Strengthening EPC Tags Against Cloning

Ari Juels

RSA Laboratories

Bedford, MA, USA

WiSE'05, September 2, 2005, Cologne, Germany. Pg 67-75

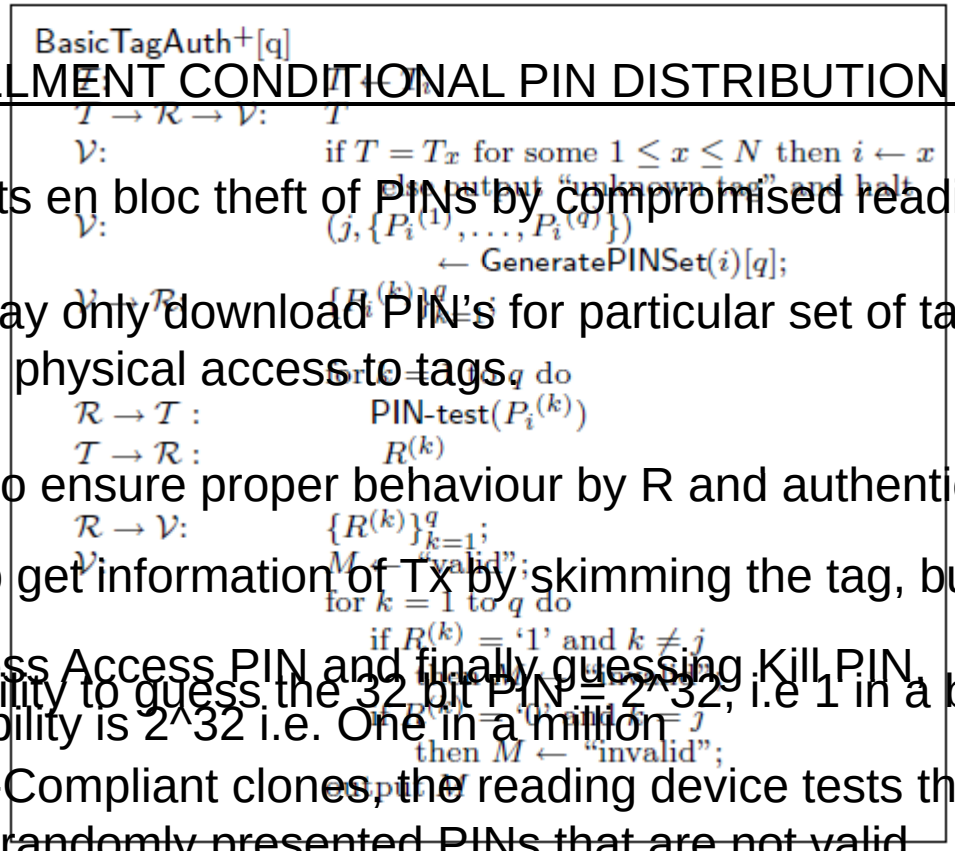
Presented by: Sagar Kapoor

SUMMARY

- This article discusses the possibility of EPCglobal Class1 Generation2 UHF tags(EPC tags) as a potent mechanism for object identification.

- Article presents simple techniques to strengthen the resistance of EPC tags against elementary cloning attacks.

PROTOCOLS



FULFILLMENT CONDITIONAL PIN DISTRIBUTION (FCPD)

Prevents en bloc theft of PINs by compromised reading devices.

User may only download PIN's for particular set of tags if it appears to have physical access to tags.

Aim is to ensure proper behaviour by R and authenticity of tags

Easy to get information of Tx by skimming the tag, but not 32 bit PIN.

To guess Access PIN and finally guessing Kill PIN.

Probability to guess the 32 bit PIN = 2^32, i.e 1 in a billion

Probability is 2^32 i.e. One in a million

For Non-Compliant clones, the reading device tests the response of tag to randomly presented PINs that are not valid.

For untrusted readers

Probability of successful attack is just 1/q.

Probability of successful attack is just 1/q.

APPRECIATION 1

- Techniques presented looks promising.
- Current scenario is being discussed with facts
  - " Media reports have suggested such a plan by the European Central Bank to combat counterfeiting of Euro banknotes "
  - " More recently, the U.S. FDA (Food and Drug Administration) has issued a report that endorses RFID as a tool to combat the counterfeiting of pharmaceuticals "
  - "The United States Department of Defence and several dominant retail corporations such as Wal-Mart have mandated the use of RFID tags by their top suppliers beginning in 2005 "
- No false promises made.
  - " These protocols do not defend against a full range of attacks, but still have significant practical application. "
  - " We emphasize that our techniques defend only against a limited set of attacks "
- Bold challenges
  - " Our techniques can strengthen EPC tags against cloning even in environments with untrusted reading devices. "
  - "EPCglobal Class-1 Generation-2 UHF standard for EPC tags, which is likely to predominate in supply chains. "
  - " we believe that users will come to rely implicitly on RFID tags to authenticate goods. "

CRITICISM 1

- Does it work .. ??
  - Nothing is presented in the article showing that the schemes were tested.
- Schemes proposed not discussed in details
- Examples mainly human engineered.
  - Excon Corp- a shipping company- swaps in the bogus cases while it has custody of the real ones.
  - Dupyu Stores- Dupyu staff attach cloned tags to counterfeit, look-alike packages
  - A seller of counterfeit handbags can attach EPC tags carrying duplicated, valid EPCs

CRITICISM 2

- Failed to define “ Valid ”
  - For clarity of notation, let us denote by PIN-test(*K) an* EPC-tag (meta-)command that causes a tag to output a bit-response *b. The value of b is a ‘0’ if K is the correct kill PIN* for the tag and ‘1’ otherwise
- Assumption of a secure reader and server
- Techniques proposed cannot be used for stronger attacks.

QUESTION

Can we rely on the techniques presented in the article?

Doesn't the assumption of secure server/reader looks like a compromise to security?

THANK YOU