Privacy and Security in library RFID

Issues, Practices and Architecture

David Molnar and David Wagner

University of California, Berkeley

CCS '04 October 2004

Overview

- Motivation
- RFID Background
- Library RFID Issues
  - Current Architectures, Attacks
- Private Library RFID Architecture
  - Private Collision Avoidance
  - Private Authentication
- Related Work, and Conclusions

Tagging

- RFID Tag – Small low cost device, limited data capacity
- Driving force
  - Logistics and supply chain applications
  - Proximity cards
  - Pet tracking
- Tagging pallets vs. Item level tagging
- Library RFID applications
  - Privacy implications in a concrete real-world setting

RFID Background

- Passive tags are powered only within range of a reader
  - Limited computation time
  - Out-of-range precomputation is impossible
- Extremely few gates (500-5000)
  - AES, #functions (SHA1) or pseudo-random functions
  - Simple password comparisons and XOR operations
- No physical security
- Economic pressure to manufacture 'inexpensive' tags

Library RFID Tags

Tag Type	Example Library	Example Vendors
Checkpoint WORM	Santa Clara City	Checkpoint
Checkpoint writeable	None	Checkpoint
TAGSYS C220-FOLIO	U. Delaware	VTLS, TechLogic
ISO 15693/18000-3 MODE 1	National U. Singapore	3M, Bibliotheca, Libramation
ISO 18000-3 MODE 2	Not yet available	Coming soon
EPC Class 1 13.56MHz	Not for library	WalMart
EPC Class 0 915MHz	Not for library	WalMart
EPC Class 1 915MHz	Not for library	WalMart

ISO 15693-3 and 18000-3 Mode 1 compliant (3M Library solutions)

- MODE-2 Tags (not currently offered)
  - High speed data transfer and communications
  - Random number generator, semi-nonvolatile RAM
- EPC (915 MHz) vs. Library RFID (13.56 MHz) tags

More data on Tags

- No strict regulation
- Interaction distance – 8 to 24 inches
  - Regulated by limitations on reader power and antenna size
  - Illegal readers?
- Eavesdropping possibilities
  - Asymmetry in signal strength
- Use of collision avoidance ID to track tags

Library RFID Architecture

- Limited scope for updating the system
- What's on the Tag?
  - Bar Code (from the bibliographic database)
  - Shelf location, last checked out date, author, title, etc
- How exit sensors work
  - Use of a security bit (needs to be set correctly)
  - Query database with Tag information (latency)
- Adversaries can track reading habits without the database!

Attacks on current RFID architectures

- Adversary characteristics
  - Access to a reader, no access to the bibliographic database
  - Power to perform passive eavesdropping and active attacks
- Static tag data, no access control
- Collision avoidance Ids
- Write locks, race conditions, Security Bit DoS Attacks
- Tag password management

Static Tag Data, without Access Control

- ID of tag remains constant throughout lifetime
- No read passwords or access control
- Privacy concerns
  - Profiling
- Tracking, in conjunction with other types of surveillance
- Hotlisting
  - Target marketing
  - Anecdotal evidence of hotlisting in practice

Collision Avoidance ID-s

- Globally unique and static collision ID
  - ISO 18000-3 Mode 1 – 64 bit MFR Tag ID,
    - Support inventory command with no access control
    - Slotted and non slotted collision avoidance
  - EPC Class 1 13.56 MHz use EPC identifier
  - ISO 18000-3 Mode 2 – 64 bit MFR id
    - Globally unique seed for PRNG may be derived from the MFR ID
  - EPC 915 MHz tags - Three collision avoidance modes
    - Adversarial reader asks tag to use the EPC ID

RFID hardware is incompatible with privacy concerns?

Security Bit DoS attack

- Vandalism of RFID tags
- Unprotected write commands, protected lock commands
  - No unlock command (EPC, ISO 18000-3 Mode1 / Mode2)
  - *Consistent only with supply chain requirements*
- Set security bit to desired value, and lock the tag!
- Write unique id in unlocked portion of the tag for tracking
- Adaptations
  - TAGSYS C220 – special area of memory for security bit
  - Checkpoint – Database lookup

Security Bit DoS (2)

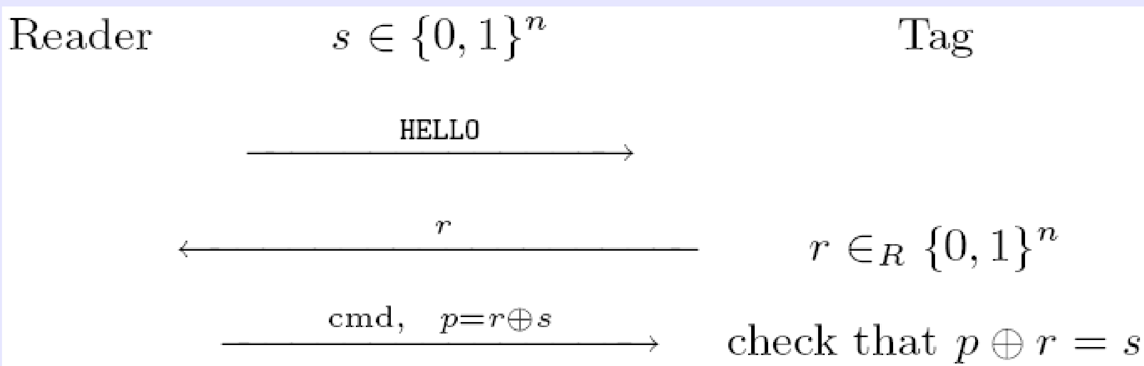
- Support lock/unlock/write commands
  - Hash locks
    - possibility of session hijacking
    - Bypass write lock by racing a legitimate reader
- Tags left unlocked by accident?
- Command sequences that force restarting collision avoidance

Tag Password Management

- Static passwords sent in the clear from the reader
- Single password per site – open to compromise
  - Write passwords required at checkout
- Different passwords per tag
  - Mapping tags to passwords?
  - Need to reconcile privacy and prudent password management

Tags with Private Collision Avoidance

- Random transaction Ids on Rewritable tags
  - Allows tracking, but not hotlisting
- Improved passwords via persistent state
  - Harder to eavesdrop on the tag to reader channel



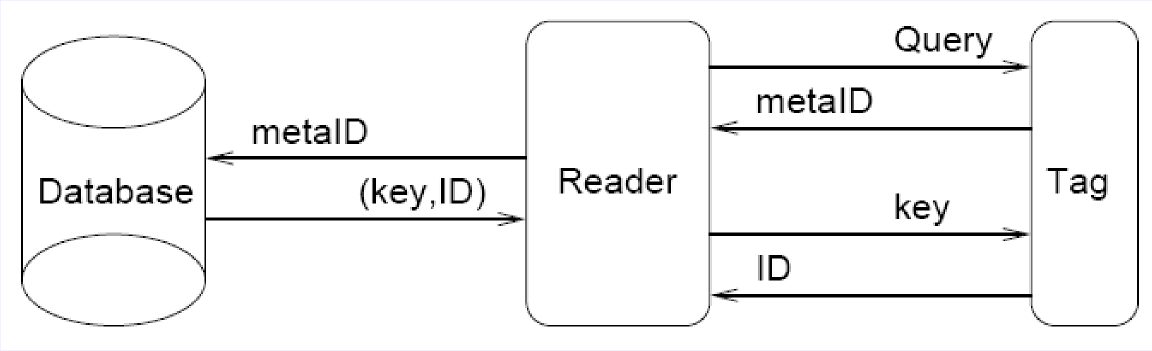
  - How to generate the nonce?

Private Authentication

- RFID Authentication scheme as a triplet of (Generator, Reader and Tag) probabilistic polynomial time algorithms
  - G(1k) – generator for TK, RK
  - Interaction between the algorithms T(TK) and R(RK)
- Privacy
  - Adversary unable to distinguish tags with different secrets
- Secure
  - Adversary needs secret key for interaction with tag/reader
- Performance - scalability

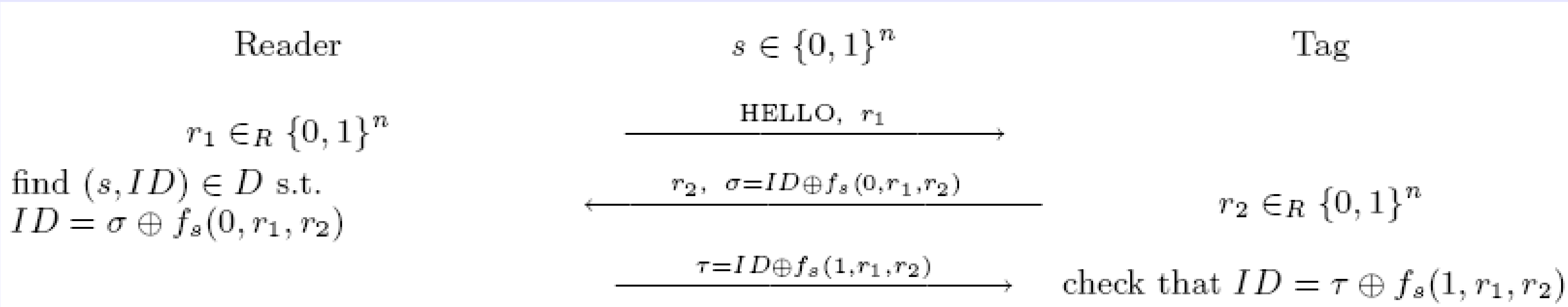
Lock Protocol (Weis et. al.)

- Set up: Tags are given a unique (s, ID) pair
  - Tag to reader (r, $f_s(r)$, ID)
  - Reader
    - Finds an ID consistent with the message
    - Send ID to Tag



- Use of backward channel
  - One time pads
- Chaff commands

Basic PRF private authentcation

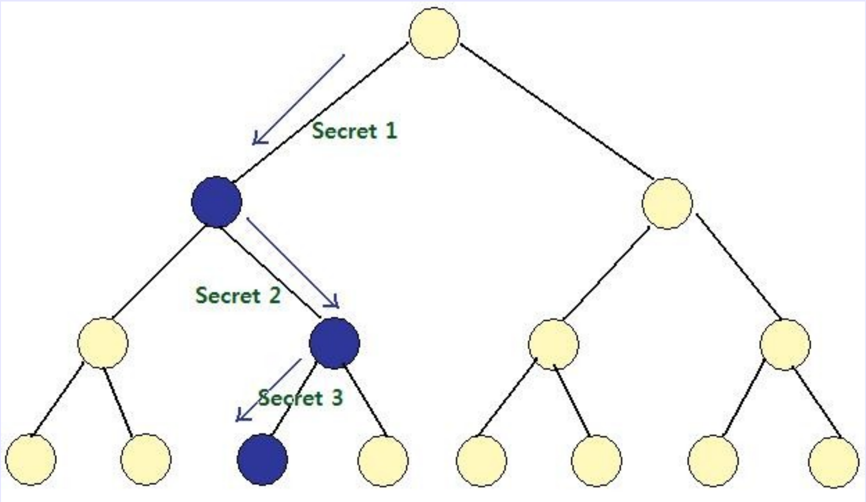


- $(G_{basic}, R_{basic}, T_{basic})$
- Reader workload linear in proportion to number of tags

Tree based Private Authentication

- O(n *lg* n) – reader work, tag storage, interaction rounds
  - Assumption - existence of a basic scheme

- Modifications:
  - Larger branching factors
  - XOR scheme instead of PRF
  - Perform all levels in parallel



Unoptimized algorithm (2)

Algorithm 4.1: $G_{\text{TREE}}(1^k, N)$

Fix $\ell \leftarrow \log N$
for $i = 1$ **to** ℓ
  for $j = 0$ **to** 1
    $s_{i,j} \leftarrow G_1(1^k)$
for $h = 1$ **to** N
  Parse h in binary as $(b_1, \ldots, b_\ell)$
  $TK_h \leftarrow (s_{1,b_1}, \ldots s_{\ell,b_\ell})$
$RK \leftarrow (s_{1,0}, s_{1,1}, \ldots, s_{\ell,1})$
Output $RK, TK_1, \ldots, TK_N$.

S[1,0]	001
S[1,1]	110
S[2,0]	101
S[2,1]	110
S[3,0]	111
S[3,1]	001

N = 3 k = 3

h : 1 to N	TK[h]
000	001 101 111
001	001 101 001
010	001 110 111
011	001 110 001
100	110 101 111
101	110 101 001
110	110 110 111
111	110 110 001

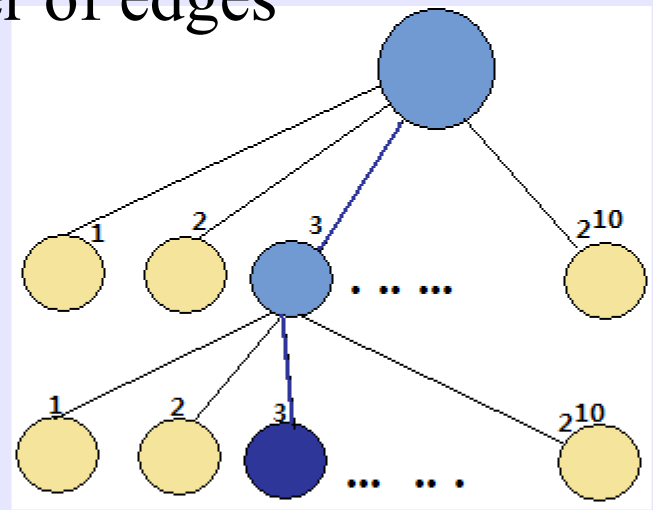
Unoptimized Algorithm (2)

Algorithm 4.2: $(R_{\text{TREE}}, T_{\text{TREE}})$ (RK, TK)

Fix $\ell \leftarrow \log N$
Parse RK as $(u_{1,0}, u_{1,1}, \ldots, u_{\ell,1})$
Parse TK as $(v_1, \ldots, v_\ell)$
for $i = 1$ **to** ℓ
  SUCCEED $\leftarrow$ **false**
  for $j = 0$ **to** 1
    if running $(R_1(u_{i,j}), T_1(v_i))$ returns true
      then SUCCEED $\leftarrow$ **true**
  if $\neg$SUCCEED
    then fail and output 0
accept and output 1

Two Phase Tree Scheme

- A fixed security parameter k for all levels ⟶ O(k *lg* n)
- Split into two phases to get communication O(k + *lg* n)
- Phase I – Run tree scheme with a constant security parameter to identify the tag
  - Branching factor vs. Security parameter of edges



Related Work

- Blocker Tags – not applicable in library settings
- Changing RFID Ids based on # chains
- Use of pseudonyms – prevents hotlisting, not tracking
- Security through obscurity and proprietary protocols
- “Best Practices” for Library RFID

Contributions

- Survey libraries' usage of RFID deployment
  - Analysis of vulnerabilities in real world deployments
- Private authentication as a key technical challenge
- Privacy friendly symmetric key authentication
  - Authentication of reader vs. Tag identification

Other comments

- Utilizing the physical characteristics of passive tags
  - Spoofing
    - reject tag replies with anomalous response times or signal power levels
  - Session Hijacking
    - Frequency Hopping
    - Passive tags designed such that their operating frequency is completely dictated by the reader.

Other Reads

- Item-Level Tagging Gains Momentum – Integrated Solutions Magazine, March 2008
- http://solutions.3m.com/wps/portal/3M/en_US/library/home/products/rfid_system/
- On the cryptographic applications of random functions (LNCS, 1985)
- Privacy aspects of low cost radio frequency identification systems (LNCS 2004)