Lightweight Cryptography and RAIN RFID

Matt Robshaw
Technical Fellow, Security Solutions

NIST, October 17-18, 2016

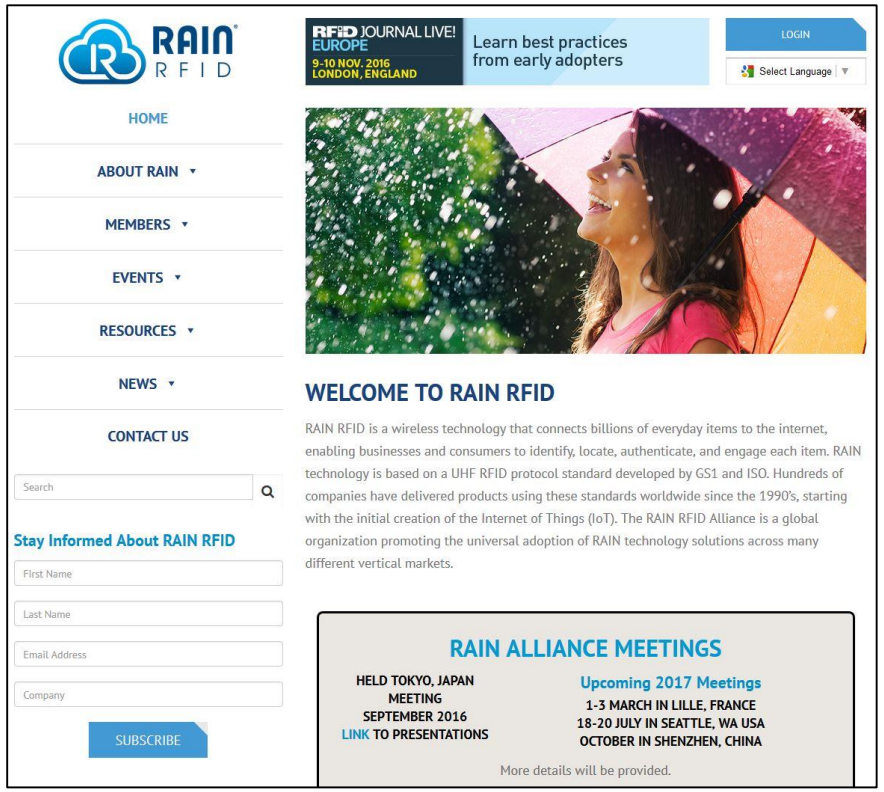
Overview

- RAIN RFID
- The product and standardization landscape
- Security and performance
- NISTIR 8114: Profile feedback
- Questions

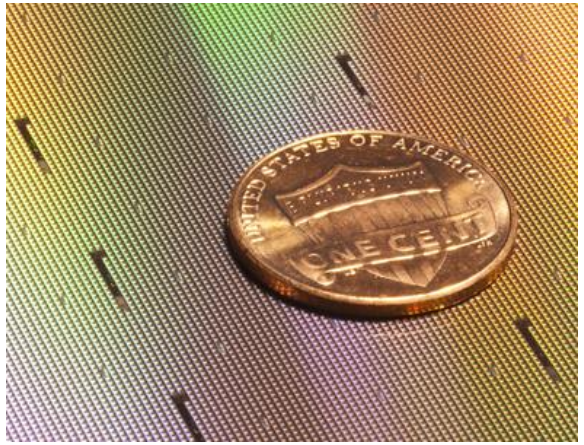
Note : This presentation outlines the personal views of the presenter

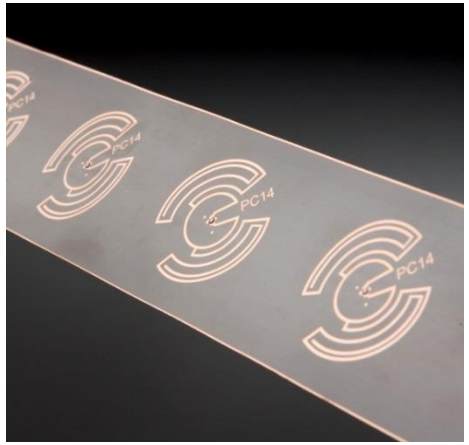
RAIN RFID

- RFID: Radio-frequency identification
  - Many different systems at different frequencies
- Ultra-high frequency (UHF): Long read range, passive tags
- The original motivation for the term “Internet of Things”
  - Kevin Ashton, AutoID Center
  - A simple way to provide connectivity to an object or device
- RAIN: RAdio-frequency IdentificatioN
  - Industry alliance with >120 members
  - www.rainrfid.org

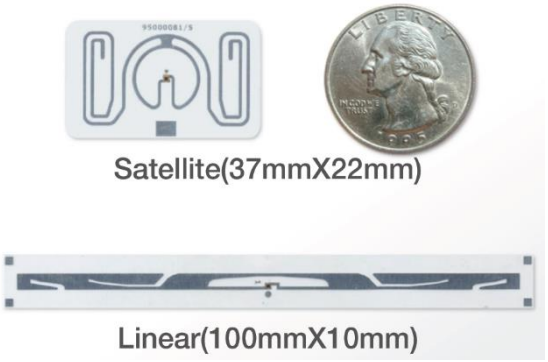


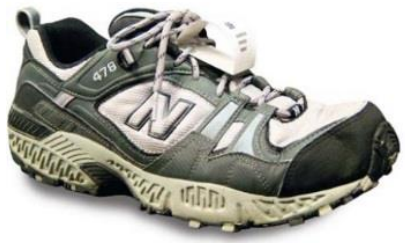
Chips and Tags (i)



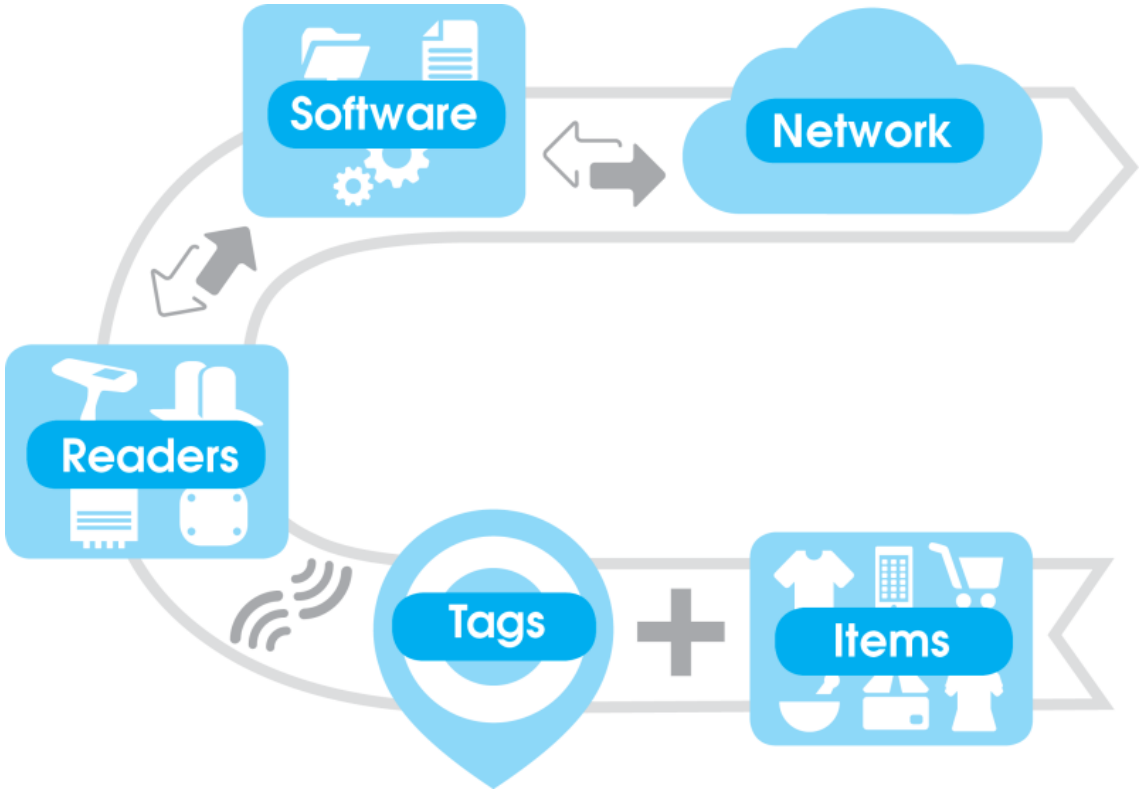


Chips and Tags (ii)





Chips and Tags … In Context



What Does a RAIN RFID Chip Currently Do?

- Chips communicate wirelessly, *i.e.* not line-of-sight

- Chips store a chip identifier (TID) and a product identifier (EPC)
  - TID is fixed by the chip manufacturer
  - Electronic Product Code (EPC) identifies the individual object; not just the product type

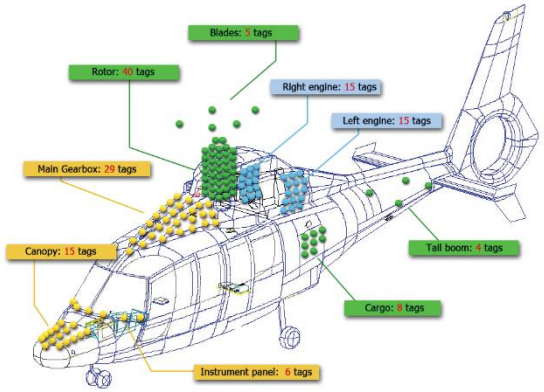
- Most RAIN RFID chips, but not all, have a small amount of user memory
  - 512 bits is a lot, often $\leq$ 64 bits
  - Some specialty chips provide $\geq$ 2k bits

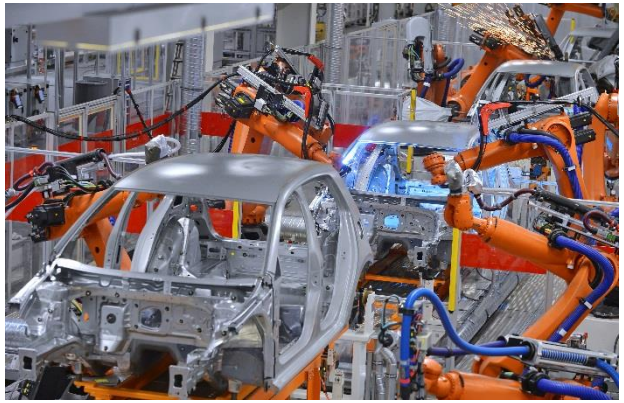
- Applications read and write product identifiers and/or small amounts of application data

Example RAIN RFID Applications

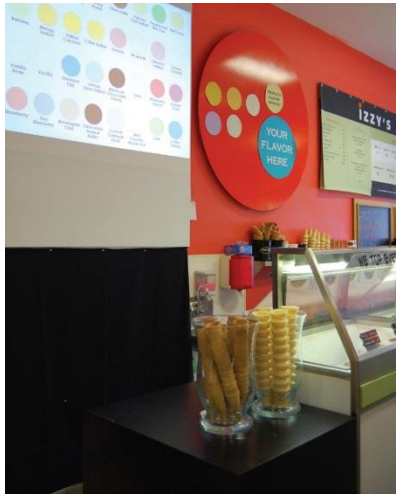
Example RAIN RFID Applications

Example RAIN RFID Applications





Example RAIN RFID Applications



What Could a RAIN RFID Chip Do?

- RAIN RFID capabilities are defined by the *over-the-air* protocol

- The revision of EPCglobal Gen2v1 to Gen2v2 brings 12 additional (optional) commands
  - Gen2v2.0.1 is available for download at *www.gs1.org/epc-rfid*

Authenticate	TagPrivilege
Challenge	FileOpen
ReadBuffer	FileList
KeyUpdate	FilePrivilege
SecureComm	FileSetup
AuthComm	
Untraceable	

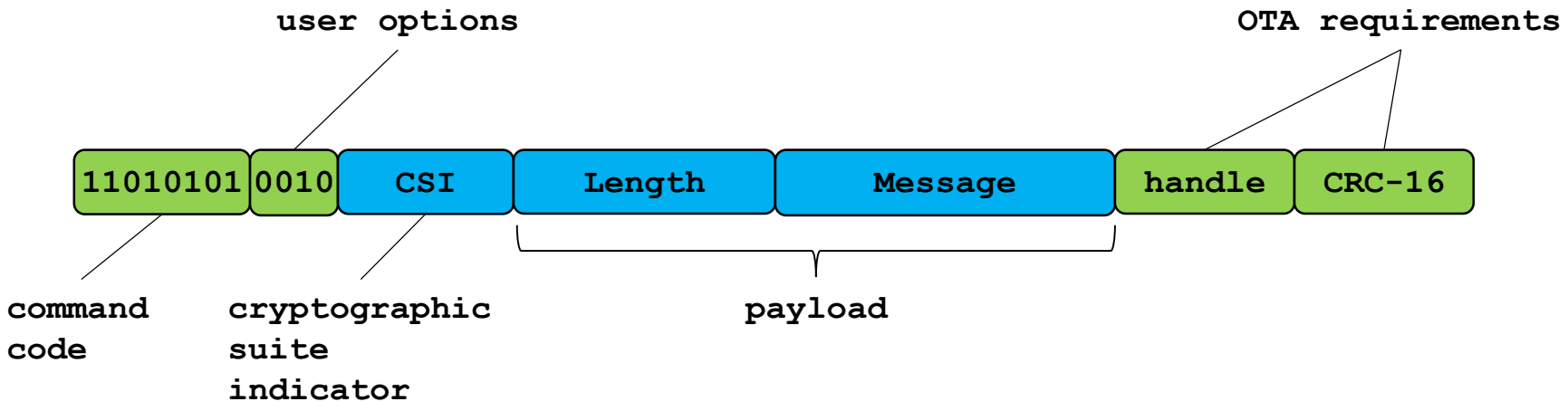
What Crypto is Included?

None

(by design)

Standards and RAIN RFID (i)

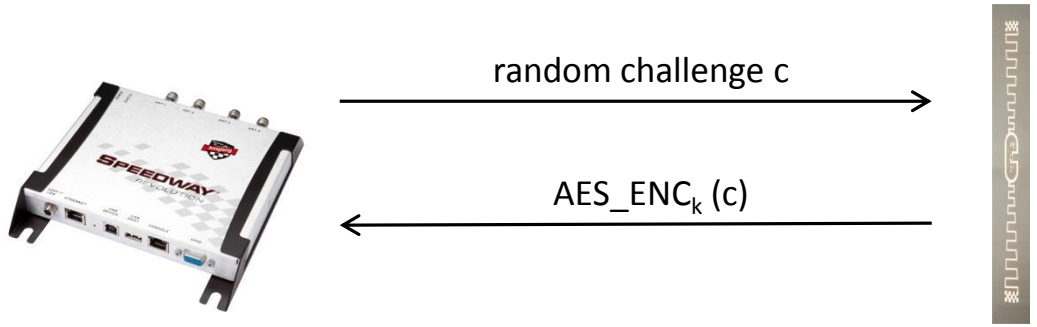
- EPCglobal Gen2v2 specifications defines the commands and response across the air interface
  - However the choice of underlying cryptography is left open
  - This provides the greatest flexibility for adoption
  - Example: the AUTHENTICATE command



Standards and RAIN RFID (ii)

- NIST and ISO/IEC JTC-1 SC27/WG2 (and others) define primitives
  - Can be extended by defined modes of operation, or higher-level constructions …

- Consider simple challenge-response using AES; but this is not enough for inter-operability …



  - What is the challenge length? Can it be variable?
  - How should the tag format the input to the encryption operation?
  - Can we support future versions or change of purpose?

Standards and RAIN RFID (iii)

- The missing link is provided by work in ISO/IEC SC31/WG4
  - *Automatic Identification and Data Capture Techniques, Radio Communications*
  - In particular the multi-part standard ISO/IEC 29167

- Each part of ISO/IEC 29167 is dedicated to a cryptographic technology
  - A cryptographic suite
  - Each cryptographic suite is assigned a CSI number
  - Each cryptographic suite defines how cryptography should be used with the air-interface commands

- ISO/IEC 29167 can be extended with new parts (new cryptographic suites)

Relationship Between Standards

Over-the-Air Interface

- CHALLENGE
- AUTHENTICATE
- SECURECOMM
- AUTHCOMM
- KEYUPDATE

e.g. AUTHENTICATE:

Command	RFU	SenRep	IncRepLen	CSI	Length	Message	RN	CRC
8	2	1	1	8	12	Variable	16	16
11010101	00	0: Store 1: Send	0: Omit length 1: Include length	CSI	Message length	Message	Handle	CRC-16

Cryptographic Suites

- 29167-10
- 29167-11
- 29167-12
- *etc.*

e.g. To use AES with AUTHENTICATE set CSI = 00_x, Length = 060_x and format Message in the following way:

AuthMethod	CustomData	TAM1_RFU	KeyID	IChallenge_TAM1
2	1	5	8	80
00_b	0_b	00000_b	[7:0]	Random Interrogator Challenge

Cryptographic Primitives

- AES (NIST)
- PRESENT (ISO/IEC 29192-2)

e.g. NIST FIPS 197 defines AES-128 as a function with $|P| = |C| = 128$ and $|K| = 128$ so that

$$C = AES_K(P)$$

ISO/IEC 29167

29167-10	AES-128	Published (revision in progress)
29167-11	PRESENT-80	Published
29167-12	ECDH	Published
29167-13	Grain-128a	Published
29167-14	AES-128	Published
29167-15	XOR	Halted
29167-16	ECDSA	Published
29167-17	CryptoGPS	Published
29167-18	Hummingbird v2	Withdrawn
29167-19	RAMON	Published
29167-20	Algebraic Eraser	Working draft
29167-21	Simon	Working draft
29167-22	Speck	Working draft

ISO/IEC 29167

29167-10	AES-128	Published (revision in progress)
29167-11	PRESENT-80	Published
29167-12	ECDH	Published
29167-13	Grain-128a	Published
29167-14	AES-128	Published
29167-15	XOR	Halted
29167-16	ECDSA	Published
29167-17	CryptoGPS	Published
29167-18	Hummingbird v2	Withdrawn
29167-19	RAMON	Published
29167-20	Algebraic Eraser	Working draft
29167-21	Simon	Working draft
29167-22	Speck	Working draft

Symmetric

RAIN RFID, Cryptography, and Performance

Starting Point

- The main advantages of RAIN RFID are that it is passive and has a long read-range
  - Adding features requires careful analysis

- Different use-cases may prioritize different performance attributes
  - *e.g.* read range, throughput, area

- Different use-cases may have different security/threat models

- The deployment eco-system is complex
  - There are different chip vendors and different reader vendors
  - Different solution providers might address very different markets

Cryptography and RAIN RFID

- There is currently one RAIN RFID chip that provides crypto: the UCODE DNA uses AES-128
- However lightweight cryptography allows us to explore a different set of trade-offs
- It can be difficult to set performance limits; however an algorithm that offers implementation flexibility has the greatest chance of satisfying a more complete range of use-cases

Cryptography and RAIN RFID

- Currently the most interest seems to be around symmetric algorithms

- There is a tendency to focus on block ciphers, but not exclusively
  - Grain-128a is of some interest

- Device authentication is likely to be an important goal in the near future
  - Tag authentication
  - Reader/Mutual authentication
  - Other demands are likely to develop

Block Cipher Parameters (i)

- It would be useful to have a discussion about key lengths
  - NISTIR 8814 states a lower-bound of 112 bits
- It is arguable whether an algorithm with a 128-bit key and “poor” side-channel profile is necessarily better than an algorithm with a 80- or 96-bit key and “good” side-channel profile
- There are significant applications where a tag will be used in only a very limited way*; e.g.* brand protection
  - A tag may be authenticated only a handful of times
  - The cryptography is used for tag authentication, not for data protection
- To extend cryptographic protection as far as possible, it would be helpful to have an option to support key lengths <112 bits in certain situations; with guidance and caveats

Block Cipher Parameters (ii)

- There is no demand for very short block lengths (*e.g.* 48 bits)

- However 64-bit block sizes can be both useful and appropriate for RAIN RFID
  - Helps in implementation and reducing over-the-air data transmissions

- For RAIN RFID it is very hard to come up with a scenario that gets anywhere close to 2^{32} uses of a 64-bit block cipher
  - In anti-counterfeiting applications a tag might be authenticated only a handful of times
  - Even encrypting and re-encrypting 8k bits of memory up to 100,000 times requires < 2^{24} iterations of a 64-bit block cipher

Cryptography and RAIN RFID

- The ability to provide a small area implementation is vital
  - This allows engineers to make appropriate implementation trade-offs
  - It gives room for engineers to explore side-channel issues and counter-measures
- The ability to provide a range of low-power implementations is vital
- Cipher latency is generally less important than area and power consumption
  - The latency targets mentioned in NISTIR 8114 seem to be quite aggressive
- In summary, flexibility gives the opportunity to find the right trade-off

Draft NISTIR 8114

- Very useful document – thank you!

- It would be worth discussing the minimum key length of 112 bits

- The idea of profiles is an interesting one
  - Might combining a primitive with a use-case be overly restrictive? How many profiles are expected?
  - When trying to write a profile, specifying the contents of the different fields was difficult

- Likely more discussion during the workshop

Conclusions

- The NIST initiative on lightweight cryptography is very welcome and timely
- There will be considerable interest from industry in the development of a portfolio
- It will significantly help extend cryptography and security to many more devices and applications
- We have a great pool of research on lightweight cryptography … let’s put it to use!

- Thank you for your attention!