RFID Security

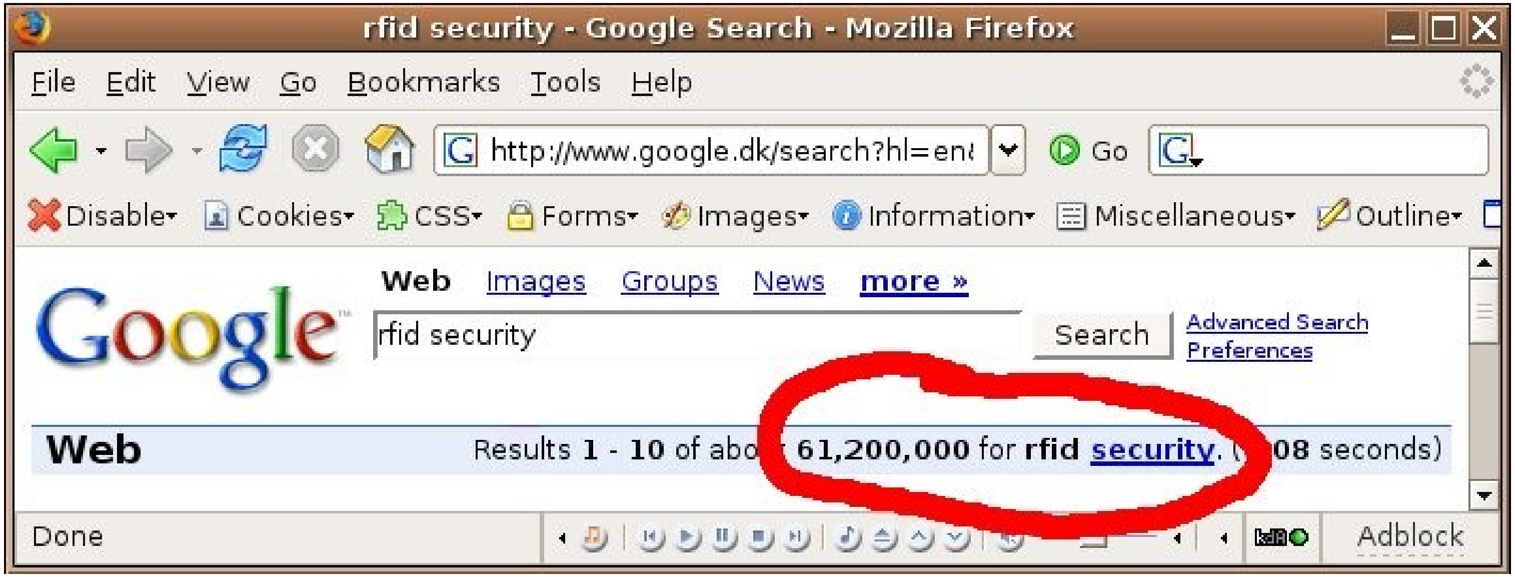
April 10, 2006

Martin Dam Pedersen
Department of Mathematics and Computer Science
University Of Southern Denmark

Outline

- What is RFID
- RFID usage
- Security threats
- Threat examples
- Protection Schemes for basic and advanced tags
- The future
- Literature

Plenty of information



rfid security - Google Search - Mozilla Firefox

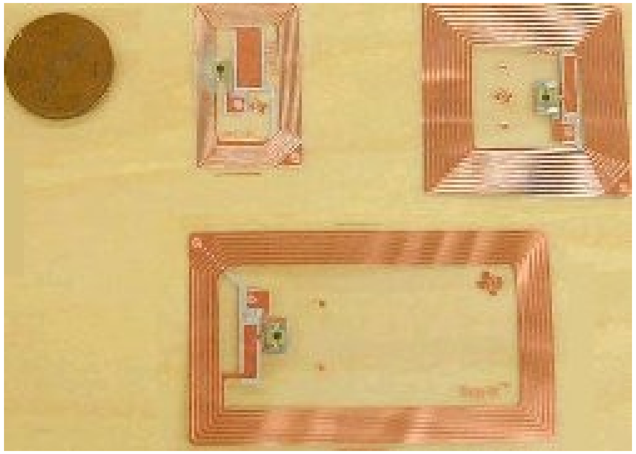
http://www.google.dk/search?hl=en

rfid security

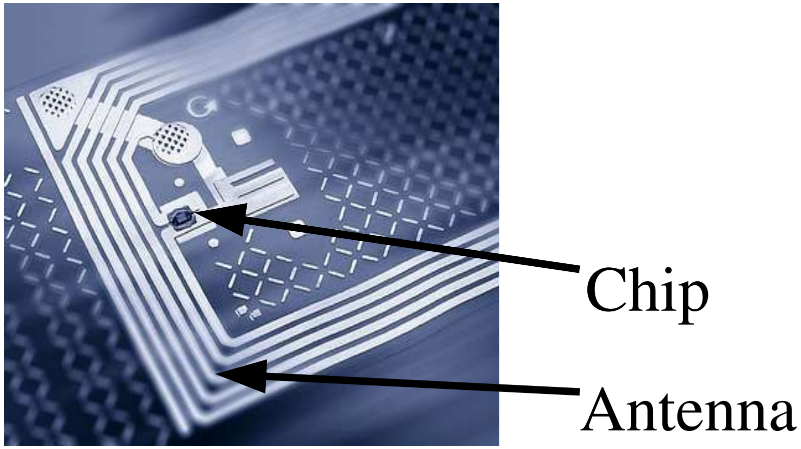
Results 1 - 10 of abo 61,200,000 for rfid security. (08 seconds)

What is RFID

- Radio-Frequency IDentification
  - RFID System
    - Tags
    - Readers
    - Backend servers



RFID System



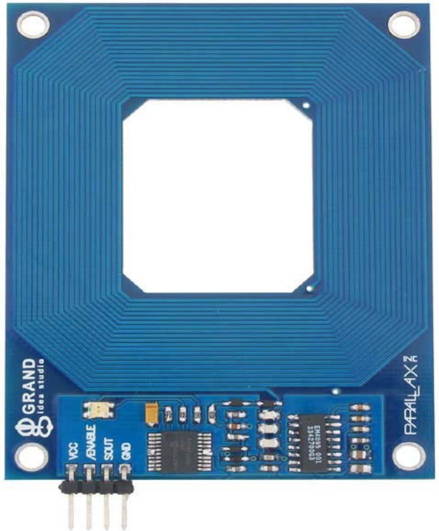
- Tag (transponder)
  - Small chip and antenna
  - Unique serial number
  - inexpensive(7.5cents)
  - Cryptography is possible in more advanced(Expensive) tags.
    - Symmetric-key
    - Public-key
    - Hashing

RFID System

- Tag types
  - passive(HF, UHF)
    - powered by reader and transmits a response
    - Very small(Chip 0.15mm×0.15mm, Antenna size of a stamp)
    - Read distances ranging from 2mm - 5m
  - semi-passive, active(small battery)
    - Self powered
      - active tags are fully self powered
      - semi-passive only powers it's circuit
    - size of a coin
    - larger ranges (>10 meters)

RFID Systems

- Reader (transceivers)
  - Read/Write data on tag
  - Communicates with back end system



RFID System

- Backend server
  - Stores information about tags
  - can perform necessary data computations
  - links tag-ids to more rich data

RFID usage

- Replacement of bar codes. EPC(Electronic Product Code) tags combined with Auto-ID gives unique serial numbers to items.
- Animal tracking

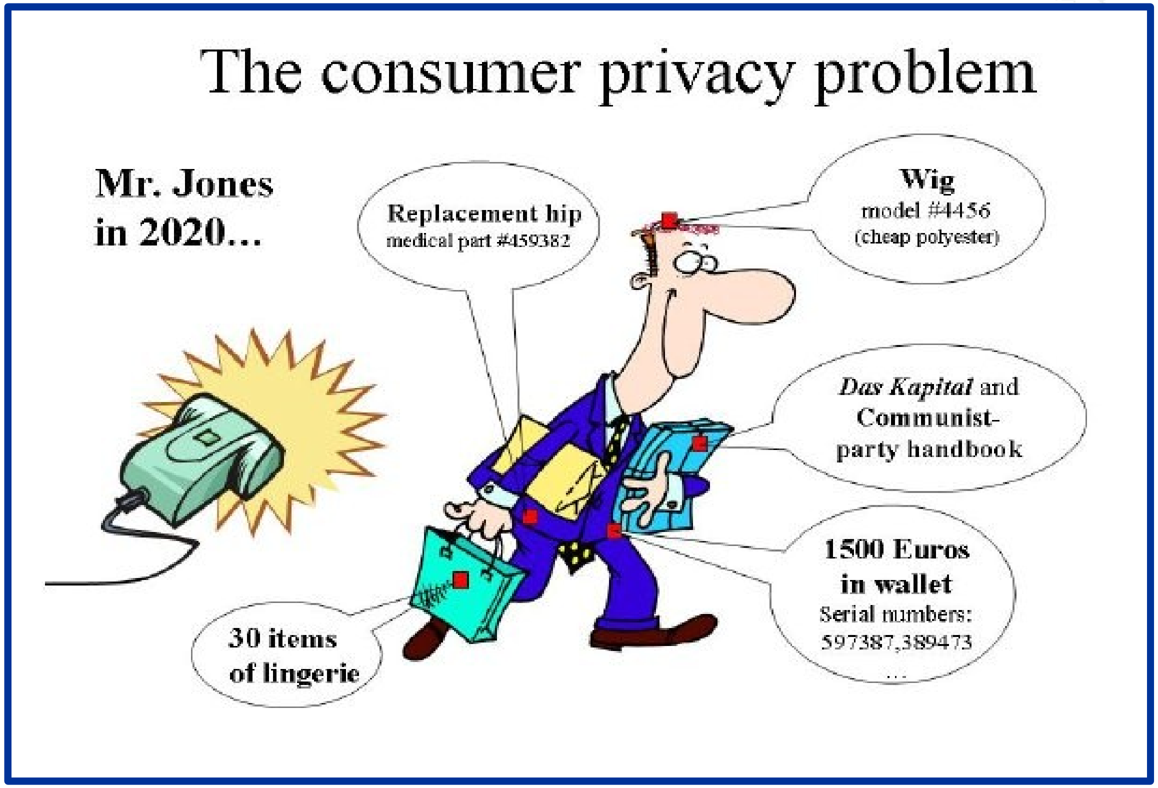
- Payment systems
  - Toll-payment at Storebæltsbroen (BroBizz)
  - Stockholm road pricing
- Anti theft
- Anti forgery

RFID usage

- Access control
- Supply chain
  - Inventory Control
  - Logistics
  - Retail shops
- Human implants
- Libraries
- Etc.......

Security threats

- Eavesdropping
- Cloning
- Spoofing
- Tracking
- DOS



Threat examples

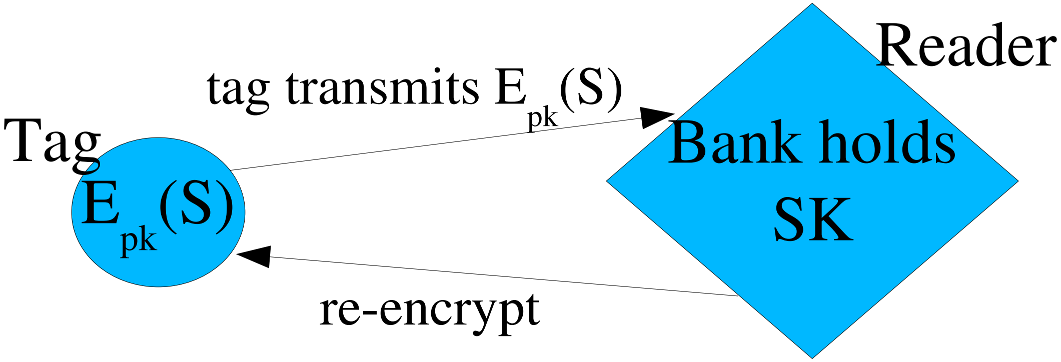
- Someone checking whats in your bag
- Cloning access control badges gives access to unauthorized personal in buildings/cars.
- Harvesting id's from store shelfs makes it possible to calculate how much is sold from the store.
- Tracking a persons movement, violating the concept of “location privacy”

Protection Schemes for basic tags

- Killing/Sleeping
  - using PIN
  - Special device incorporated in shopping bag.
  - If killed it's not usable in “smart” home devices.
- Collection of id's
  - Tag is sending a different id at each reader query
  - Reader stores all id's, and can therefore identify the tag.
  - To avoid harvesting id's, slow down responses when queried too quickly
  - Readers can refresh id's

Protection Schemes for basic tags

- Encrypting id, public/private key
  - ID on tag encrypted with the banks public key
  - Bank can decrypt with private key
  - to avoid tracking, re-encrypt periodically by El Gamal which gives a different cipher text.



Protection Schemes for advanced tags

- Hash Lock
  - Locked tag only transmits metaID.
  - Unlocked can do all operations.
  - Locking mechanism.

    1) Reader R selects a nonce and computes metaID=hash(key).

    2) R writes metaID to tag T.

    3) T enters locked state.

    4) R stores the pair (metaID, key).

Protection Schemes for advanced tags

- Hash Lock
  - unlocking mechanism.

    1) Reader R queries Tag T for its metaID.

    2) R looks up (metaID,key).

    3) R sends key to T.

    4) if (hash(key) == metaID), T unlocks itself
  - Spoofing attack is possible, but can be detected.

Protection Schemes for advanced tags

- Symmetric key tags
  - $C = E_k(M)$
  - Challenge-response protocol

    1) Tag identifies itself by transmitting T

    2) Reader generates a nonce N and transmits it to the tag

    3) Tag computes and returns $C = E_k(N)$

    4) Reader checks that C indeed is equal to $E_k(N)$.

Protection Schemes for advanced tags

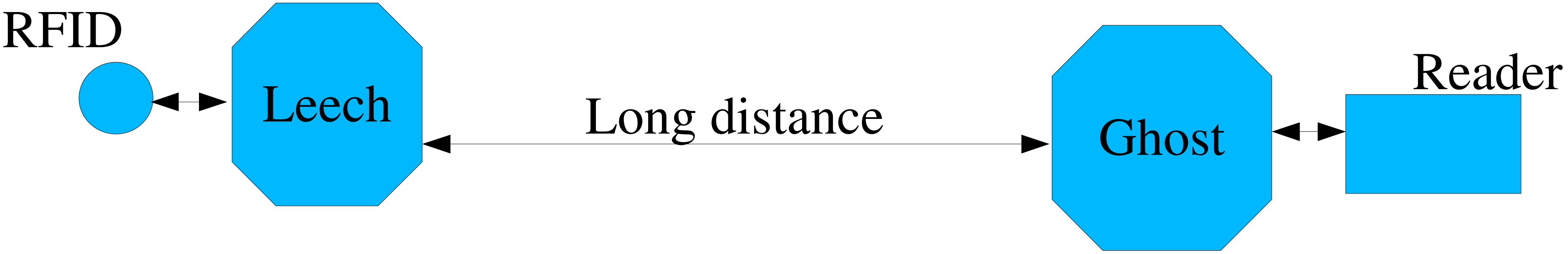
- Symmetric key tags
  - If implemented in the right way, almost impossible to break.
  - In practice resource constraints leads to bad implementations.

Protection Schemes for advanced tags

- The Digital Signature Transponder(DST) from TI(texas Instruments)
  - Theft protection in cars. Used in SpeedPass™(payment device to ExxonMobil petrol stations)
  - Performs a challenge-response protocol.
  - $C = E_k(R)$, where R is 40 bits, and C is 24 bits, secret key k is 40 bits.
  - The short key is vulnerable to brute force attack.
  - TI did not publish the encryption algorithm E, “security by obscurity”.
  - Cracked in 2004 !!

Protection Schemes for advanced tags

- Man-in-the-middle-attack
  - Almost any security application of RFID, involves a presumption of physical proximity.
  - Can bypass any cryptographic protocol
  - Phone equipped with a GPS receiver could sign outgoing messages.



The future

- More and more RFID tags in new applications
- D.O.S. becomes a larger problem
- Cheaper tags makes it possible to build in more advanced cryptography for the same money
- Probably don't replace bar codes completely because of the cost(5 cent tag on a 29 cent chocolate bar) .

Literature

- Ari Juels, RSA Laboratories: ”RFID Security and Privacy: A Research Survey”
- RSAlabs page on rfid: http://www.rsasecurity.com/rsalabs/node.asp?id=2115
- Wikipedia: http://en.wikipedia.org/wiki/Rfid
- Stephen August Weis: “Security and Privacy in Radio-Frequency Identification Devices”
- http://www.rfidjournal.com/