



- SOFTWARE
- Desktop Software
- Enterprise Software
- Supply Chain Management Software
- Operating Systems Software
- Systems Management Software
- Service Oriented Architecture (SOA) and Web Services
- Business Intelligence Software
- Database Software
- Storage Software
- Security Software

Security Software

Send to a friend Print

Short keys leave UK passports open to hackers

Author: [Ian Grant](#)
Posted: 12:48 18 Sep 2009
Topics: [Security](#)



UK and Dutch passports can be hacked using brute force because they use short keys to protect the information on their embedded RFID chips, an RFID expert told the European Network and Information Security Agency (Enisa) this week.

The US had chosen a longer key for its identity documentation and was thus better protected, security firm RSA's Ari Juels told Enisa's summer school this week.

Juels said the use of radio frequency identification (RFID) tags was likely to increase vastly because they were so useful for tracking things and recording their histories. But privacy, counterfeit and unauthorised reading concerns needed addressing, he said.

The tags were getting cheap and powerful enough to carry "reasonable" protection such as AES encryption and challenge and response processing, he said.

Key management was the biggest problem, but it could be overcome by having the tag carry its own key, or rather a part of the key, he said.

Splitting the key using a technique called dsecret sharing between several items that were likely to travel together reduced the risk of the key being discovered, he said.

This allowed a farmer to microchip his herd of cows, but because each cow carried only part of the key, its identity could not be discovered unless the rest of the herd was present to complete the key.


A similar principle could be applied to passports and identity cards, drugs and other high value items he said.

The use of RFID chips as vehicle anti-theft devices, where the tag on the key had to match the tag on the car, had cuts thefts by 90%, he said.

The advantage of this was that once the goods were sold or otherwise ended their journey, the key disappeared, he said.

This solved the retailers' problem of having to "kill" tags at the point of sale to stop them from being used to trace the consumer's subsequent journey.

AUTHOR PROFILE



Ian Grant

- Email Ian
- articles by Ian

RELATED CONTENT

- CW Articles
- Web Content
- Enisa publishes IT security report on 30 countries
- Everything you wanted to know about Web 2.0 Security and Privacy
- EC forms a single cyber security agency for Europe
- Uncontrolled printing
- Hackers help get news out of Iran

RELATED DOWNLOADS

- WHITEPAPER**
The sheer volume of email poses new challenges for IT Managers. Email forms part of the business records within all organisations, and secure, retrievable management of email records is essential.
- PODCAST**
RSA's Art Coviello on IT security in the credit crunch.

- WHITEPAPER**
Working from home is on the increase; but the threats remain. Spyware, and viruses are lurking and inappropriate web use presents legal risks & security threats.

SPONSORED LINKS

- SIGN UP TO**
- Digital Magazine
 - Print Magazine
 - Email Newsletters
 - RSS Feeds
 - News Widgets
 - Research Panel
 - Mobile News
 - Events

- DOWNTIME**
- Photo Stories
 - Dilbert
 - Sudoku
 - Puzzler
 - Downtime blog
 - Videos

Stay a step ahead
with the most relevant
offerings from
ComputerWeekly.com's
Industry Resources

[LEARN MORE](#)

RELATED TAGS

[ari juels](#) [european network](#) [information security](#) [keys leave](#)
[leave uk](#) [passports open](#) [rfid chips](#) [rfid expert](#) [security](#)
[agency](#) [uk passports](#)

 [Send to a friend](#)  [Print](#)

ADVERTISEMENT

ADVERTISEMENT

ADVERTISEMENTS

PRODUCTS & SERVICES

-  [RSS](#)
-  [Email Newsletters](#)
-  [Digital Magazine](#)
-  [Blogs](#)
-  [Webinars](#)
-  [Videos](#)
-  [Podcasts](#)
-  [Whitepapers](#)

[Photo Stories](#)