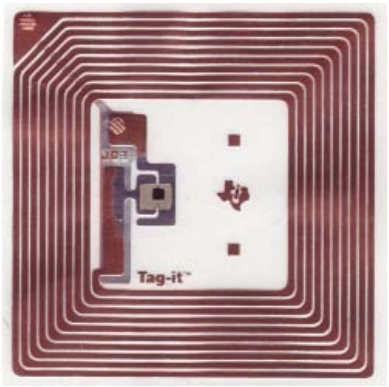
17 September 2009, 09:48

« previous | next »

Privacy for RFID tags



A Texas Instruments RFID tag

A common complaint about proposals to use RFID (Radio Frequency Identity) to tag everything from bank notes to underwear is that it opens the way for sophisticated privacy invasion. Someone with a reader could, once RFID is pervasive, read the valuables you're carrying, the contents of your wallet, and plan an attack accordingly. The solution so far: a kill function to disable the tags at the point of sale.

Speaking at this week's Enisa-Forth Summer School on Network Information and Security, RSA chief scientist Ari Juels noted problems with the kill function, mostly to do with key management: "Cryptography is not hard; managing privileges is hard."

Juels' idea – which he worked on with colleagues Bryan Parno and Ravi Puppu – is instead to share a secret key across a group of tags. For example, split the key across the RFID tags on each of a set of bottles. A pharmacy taking delivery can check and store the keys transparently. "You can reconstruct the key when the bottles are together," he explained. "But when the bottles are dispersed, the key essentially vanishes. You have automatic privacy protection. Plus, no kill function – and no key management burden through the supply chain."

One problem is that this system invalidates one of the promises usually made about using RFID tags; users will be able to check the tags themselves as an anti-counterfeiting measure. Juels admits that's true, but says there are alternative solutions to that. "Treating the fundamental privacy problem is so challenging that more sophisticated functions will have to wait."

In other recent work, Juels and colleagues cloned a State of Washington electronic driver's licence and showed it could be read at a range of more than 50 metres under experimental conditions – and at 0.5 metres in the State-supplied protective sleeve.

(Wendy M. Grossman)

(trk)

Add your comment

Print version | Send by email

« previous | next »

Share this article

Internet Toolkit

- Anti-Virus
- Browsercheck
- Emailcheck
- Conficker test
- Test SSL certificates
- Whois query
- My IP address
- Traceroute
- DNS query
- Subnet calculator
- MAC addresses
- RFCs
- Ping
- Bandwidth calculator
- Spam list query
- IP addresses

H SECURITY

All Around My (Black) Hat

Wendy Grossman reports on the proceedings at the Black Hat security conference 2009

Protecting SSH from brute force attacks

Using just open source tools and a few tweaks, it is possible to detect and block suspicious login attempts

The H Security Conficker information site

The H Security information page on Conficker is where you can find the latest stand-alone removal tools, news, scanners and tips about the Conficker worm.

HOT ON H

Testing email with encryption

It can be very useful to be able to talk directly with your SMTP or IMAP server for diagnostic purposes. Things get a bit more complicated when encryption rears its ugly head, but with the right tools, it doesn't have to be a black art

The path to GNOME 3.0

GNOME release manager Vincent Untz talks to heise open and The H about the projects future plans for the popular desktop manager

Trademarks - The dinosaur in the room

Branding is just as vital to the success of FOSS projects as it is to proprietary software. Richard Hillesley examines the importance of trademarks for open source

H OPEN

The Next Round – The new features of Linux 2.6.31

New features include the support of Kernel-Based Mode-Setting (KMS) and USB 3.0 as well as drivers for the Sound Blaster X-Fi. The developers also made a considerable number of further improvements to the experimental Btrfs and added performance counters

Linux and Digital Rights Management (DRM)

The principles of open source software and the film and record companies' perceived need to control how film, video and audio recordings are consumed seem incompatible. This article explores the issues

What's new in Red Hat Enterprise Linux 5.4

The latest RHEL version offers numerous virtualisation advancements and enhances its hardware support via countless upgraded and extended drivers

HITS OF THE H

Open source stars for Mac OS X: Part 1

Open source isn't just for Linux users, there are many excellent free open source applications available, ready to run, for Apple OS X too. Part 1 of this 2 part feature looks at alternative browser, mail, messaging, productivity and image editing apps.

The Btrfs file system

Btrfs, the designated "next generation file system" for Linux, offers a range of features that are not available with other Linux file systems – and it's nearly ready for production use

Build a Wi-Fi antenna using household materials

You can make your own directional Wi-Fi antenna using commonplace items like a toilet brush holder. Here's how

Welcome to The H

The H is the new name for heise online UK. The H is about security and open source. Read more of what The H is about

The H
Last 7 days
News Archive
Features
Forums

The H open source
Last 7 days
News Archive
Features
Forums

The H Security
Last 7 days
News Archive
Features
Forums

The H Internet Toolkit
Anti-Virus
Browsercheck
Emailcheck
Test SSL certificates
Whois query

My IP address
Traceroute
DNS query
Subnet calculator
MAC addresses

RFCs
Ping
Bandwidth calculator
Spam list query
IP addresses

Privacy Policy Contact us