Клонирование Mifare

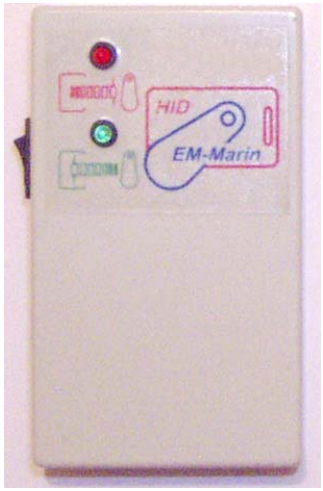
Клонирование UID Mifare карты, как состоявшийся факт и его последствия при использовании в качестве идентификатора в СКУД.

С чего начиналось

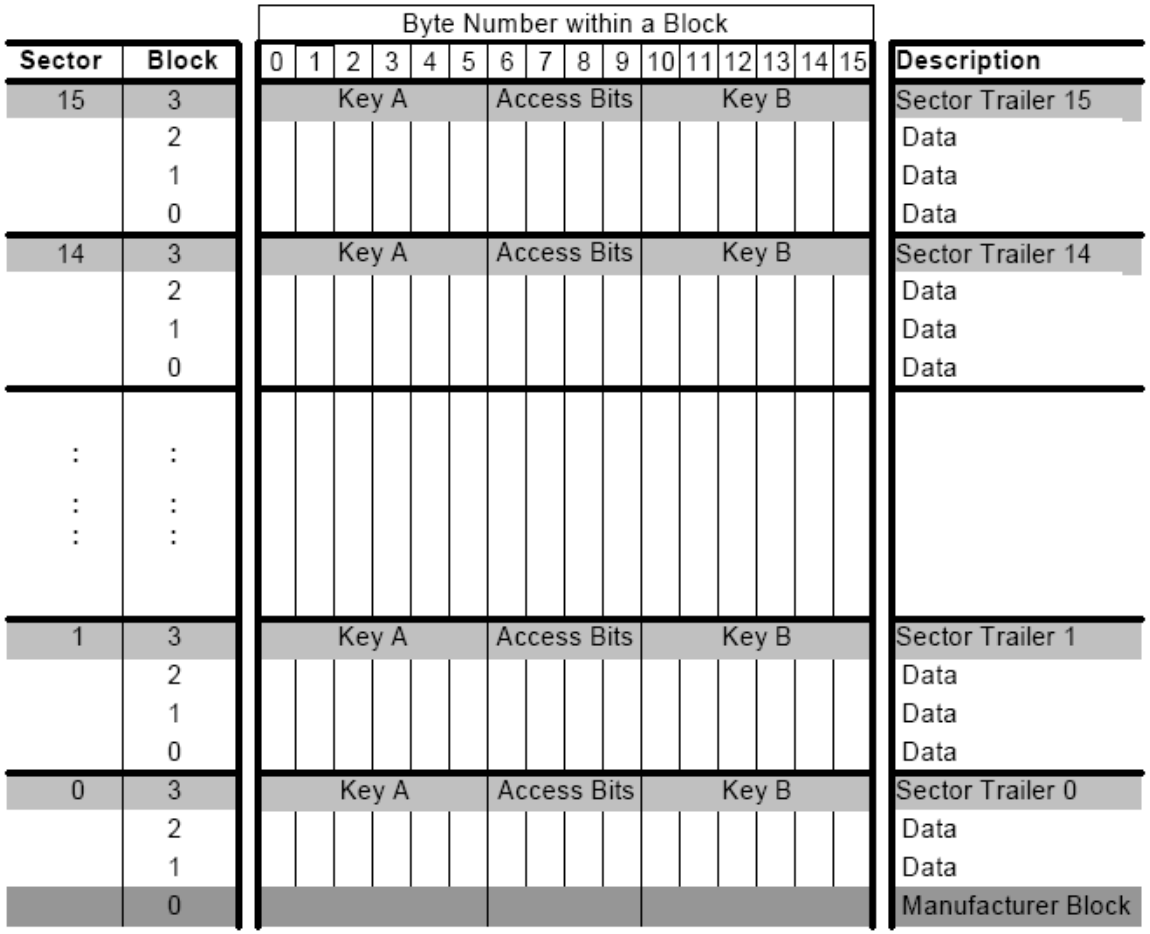
- Em-marin 125Khz

Бегство от Em-marin

Дубликаторы

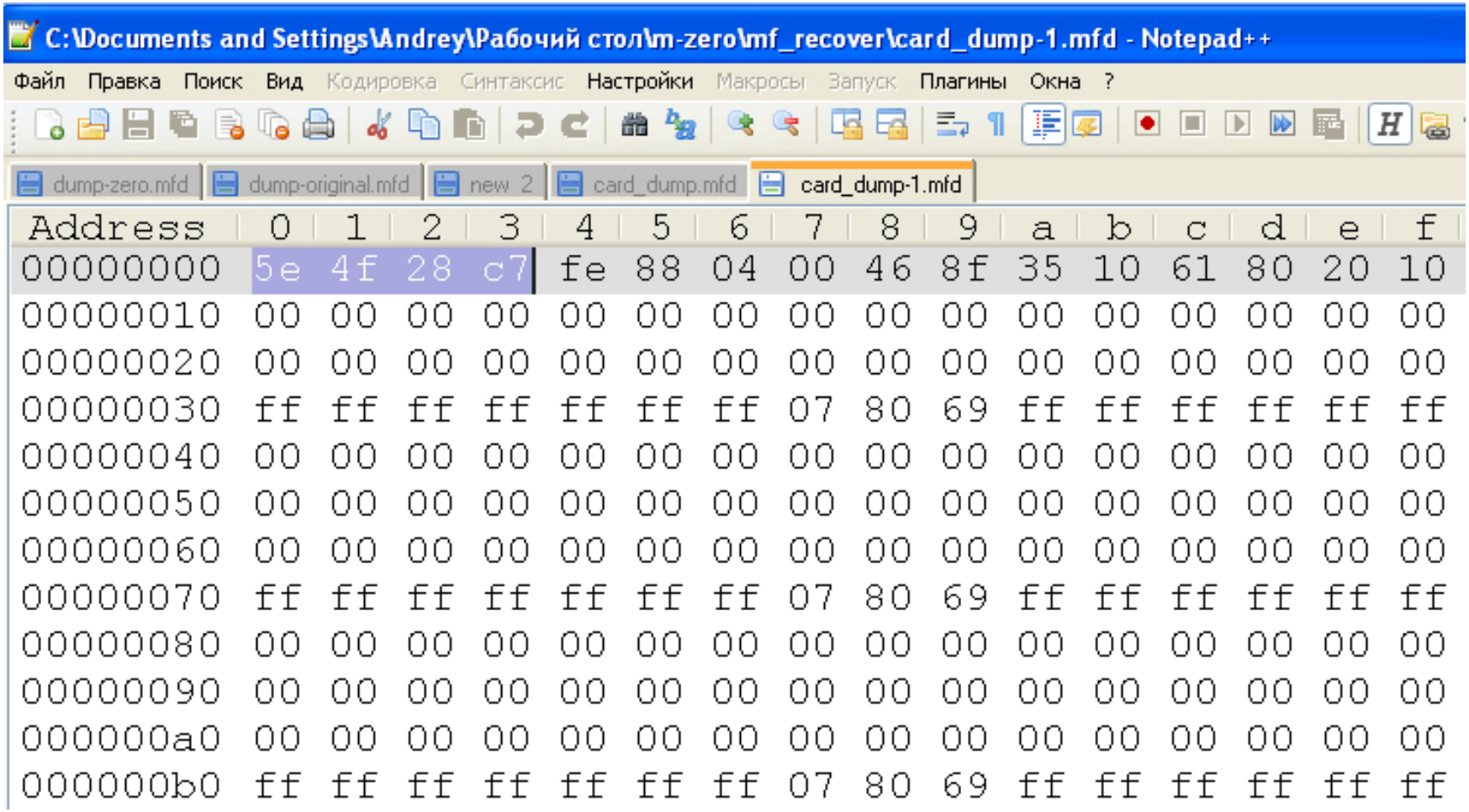


Как устроен Mifare



Sector	Block	Byte Number within a Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Description
15	3	Key A | Access Bits | Key B	Sector Trailer 15
	2		Data
	1		Data
	0		Data
14	3	Key A | Access Bits | Key B	Sector Trailer 14
	2		Data
	1		Data
	0		Data
:	:		
:	:		
:	:		
1	3	Key A | Access Bits | Key B	Sector Trailer 1
	2		Data
	1		Data
	0		Data
0	3	Key A | Access Bits | Key B	Sector Trailer 0
	2		Data
	1		Data
	0		Manufacturer Block

Теперь по настоящему

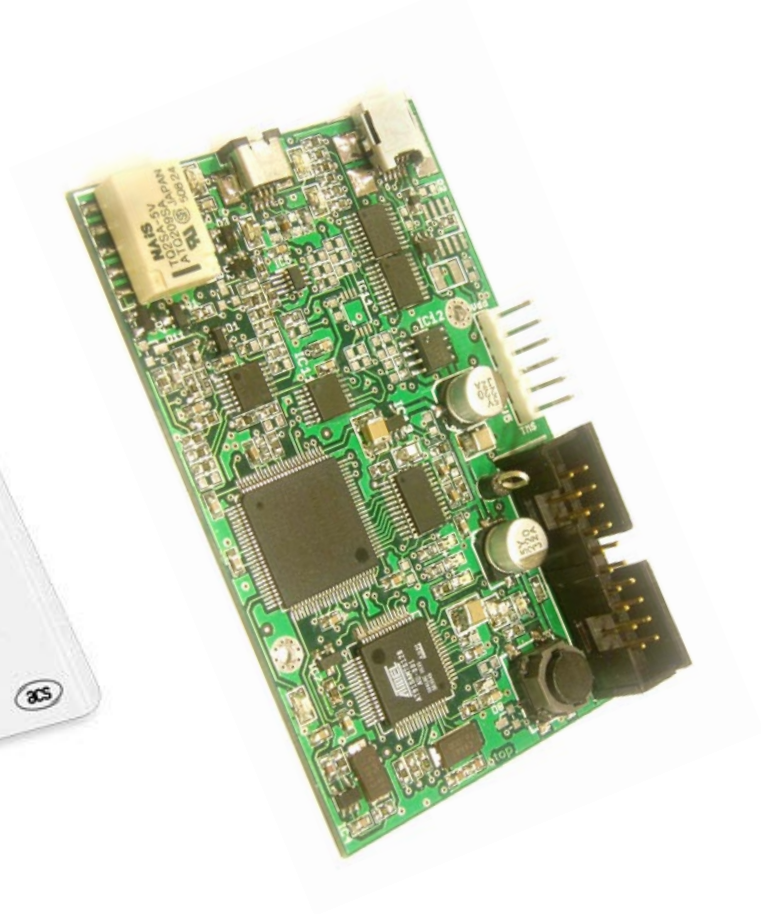


Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	5e	4f	28	c7	fe	88	04	00	46	8f	35	10	61	80	20	10
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000b0	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff

Mifare – держался до 2011

- 27 октября 2010 год

Манипуляции с UID Mifare



Mifare Zero

ATR: 3B 8F 80 01 80 4F 0C A0 00 00 03 06 03 FF 88 00 00 00 00 1C

Manufacturer	Product	ATQA	SAK	ATS (called ATR for contact smartcards)	UID lenght
NXP	MIFARE Mini	00 04	09		4 bytes
	MIFARE Classic 1k	00 04	08		4 bytes
	MIFARE Classic 4k	00 02	18		4 bytes
	MIFARE Ultralight	00 44	00		7 bytes
	MIFARE DESFire	03 44	20	75 77 81 02 80	7 bytes
	MIFARE DESFire EV1	03 44	20	75 77 81 02 80	7 bytes
IBM	JCOP31	03 04	28	38 77 b1 4a 43 4f 50 33 31	
	JCOP31 v2.4.1	00 48	20	78 77 b1 02 4a 43 4f 50 76 32 34 31	
	JCOP41 v2.2	00 48	20	38 33 b1 4a 43 4f 50 34 31 56 32 32	
	JCOP41 v2.3.1	00 04	28	38 33 b1 4a 43 4f 50 34 31 56 32 33 31	
Infineon	MIFARE Classic 1k	00 04	88		
Gemplus	MPCOS	00 02	98		
Innovision R&T	Jewel	0c 00			
Nokia	MIFARE Classic 4k - emulated (6212 Classic)	00 02	38		4 bytes
	MIFARE Classic 4k - emulated (6131 NFC)	00 08	38		4 bytes

Ловим клон

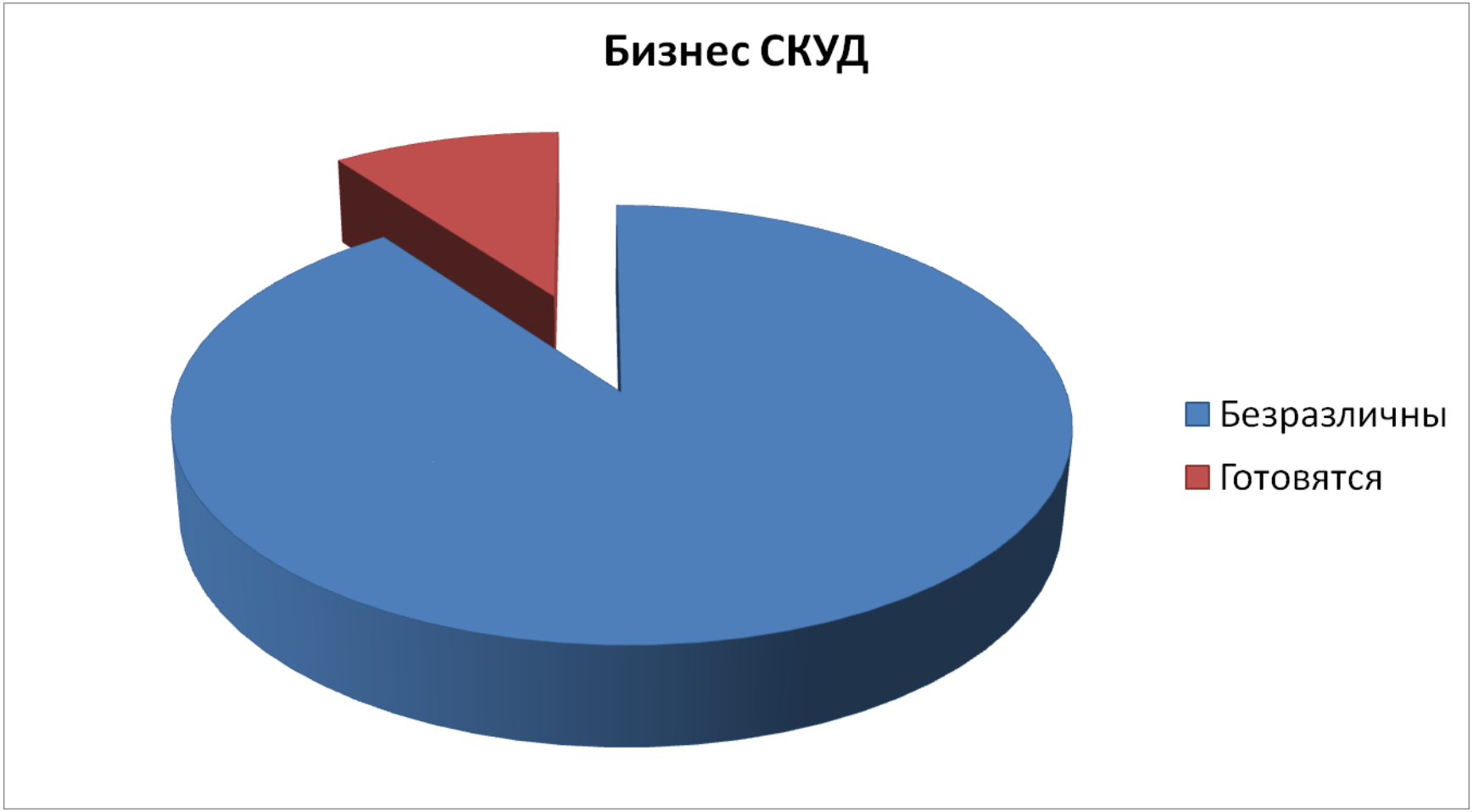
- По изготовителю
  - ATR (*Answer To Reset)*
  - ATQUA *(Answer To reQuest (Type A))*
  - SAK *(Select AcKnowledge)*
- APDU *(Application Protocol Data Unit)*для блока производителя
- Запись тайминга в сектора и синхронизация с базой

Технологии на шаг впереди

Бережём ключи от секторов

- Слабое звено
  - Mifare Classic
  - Человеческий фактор
- Обязательно использовать зашифрованные сектора при авторизации
- Анализ активности
- Замена карт по-творчески

Не инвестируем в безопасность



Закон с нами

- Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

- Статья 159. Мошенничеството есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием

Мера ответственности

- Продавать Mifare Zero – законно
- Вне закона если это:
  - Общественный транспорт
  - Горнолыжные подъемники
  - Вход в ресторан гостиницы
  - Парки отдыха
  - Планетарии
  - Культурно-развлекательные заведения
  - Игровые автоматы
  - Платные парковки

Конец

Андрей Цуманов
+7 (495) 771-57-89