logo2

Chameleon RFID and Tracking Prevention

Marek Klonowski, Mirosław Kutyłowski, Piotr Syga

Wrocław University of Technology
Wrocław, Poland

RFID Sec Asia 2013, Guangzhou

Assumptions

RFID

1. no secret shared with the system database,
2. no computations based on shared secrets,
3. no cryptographic functions implemented
4. the RFID has some built-in source of randomness

- most papers assume some (lightweight) cryptographic features on the RFID
- lightweight might be not strong enough
- for practical applications these cheap tags might be still too expensive

Privacy Threats

Tracking

- if an RFID tag has a static ID and no encryption/blinding, then tracking is easy
- authentication does not help much – the adversary might be passive (eavesdropper)
- automatic collection of data from the tags + data processing – a lot of data revealed

Challenge

How to develop a system that provides **privacy by design**?

Attack model

Assumptions

1. an adversary can eavesdrop communication **on many places but not everywhere**,
2. only a fraction of locations of system readers might be monitored by the adversary

Goal

1. the adversary should loose control at the moment when he does not listen to interactions with the tag just a few times
2. no data written by the reader on the tag – as it would open room for tracing of special kind (by malicious readers only)
3. tag recognition at the central system only

Chameleon RFID Scheme
description

System database

for each RFID it keeps a record

presentedID, permanentID

- *presentedID* is the last ID seen from the RFID
- *permanentID* is the fixed ID of the RFID stored in the system only

RFID

each RFID keeps two IDs:

currentID, *previousID*

- *previousID* is the ID presented to the system reader recently
- *currentID* is the ID to be shown now

the regular situation:

RFID		system	
previousID:	K_t	*presentedID*:	K_t
currentID:	K_{t+1}	*permanentID*:	L

- *currentID* used only once against a system reader
- when the *currentID* used it becomes *previousID*, the *currentID* obtained by the UPDATE procedure

Chameleon RFID Scheme

main procedure with the reader authentication

	RFID		System (via a reader)
		SETUP	
	($currentID, previousID$)		($presentedID, permanentID$)
		ROUND	
1.	$z := currentID$	$\xrightarrow{z}$	
2.			Find $presentedID$, where Hamming distance between z and $presentedID$ is $n/2$.
3.		$\xleftarrow{L}$	Choose at random a list L of k positions where z and presentedID differ
4.	check if $currentID$ and $previousID$ disagree on L		$presentedID := z$
5.	$previousID := currentID$		
6.	$\mathrm{UPDATE}(currentID)$		

Update procedure

Simplified version

for IDs of length $2n$:

1. choose n positions at random
2. flip the bits on these n positions

Full version

the IDs consist of $2n+1$ positions, each time n or $n+1$ positions chosen for flipping,

Recognition of a tag

Tag identification

- when the tag T sends its z, then z is not the *presentedID* from the database,
- ... however, z is derived by T from *presentedID* with the UPDATE procedure
- z and the *presentedID* of tag T differ on exactly n positions
- selected *presentedID* points to the *permanentID* of T

Reachability in Two Steps

Theorem

Any ID can be reached in just two updates

- w.l.o.g. we start with an all zeroes ID
- let the target ID K contain k ones, let L be the set positions of these 1's
- choose A_1, A_2 - sets of n positions such that:
  - both A_1 and A_2 contain $k/2$ positions from L
  - $A_1 \cap L$ and $A_2 \cap L$ are disjoint
  - $A_1 \setminus L = A_2 \setminus L$
- use the update with A_1 and then with A_2:
  - outside L each position is either not flipped or flipped twice
  - on L each position is flipped exactly once

Adversary's Point of View - Probability distribution

Probability distribution

- possibility of reaching in 2 Updates does not mean that each ID is reached with the same probability
- In fact probabilities are very different, the adversary can work with the most probable options

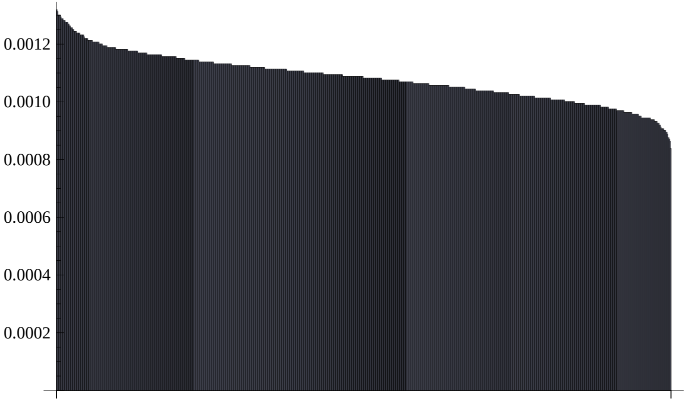
Intuition

after some number of interactions the probabilities get almost uniform logo2

Experimental Results

Chameleon RFID

Klonowski, Kutylowski,Syga



histogram of frequencies of all IDs after 8 Updates for 12-bit ID's

Analytic results

Goal

Estimate from above the distance between the uniform distribution and the actual distribution

Stochastic process

Markov chain model

- *currentID* is the state of the chain
- UPDATE defines the transition step of the Markov chain

Simple facts

probability distribution of this Markov chain converges to the uniform distribution (stationary distribution)

Coupling method

A powerful method for estimating the convergence rate of Markov chains

- two genuine copies of the original Markov chain run in parallel
- the transitions of the chains have some dependencies (this is the art to define then properly)
- **Coupling Lemma: if after t steps the states of both chains are the same with probability at least $1-\varepsilon$, then the probability distribution at step t differs from the stationary distribution by at most ε**

Definition of the Processes

Strategy

Run the first process freely; define the transitions of the second process dependent on the first process state and the transition chosen

States after step t

the first and the second process have the same bits apart from the positions from some set P

States after step t

assume that the first process chooses positions A for the update, the second process uses a set A' such that $A \setminus P = A' \setminus P$

Case 1: $A \cap P$ contains at most $|P|/2$ positions:

Case 2: $A \cap P$ contains more than $|P|/2$ positions:

Definition of the Process
continued

States after step t

assume that the first process chooses positions A for the update, the second process uses a set A' such that $A \setminus P = A' \setminus P$

Case 1: $A \cap P$ contains at most $|P|/2$ positions: choose $A' \cap P$ at random as a set disjoint from $A \cap P$, but with the same number of elements

Case 2: $A \cap P$ contains more than $|P|/2$ positions: choose A' so that $P \setminus A \subseteq A$ and $A \cap A'$ is chosen at random

Rationale Behind Rapid Mixing

Observation 1

Let $|A \cap P| = h$ and $|P| = k$

1. if $h \leq k/2$, then we remove $2k$ positions from P, so we are left with $2(k/2 - h)$ positions where they differ
2. if $h > k/2$, then we remove all but $2(h - k/2)$ positions from P.

Observation 2

If k is big, then h is close to $k/2$
It is easy to reduce k to small values .

Rapid mixing theorem

Theorem

Let us consider a tag with ID of the length $2n$ starting from an arbitrary state with even number of ones.

Then after $3.6 \log n + 2$ rounds its distribution differs from the uniform distribution over $2n$ bit strings with even number of ones, by no more than $\frac{1}{2n}$.

Rapid mixing theorem

Small n case

In fact the interesting case is that n is small. Then we can use concrete analysis instead of general formulas.
Even better results with simple combinatorics (an example in the paper).

Ambiguity and Splitting

Number of candidates

- each ID of length $2n$ has many other ID's with the Hamming distance n, the fraction of these ID's is about

$$\frac{1}{\sqrt{\pi n}}$$

  an this may lead to problems with tag identification (many candidates in the database
- solution: divide the ID into sub blocks of a small length (e.g. 10) and run the UPDATE independently on each sub block

Few application areas

Restricted areas

when a tag leaves a restricted area, then it becomes “contaminated” and cannot return back to the restricted area. The internal database does not keep external updates. The contaminated tag can live only outside.

Ownership transfer

Easy and robust transfer. After a few updates the previous owner knows nothing about the ID of the tag.
Unconditional security.

Leaked database

If the adversary gets the database with the ID’s, then still the adversary cannot start own readers in order to trace the tags.

Such an attempt would make the tags unusable.

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, +48 71 3202105
   fax: +48 71 3202105