RFID Transponder Security Overview

Vendor	Tag	Frequency	Function	Mem (bits)	Authentication	Encryption	UID (bits)	Emulation Possible	Secure	Doc
Atmel	Temic T5557	125 kHz	r/w	330	32Bit Password Send in clear	no	40	yes	no	1
	Temic T5567									2
	Temic T5577			363						2
NXP	Hitag1	125 kHz		2048	2x32Bit Keys and 4x32 Bit Passwords	yes	32		no	3
	Hitag2			256	48Bit Key and 24 Bit Password					4
	HitagS-256					no				5
	HitagS-2048			2048						5
	Mifare Classic	13,56 MHz		8K und 32K	48Bit Key	yes	32 oder 56			13
	Mifare Desfire			32K	112Bit Key		56		no	14
	Mifare Desfire EV1			16K, 32K, 64K	56, 112, 128, 168 Bit			no	yes	
	Mifare Desfire EV2									
EM Microelectronic	EM4450	125 kHz		1024	32Bit Password Send in clear	no	32	yes	no	6
	EM4550									6
	EM4205			512						7
	EM4305									7
	EM4469						32 plus 10 Bit CustomerCode			8
	EM4200		Readonly (UID)	0	no		128		no	9
	EM4100						64			10
	EM4102									11
	TK4100									12
Legic	Prime	13,56 MHz	r/w	1-16K	no	no	32	yes	no	15
	Advant			16-64K	56, 112, 128, 168 Bit	yes	56	no	yes	

Updated: 2016-01-08/2

OpenSource Security
Am Bahnhof 3-5
48565 Steinfurt
info@os-s.de
http://www.os-s.de

Datasheets

1 http://www.apdanglia.org.uk/ATMEL%20T5557%20RFID%20TAG%20SPECS.pdf
2 http://www.atmel.com/images/atmel-9187-rfid-ata5577c_datasheet.pdf
3 http://www.nxp.com/documents/short_data_sheet/HT1X_SDS.pdf
4 http://www.nxp.com/documents/short_data_sheet/HT2X_SDS.pdf
5 http://www.nxp.com/documents/short_data_sheet/HTSICH56_48_SDS.pdf
6 http://www.emmicroelectronic.com/sites/default/files/public/products/datasheets/em4450_ds.pdf
7 http://www.emmicroelectronic.com/sites/default/files/public/products/datasheets/em4205-4305_ds.pdf
8 http://pdf.datasheetcatalog.com/datasheets2/31/312814_1.pdf
9 http://www.emmicroelectronic.com/sites/default/files/public/products/datasheets/em4200_ds.pdf
10 http://www.mikroe.com/download/eng/documents/development-tools/components/em4100_datasheet.pdf
11 http://www.nesweb.ch/downloads/X400RFID.pdf
12 http://www.cika.com/soporte/Information/Tarjetas/Rfid/TK4100_DATA.pdf

Hacking Reports

13 http://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2008-21/SAR-PR-2008-21_.pdf
14 https://www.iacr.org/workshops/ches/ches2011/presentations/Session%205/CHES2011_Session5_1.pdf
15 https://srlabs.de/blog/wp-content/uploads/2010/07/100616.EUSecWest.LegicPrime.pdf

Color Legend (Emulation Effort)

Currently secure. No vulnerabilities known.

Published attacks. Very complex and resource intensive.

Access to transponder*, reader (lock) and transponder* required **

Access to reader (lock) and transponder* required.

Only access of the transponder* required

* In all cases no physical access to the transponder is needed.
Radio access (1-30 cm) is usually sufficient.

** The attack requires several steps:
1. Reading the UID of the transponder to be emulated
2. Communicating with a valid reader (lock)
3. Breaking the key used (< 5min)
4. Reading the transponder completely