due to the birthday paradox).

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Predistribution

Attempt to solve the problem

Multiple Keys

increase the number of keys that **must** be shared in order to establish a connection:

- less likely that the adversary has all of them

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Predistribution

Attempt to solve the problem

Multiple Keys

increase the number of keys that **must** be shared in order to establish a connection:

- less likely that the adversary has all of them
- but one has to increase k/n making collecting keys much easier (in order to have u shared keys the devices must get $\approx n^{1-1/u}$ keys)

Attack resilience

probability to break a connection:

- decreases, if the adversary can capture only a small number of devices,
- increases, once the number of captured devices exceeds some level.

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Idea 1 - codesign of fixed and ad hoc networks

- a mobile artefact working offline may be in contact with some security infrastructure from time to time

Key Predistribution

Ideas

Idea 1 - codesign of fixed and ad hoc networks

- a mobile artefact working offline may be in contact with some security infrastructure from time to time
- an artefact meeting an authorization station may refresh its secret keys

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Idea 2 - compatibility with the past

- each of the keys used occurs in infinite many variants $\ldots K_{-2}, K_{-1}, K_0, K_1, K_2, \ldots$, where

$$K_{i+1} = G(K_i)$$

Trust & Security for Ad Hoc Networks

M. Kutyłowski

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Idea 2 - compatibility with the past

- each of the keys used occurs in infinite many variants $\ldots K_{-2}, K_{-1}, K_0, K_1, K_2, \ldots$, where

$$K_{i+1} = G(K_i)$$

- G is a trapdoor one-way function:
  - one can compute G easily,
  - but without trapdoor information it is impossible to compute K_i from K_{i+1}

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Idea 2 - compatibility with the past

- each of the keys used occurs in infinite many variants $\ldots K_{-2}, K_{-1}, K_0, K_1, K_2, \ldots$, where

$$K_{i+1} = G(K_i)$$

- G is a trapdoor one-way function:
  - one can compute G easily,
  - but without trapdoor information it is impossible to compute K_i from K_{i+1}
- so a device holding K_i can speak with a device holding K_j for $j > i$ after computing $G^{j-i}(K_i)$.

Key Levels
design idea

Refreshing

- from time to time a mobile artefact visits Key Refreshment Booth:
  for each K_i held by a device it asks for K_j with the lowest j available for it at the moment

Key Levels
design idea

Refreshing

- from time to time a mobile artefact visits Key Refreshment Booth:
  for each K_i held by a device it asks for K_j with the lowest j available for it at the moment
- the system provider does not have to store all K_j in advance: it may use the trapdoor to derive all versions of the key from just one K_i

Key Levels
design idea

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Refreshing

- from time to time a mobile artefact visits Key Refreshment Booth:
  for each K_i held by a device it asks for K_j with the lowest j available for it at the moment
- the system provider does not have to store all K_j in advance: it may use the trapdoor to derive all versions of the key from just one K_i

Communication

- if devices $\mathcal{A}$ and $\mathcal{B}$ hold, respectively, K_a and K_b, they use $K_{\max(a,b)}$ for communication
- i.e. one of the devices has to reconstruct the older key version

Key Levels
Immunity against adversary

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Goal

- the adversary has to collect new keys all the time, authenticating himself against Key Refreshment Booth the attack never ends!

Key Levels
Immunity against adversary

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Goal

- the adversary has to collect new keys all the time, authenticating himself against Key Refreshment Booth the attack never ends!
- a device can refuse to talk with a device without fresh keys according to its current policy

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Key Levels

just two levels

Level assignment

an artefact getting a key K receives:

- K_1 with probability p,
- K_2 with probability $1 - p$.

Key Levels

just two levels

Level assignment

an artefact getting a key K receives:

- K_1 with probability p,
- K_2 with probability $1 - p$.

Attack failure

An adversary having a version of K fails to break a link, if

- it has K_2
- A and B share K_1

Key Levels

just two levels

Level assignment

an artefact getting a key K receives:

- K_1 with probability p,
- K_2 with probability $1 - p$.

Attack failure

An adversary having a version of K fails to break a link, if

- it has K_2
- A and B share K_1

Attack failure probability

- the attack fails with probability $p^2(1 - p)$
- maximized for $p = \frac{2}{3}$, and equal to $\frac{4}{27} \approx 0.15$

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Increasing attack failure probability

L levels

if a version of key K has to be installed in a device, then

- choose K_i with probability p_i

what is the optimal choice of probabilities?

Optimizing probabilities

- example: for $L = 4$ by taking derivatives we can derive

$$p_1 = \frac{552}{1263}, \quad p_2 = \frac{276}{1263}, \quad p_3 = \frac{230}{1263}, \quad p_4 = \frac{205}{1263} \quad .$$

Optimizing probabilities for levels

Idea for $L+1$ levels

- first choose
  - to go to level $L+1$, or
  - to remain within levels 1 through L (probability q)

Optimizing probabilities for levels

Idea for $L+1$ levels

- first choose
  - to go to level $L+1$, or
  - to remain within levels 1 through L (probability q)
- if level $L+1$ has not been chosen, then choose one of the levels according to the optimal procedure for L levels

Optimizing probabilities for levels

Idea for $L+1$ levels

- first choose
  - to go to level $L+1$, or
  - to remain within levels 1 through L (probability q)
- if level $L+1$ has not been chosen, then choose one of the levels according to the optimal procedure for L levels
- having the optimal probability of failure for L levels, say S_L, one can optimize q and derive

$$S_{L+1} = \frac{4}{27} \cdot \frac{1}{(1-S_L)^2}$$

Attack failure probabilities
large number of levels

Influence of the number of levels

- S_L increases with L
- what is the limit?

Attack failure probabilities

large number of levels

Influence of the number of levels

- S_L increases with L
- what is the limit?

Infinitely many levels

level x for each $x \in [0, 1]$, cumulative probability distribution $F(a)$ to choose $x \leq a$, how to choose F?

Attack failure probabilities

large number of levels

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Influence of the number of levels

- S_L increases with L
- what is the limit?

Infinitely many levels

level x for each $x \in [0, 1]$, cumulative probability distribution $F(a)$ to choose $x \leq a$, how to choose F?

$$S_\infty \approx \sum_{0 \leq x \leq 1} F^2(x) \cdot (F(x+\delta) - F(x)) \quad . \tag{1}$$

so

$$S_\infty = \int_{x=0}^{1} F^2(x) \cdot F'(x) dx \quad . \tag{2}$$

Attack failure probabilities

large number of levels

Observation

$$(F^3(x))' = 3 \cdot F^2(x) \cdot F'(x) \quad . \tag{3}$$

So

$$S_\infty = \frac{F^3(x)}{3}\Big|_0^1 = \frac{1}{3} - 0 = \frac{1}{3} \quad . \tag{4}$$

So:

Lemma

$S_\infty = \frac{1}{3}$ no matter which cumulative probability distribution function F is used.

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Attack failure probabilities
large number of levels

Corollary

Choose the number of levels so that the probability is close enough to $\frac{1}{3}$, do not try to reach $\frac{1}{3}$.

Table: Probabilities S_L

for the optimal choice of probabilities

$L=2$	$L=3$	$L=4$	$L=5$	$L=6$	$L=7$	$L=8$
0.1481	0.2042	0.2339	0.2524	0.2651	0.2745	0.2818

$L=10$	$L=12$	$L=16$	$L=20$	$L=24$	$L=28$	$L=32$
0.2912	0.2980	0.3065	0.3118	0.3153	0.3178	0.3197

Multiple keys

Idea

- if the number of shared keys required is u, then the adversary has to know
  - each of the keys
  - and of the right level
- conditional success probability for adversary for each key is $\geq \frac{2}{3}$, but the adversary has to succeed for each single key

Multiple keys

Idea

- if the number of shared keys required is u, then the adversary has to know
  - each of the keys
  - and of the right level
- conditional success probability for adversary for each key is $\geq \frac{2}{3}$, but the adversary has to succeed for each single key

Impact

- dramatic improvement of security when the adversary has captured a limited number of keys
- what happens if the adversary captures a large number of devices?

Compromising many devices

Coupon collector problem

- it is necessary to collect L specific keys (coupons)
- each time a random coupon out of n can be obtained by the adversary
- known phenomenon:
  - the hardest thing is to obtain the last coupons,
  - one has to collect about $L \ln L$ coupons

Number of devices to be captured
2 level scheme

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction
attacks

Theorem

Let $N_{L,p}$ denote the number of steps after which adversary collects all keys for compromising connection based on L shared keys, for $p =$ the probability of choosing the key of level 1 for the scheme with 2 levels. Then

$$E[L_{m,p}] = \int_0^\infty \left(1 - \frac{H(t)}{e^t}\right) dt \,, \qquad (5)$$

where $H(z) = \left(e^{z/m} - 1 - p^2(e^{qz/m} - 1)\right)^m$ *and* $q = 1 - p$.

Number of devices to be captured

some values

some values

- For $m = 1$ the optimal value of p is 0.5; in this case $E[L_m] = 1.25$.
- For $m = 10$, the optimal value of p is 0.32164; then $E[L_m] \approx 40.9724$, i.e. $E[L_m] = 1.39887 \cdot m \cdot H_m$,

Number of devices to be captured

infinite number of levels

Theorem

$$E[L_\infty] = \frac{3}{2} \cdot m \cdot H_m \ ,$$

where H_m denotes the mth harmonic number.

Corollary

The highest average increase of cost for the adversary is 50%. so it does not make sense to increase the number of shared keys too much.

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Authentication with RFID's

passive RFIDs

electronic bar codes

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

energy

1. no internal source,
2. energy from the reader, induction circuit
3. no computation if not activated by the reader

communication

1. responses to the reader
2. typically: shows its ID only

computations

1. just a few hundred of gates

RFID-tags
Security requirements

Requirements

- a tag must be authenticated reliably, by legitimate readers only

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

RFID-tags

Security requirements

Requirements

- a tag must be authenticated reliably, by legitimate readers only
- untracability – nobody, except for the legitimate party, can trace the tag (privacy protection)

Trust & Security for Ad Hoc Networks

M. Kutyłowski

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction
attacks

Requirements

- a tag must be authenticated reliably, by legitimate readers only
- untracability – nobody, except for the legitimate party, can trace the tag (privacy protection)
- no cloning

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction
attacks

Requirements

- a tag must be authenticated reliably, by legitimate readers only
- untracability – nobody, except for the legitimate party, can trace the tag (privacy protection)
- no cloning
- security trade-off: moderate security and a low price

Trust & Security for Ad Hoc Networks

M. Kutyłowski

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction
attacks

Requirements

- a tag must be authenticated reliably, by legitimate readers only
- untracability – nobody, except for the legitimate party, can trace the tag (privacy protection)
- no cloning
- security trade-off: moderate security and a low price
- no use of heavy algorithms (including most symmetric algorithms), simple operations only

Example method - HB

design goals

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Goals

1. strong authentication
2. passive adversary only
3. prevent cloning

Background problem

hard problem: *learning parity with noise*

Trust & Security for Ad Hoc Networks

M. Kutyłowski

Introduction
- Hardware
- privacy, trust
- new attacks

Key Evolution
- basic scheme
- forward secure

Key levels
- introduction
- scheme

RFID authentication

HB, HB+
- protocols
- attacks

Hidden subsets
- algorithm
- properties
- reconstruction attacks

description

Public parameters: n, ε, η

Secret key: $\mathbf{x} \in \{0,1\}^n$

Reader		Tag
choose $\mathbf{a} \in_R \{0,1\}^n$	$\xrightarrow{\mathbf{a}}$	
		$\nu := \begin{cases} 1 & \text{with pbb } \varepsilon \\ 0 & \text{with pbb } 1-\varepsilon \end{cases}$
check $z \stackrel{?}{=} \mathbf{a} \cdot \mathbf{x}$	$\xleftarrow{z}$	$z := (\mathbf{a} \cdot \mathbf{x}) \oplus \nu$

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

HB

Protocol

1. repeat the basic step r times
2. count the number of successes
3. accept, if the number of successes exceeds $r \cdot (1 - \eta)$

HB
problems

Active adversary

active adversary: $a = (1, 0, 0, \ldots, 0)$ several times for learning x_1,
...then for x_2, x_3,...

Number of k bits sent during the authentication

n	$\eta = 1/20$	$\eta = 1/8$	$\eta = 1/4$
128	4	7	18
512	16	28	73

deriving internal key

practically possible if the key not too long and the error level too low

HB+ authentication protocol

Ari Juels and Stephen Weis

a step

Public parameters: n, ε, η

Secret key: $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$

Reader		**Tag**
choose $\mathbf{a} \in_R \{0,1\}^n$	$\xrightarrow{\mathbf{a}}$	
	$\xleftarrow{\mathbf{b}}$	$\mathbf{b} \in_R \{0,1\}^n$
		$\nu := \begin{cases} 1 & \text{with pbb } \varepsilon \\ 0 & \text{with ppb } 1-\varepsilon \end{cases}$
$z \stackrel{?}{=} (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y})$	$\xleftarrow{z}$	$z := (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y}) \oplus \nu$

adaptive attack against HB+ turns down to become non-adaptive against HB

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Polynomial memory attack

Gołębiewski, Majcher, Zagórski, Zawada

AD HOC NOW '2008, INSCRYPT'2008

Attack

Gołębiewski, Majcher, Zagórski, Zawada

scenario

1. collect about $2n$ transmissions
2. analyze

Efficiency

1. runtime asymptotically exponential, but for small n ...
2. input size moderate
3. the previous methods needed both time and input exponential

Attack idea

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Given

- (a_i, z_i) for $i = 1, \ldots, 2n$
- where $a_i \cdot x = z_i$ holds for MOST parameters i

1. guess n pairs (a_i, z_i) that are linearly independent, say

$$A = (a_{j_1}, z_{j_1}), (a_{j_2}, z_{j_2}), \ldots, (a_{j_n}, z_{j_n})$$

2. guess which answers are wrong assuming that their number is not greater than k, and correct them
3. k might be small for practical values of n and ϵ + deviations in minus concerning the expected value $n \cdot \epsilon$

Attack idea

1. guess n pairs (a_i, z_i) that are linearly independent, say

$$A = (a_{j_1}, z_{j_1}), (a_{j_2}, z_{j_2}), \ldots, (a_{j_n}, z_{j_n})$$

2. guess which answers are wrong assuming that their number is not greater than k, and correct them
3. k might be small ...
4. test correction: express the other a_i as a linear combination of vectors a_{j_l}:

$$a_i = \sum_{l=1}^{n} d_l a_{j_l}$$

and check if

$$z_i = \sum_{l=1}^{n} d_l z_{j_l}$$

for most cases

corollaries

1. necessary to keep the size of the key and error rate, number of transmissions large enough
2. but then communication volume becomes unacceptable

what if smarter search methods developed??

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Hidden subsets authentication

joint work with Jacek Cichoń and Marek Klonowski

PERVASIVE'2008

Hidden Subsets Identifiers

Answers from our tag

improvements due to an attack of Z. Gołebiewski, K. Majcher, F. Zagórski, M. Zawada

Answers from our tag

```
 1:    11001111010001111010
 2:    01101111011011011011
 3:    10010111100001100001
 4:    11111011100000100001
 5:    01111011101010010010
 6:    11000100000000000011
 7:    00000101101010001111
 8:    10110110111010010111
 9:    10000110110011001111
10:    00101010100111000000
```

These answers seems to be completely random. However, there are hidden regularities which allows the owner to recognize a particular tag.

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

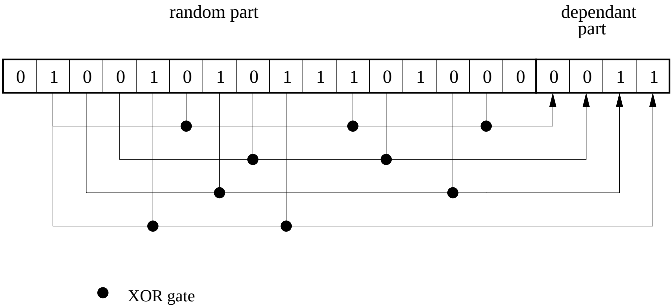
Basic idea

Idea

- there are some dependencies between the bits sent, even if most bits are set at random
- the dependencies are known only to the owner (issuer) of the tag
- one can trace the tag if and only if one knows these dependencies

Basic idea

Toy example: a (16,4)-tag



Construction idea
Linear mappings

Construction of our tag

The answers are divided into two parts. The first part (independent part) is of length *n*. The second part (dependent part) is of length *m*. We have also

$$\mathrm{T} : \{0,1\}^n \xrightarrow{linear} \{0,1\}^m ,$$

where $\{0,1\}^n$ and $\{0,1\}^m$ are treated as linear spaces over $\{0,1\}$ with mod 2 operations.

Basic idea
Generating answers

Generating an answer

1. the tag generates a random sequence of bits $\overline{x} \in_R \{0,1\}^n$

Basic idea
Generating answers

Generating an answer

1. the tag generates a random sequence of bits $\overline{x} \in_R \{0,1\}^n$
2. the tag sends the following answer

$$(x_1, \ldots, x_n, y_1, \ldots, y_m) = (\overline{x}, \mathrm{T}(\overline{x})) \in \{0,1\}^{n+m} .$$

Trust & Security for Ad Hoc Networks
M. Kutyłowski
Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Generating an answer

1. the tag generates a random sequence of bits $\overline{x} \in_R \{0,1\}^n$
2. the tag sends the following answer

$$(x_1, \ldots, x_n, y_1, \ldots, y_m) = (\overline{x}, \mathrm{T}(\overline{x})) \in \{0,1\}^{n+m} .$$

The authorized reader knows (n, m, T). Hence, it may check whether

$$(y_1, \ldots, y_m) = \mathrm{T}((x_1, \ldots, x_n)) .$$

Basic idea

Logical parts of our tag

Answers from our tag

	independent	dep.
1:	11001111010001	11010
2:	01101111011011 0	11011
3:	10010111100001 1	00001
4:	11111011100000 1	00001
5:	01111011101010 0	10010
6:	11000100000000 0	00011
7:	00000101101010 0	01111
8:	10110110111010 0	10111
9:	10000110110011 0	01111
10:	00101010100111 0	00000

Introduction
Hardware
privacy, trust
new attacks

Key Evolution
basic scheme
forward secure

Key levels
introduction
scheme

RFID authentication

HB, HB+
protocols
attacks

Hidden subsets
algorithm
properties
reconstruction attacks

Redundancy
design problem

Dependency

- For T chosen at random it may happen that some dependent bits generated by T linearly depend on the other dependent bits generated by T.
- This would be detected by reading the tag, making possible to trace it afterward without knowing the key.

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction
attacks

Redundancy

Rank of a random 01 matrix

Lemma

Let

$$A = \begin{pmatrix} \xi_{1,1} & \dots & \xi_{1,n} \\ \dots & \dots & \dots \\ \xi_{n,1} & \dots & \xi_{n,n} \end{pmatrix}$$

be a matrix of independent random bits. Then

$$\Pr[det(A) \neq 0] = \prod_{a=0}^{n-1} (1 - 1/2^a) \approx 0.2887 \quad .$$

Avoiding redundancies

quite probable unless the size of dependent part too big

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Unlinkability
game

Linking Game

1. L tags in the system
2. the adversary scans all these tags t times.
3. the challenger chooses some tag i and presents scan $t+1$ of this tag,
4. the adversary wins, if he answers with i

Unlinkability
example result

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Theorem

*Consider the Linking Game with t trials for a family of L tags from (n, k)-tags. Suppose that $n \in [128, 1024]$, $t < n - 40$. Then for all $L < 2^{n-t-32}$ the probability that **any** adversary has **an** advantage (meaning that at least one tag can be excluded) is less than 2^{-30}.*

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Reconstruction via Linear Equations

Technique

- write a system of linear equations with unknowns with values 0,1 describing the linear functions of T
- coefficients taken from answers of the tag
- solve the system of linear equations

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Against tag reconstruction

Techniques

noise each dependent bit may be wrong with probability p ,

permutation the reader and tag share and use a secret permutation σ:

1. the reader says j
2. the tag permutes its answer bits with permutation σ^j

Introduction
Hardware
privacy, trust
new attacks
Key Evolution
basic scheme
forward secure
Key levels
introduction
scheme
RFID authentication
HB, HB+
protocols
attacks
Hidden subsets
algorithm
properties
reconstruction attacks

Thank you for your attention!

contact info at: `kutylowski.im.pwr.wroc.pl`