Industrial Tutorial 2 - Threat Analysis Paradigms in Wireless Technology

Canada-France MITACS Workshop on Foundations and Practice of Security

Michel Barbeau, Joaquín García-Alfaro and Christine Laurendeau

Carleton University

Outline

- Threat analysis paradigms (C)
- Threats to confidentiality (M)
  - The WiFi/802.11 case
  - The WiMAX/802.16 case
- Threats from insiders (C)
  - The vehicular communications case
- Threats to EPC/RFID (J)

Threat Analysis Paradigms

- Rationale
- Methodologies
- Risk Factors

Why Analyze Threats?

- Countermeasures
  - We want to make sure we don't get attacked
- Efficiency
  - Why waste time researching minor threats? Why bother fixing something nobody cares about?
- Solution: Focus on critical and major threats
  - Identify the threats
  - Classify them by order of importance
  - Determine which ones require countermeasures

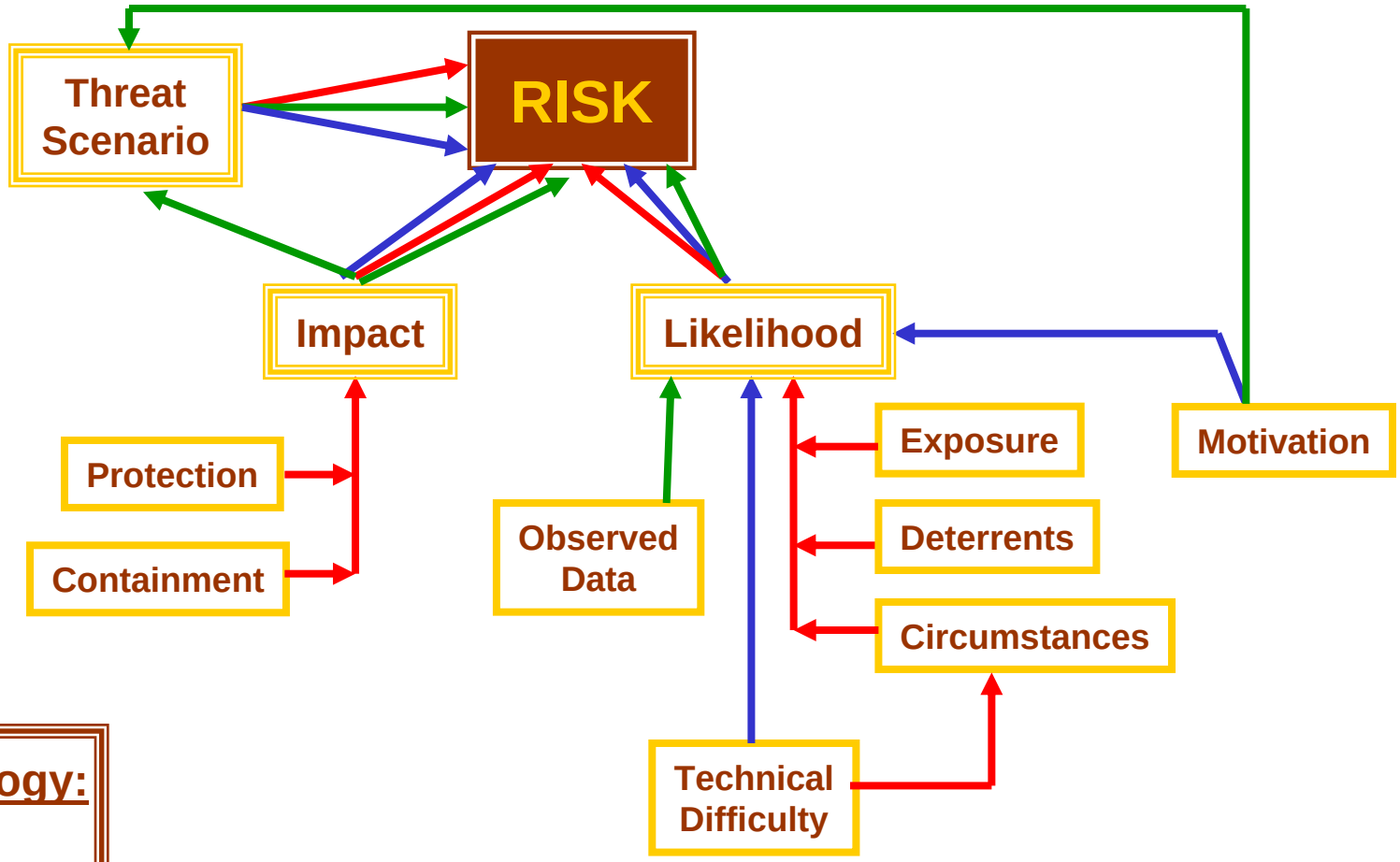
Types of Threat Analysis Methodologies

- Quantitative Methodologies
  - Use statistics, probabilistic model, historic data
  - Example Risk: Probability [0..1] of accident
  - Example Methodologies: PRA, QRAS
- Problem: Need historic data
- Qualitative Methodologies
  - Use discrete values for risk factors
  - Example Risk: Likely, Possible, Unlikely
  - Example Methodologies: ETSI, NIST, Octave, Mehari
- Problem: Values for risk factors are subjective

Qualitative Methodologies

- NIST: G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, July 2002.
- Octave: C. J. Alberts and A. J. Dorofee, *OCTAVE Criteria, Version 2.0. Technical Report CMU/SEI-2001-TR-016*, CERT, December 2001.
- Mehari: CLUSIF Methods Commission, *MEHARI 2007 Concepts and Mechanisms*, Club de la securité de l'Information français, April 2007.
- ETSI: ETSI, *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis*, Technical Specification TS 102 165-1 V4.1.1, European Telecommunications Standards Institute, 2003.

Threat Analysis Risk Factors



Methodology:

Octave
Mehari
ETSI, NIST

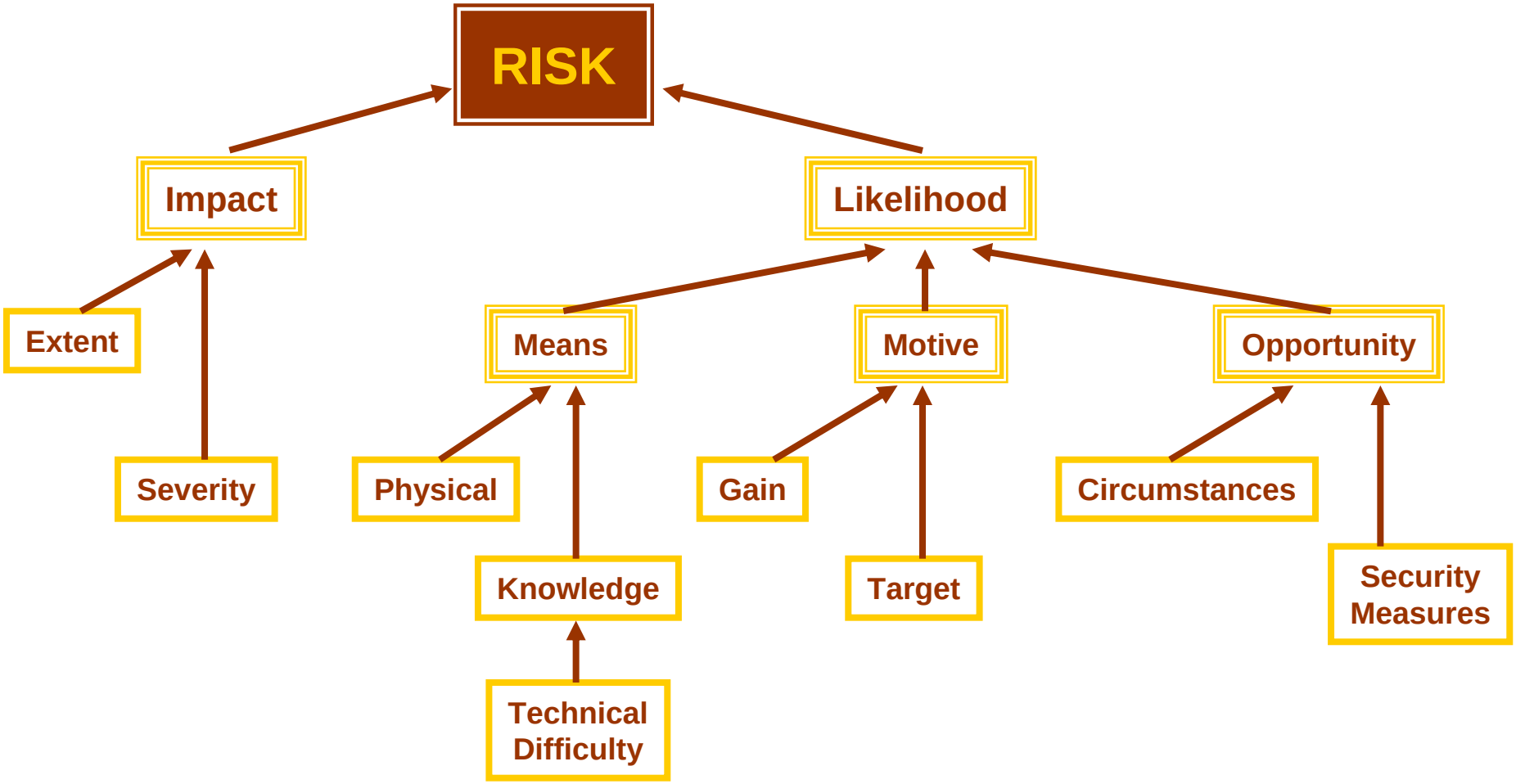
Methodology Comparisons

- ETSI, NIST
  - Use qualitative, static risk factors
- Octave
  - Threat scenario generation
  - Likelihood based on observed data
- Mehari
  - Includes knowledge base of security services
  - Dynamically adjusts risk assessment based on implemented countermeasures

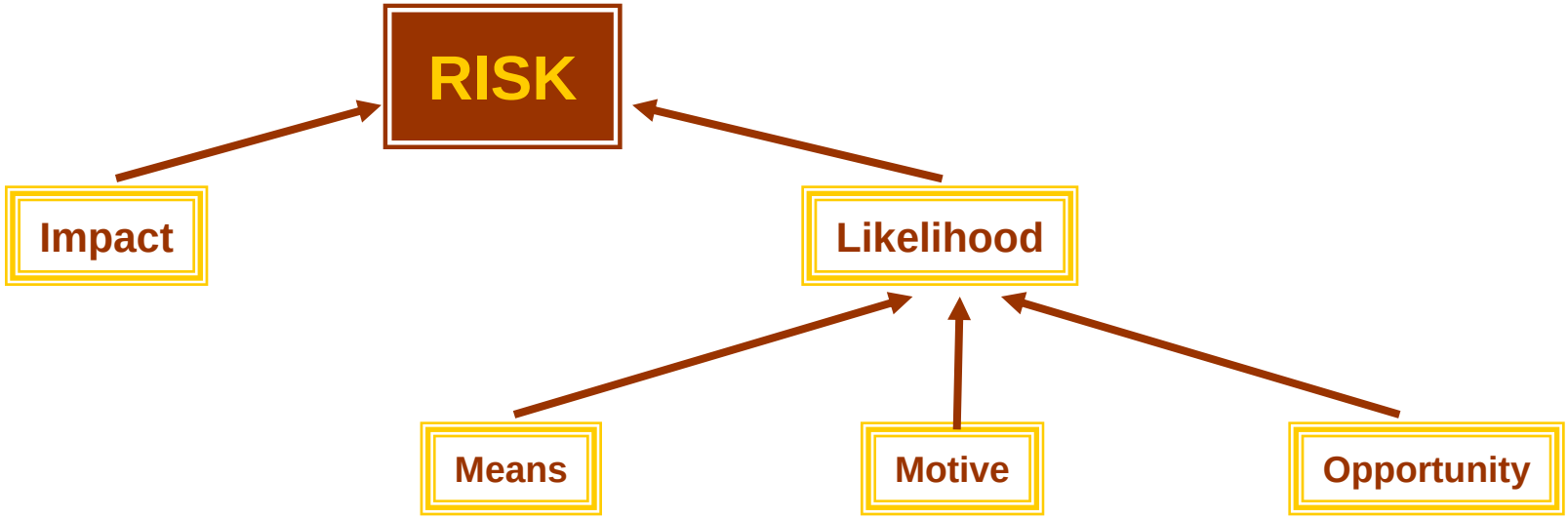
ETSI Methodology Analyses

- Three threat analyses using ETSI:
  - J. Garcia-Alfaro, M. Barbeau and E. Kranakis, *Analysis of Threats to the Security of EPC Networks,* 6th Annual Communication Networks and Services Research (CNSR) Conference, Halifax, Nova Scotia, Canada, May 2008.
  - C. Laurendeau and M. Barbeau, *Threats to Security in DSRC/WAVE*, 5th International Conference on Ad-hoc Networks, 2006.
  - M. Barbeau, *WiMax/802.16 Threat Analysis*, 1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet), 2005.
- Observations:
  - Not all risk factors have equal weight; technical difficulty is the most influential factor
  - Static risk factors preclude automation

Risk Factor Ontology



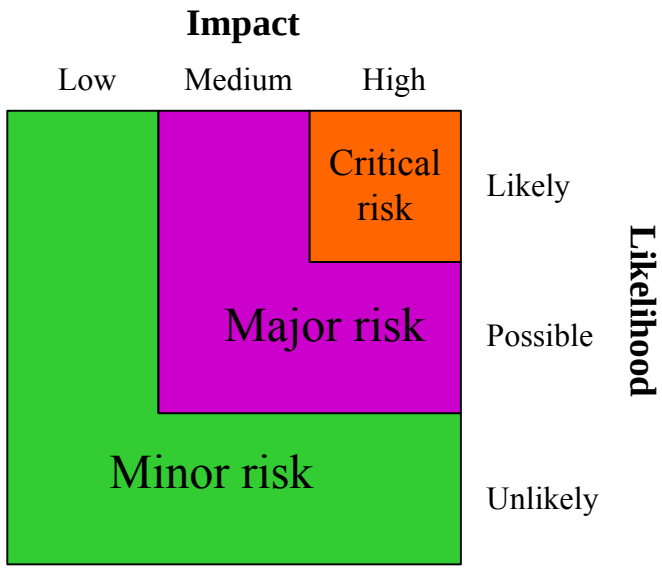
Risk Factor Priority

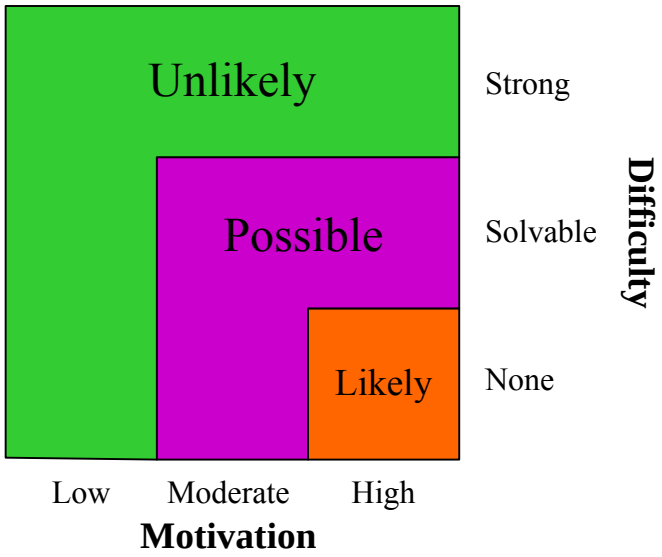


- Countermeasures aim to reduce impact and opportunity

ETSI Risk Assessment

- Overall Risk Assessment:
  - Critical, Major, Minor
- Risk Factors:
  - Likelihood of threat occurrence
  - Impact on user or system





- Likelihood Assessment Factors:
  - Motivation of attacker
  - Technical difficulty

Threats to Confidentiality

- The WiFi/802.11 case
- The WiMAX/802.16 case

What is Confidentiality?

- The contents of a message can be understood only by its source and destination

Why is it Challenging?

- Interception easiness
- Need to maintain backward compatibility
- Easiness to work around regulations

Cryptographic Techniques

- Symmetric key-based
  - Same key is used for both encryption and decryption
- Asymmetric key-based
  - A key for encryption, another key for decryption

Symmetric Key-based Cryptography

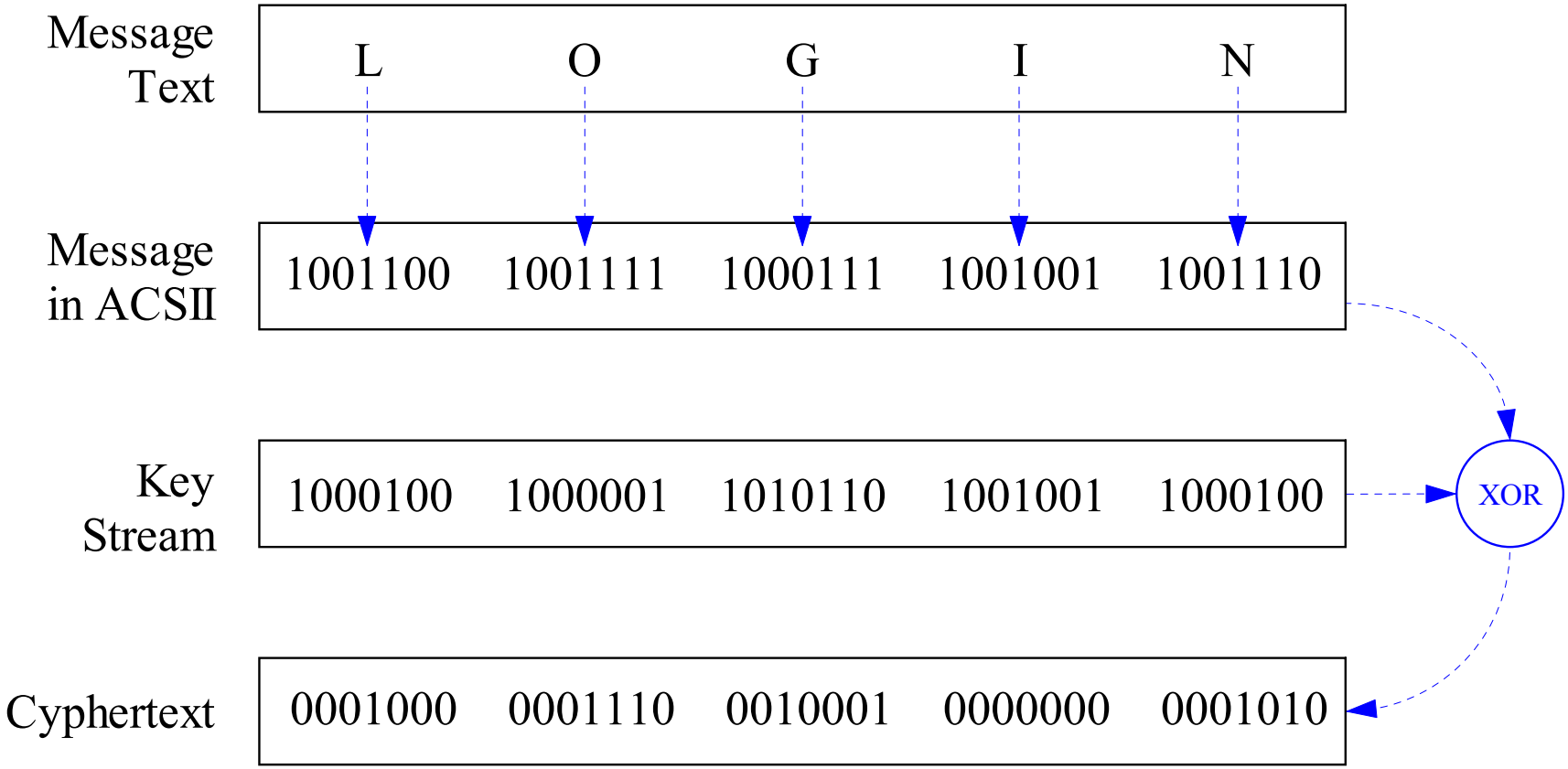
The XOR Operation

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

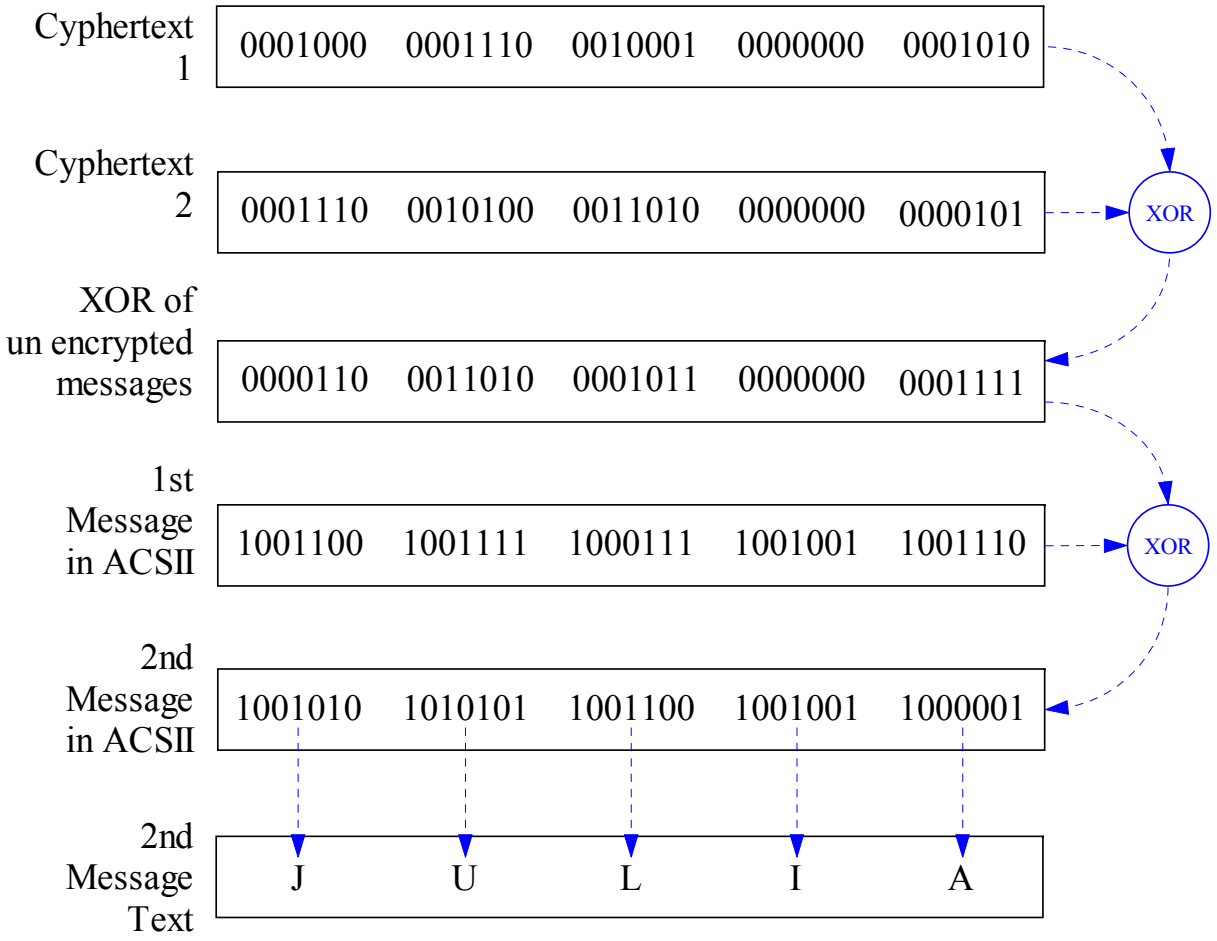
WiFi/802.11 Confidentiality

- Wired Equivalent Privacy (WEP), RC4
- *Not so secret key!*
  - Shared between all the network members: clients, access points
- *Key reuse for different messages!*
  - If one message is known, then the others can be decrypted

RC4 Encryption



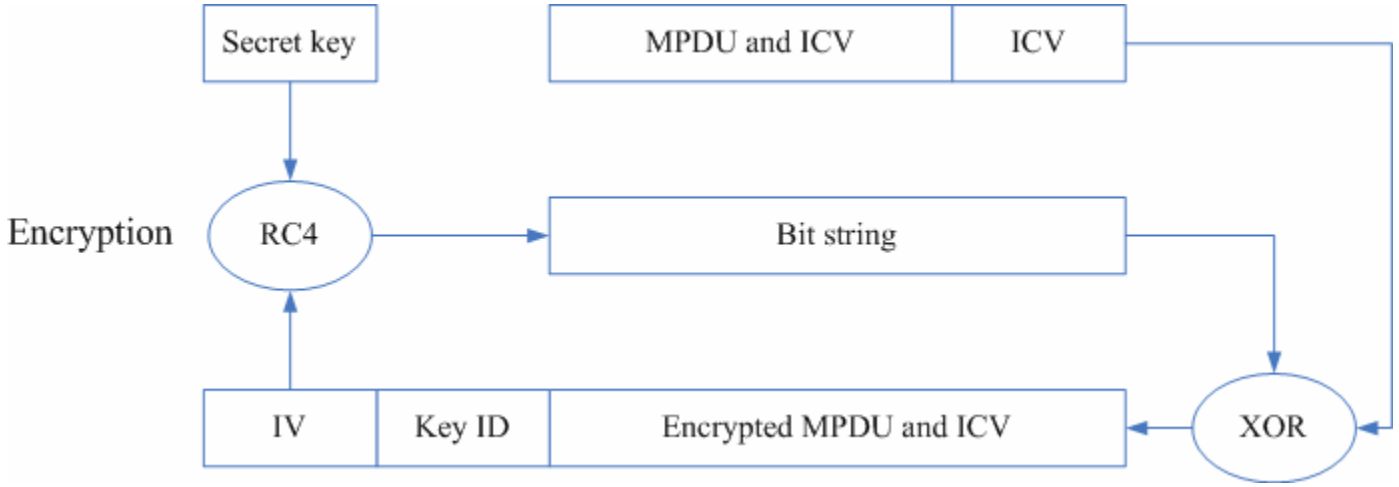
Cracking RC4 Messages



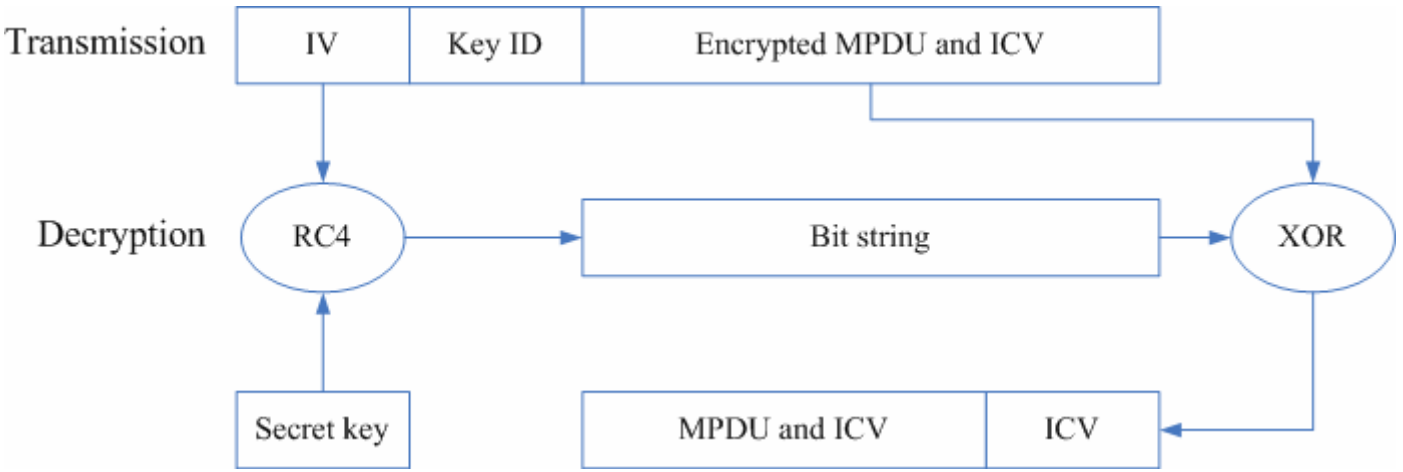
Confidentiality

- Uses Wired Equivalent Privacy (WEP) with secret key
- Data is encrypted using IV and Default key or Key-mapping key
- Initialization Vector (IV): 24-bit random val. chosen by transmitter
- Default key: 40- or 104-bit key shared between AP and several stations
- Key-mapping key: 40- or 104-bit key shared between AP and one station
- Encryption: RC4
- Integrity (are frames intact?): CRC-32 Integrity Check Value (ICV)
- An exhaustive search can find the secret key in few hours
- Can be cracked by cryptanalysis [Fluhrer et al. 2001]: e.g. AirSnort

WEP Encryption



WEP Decryption



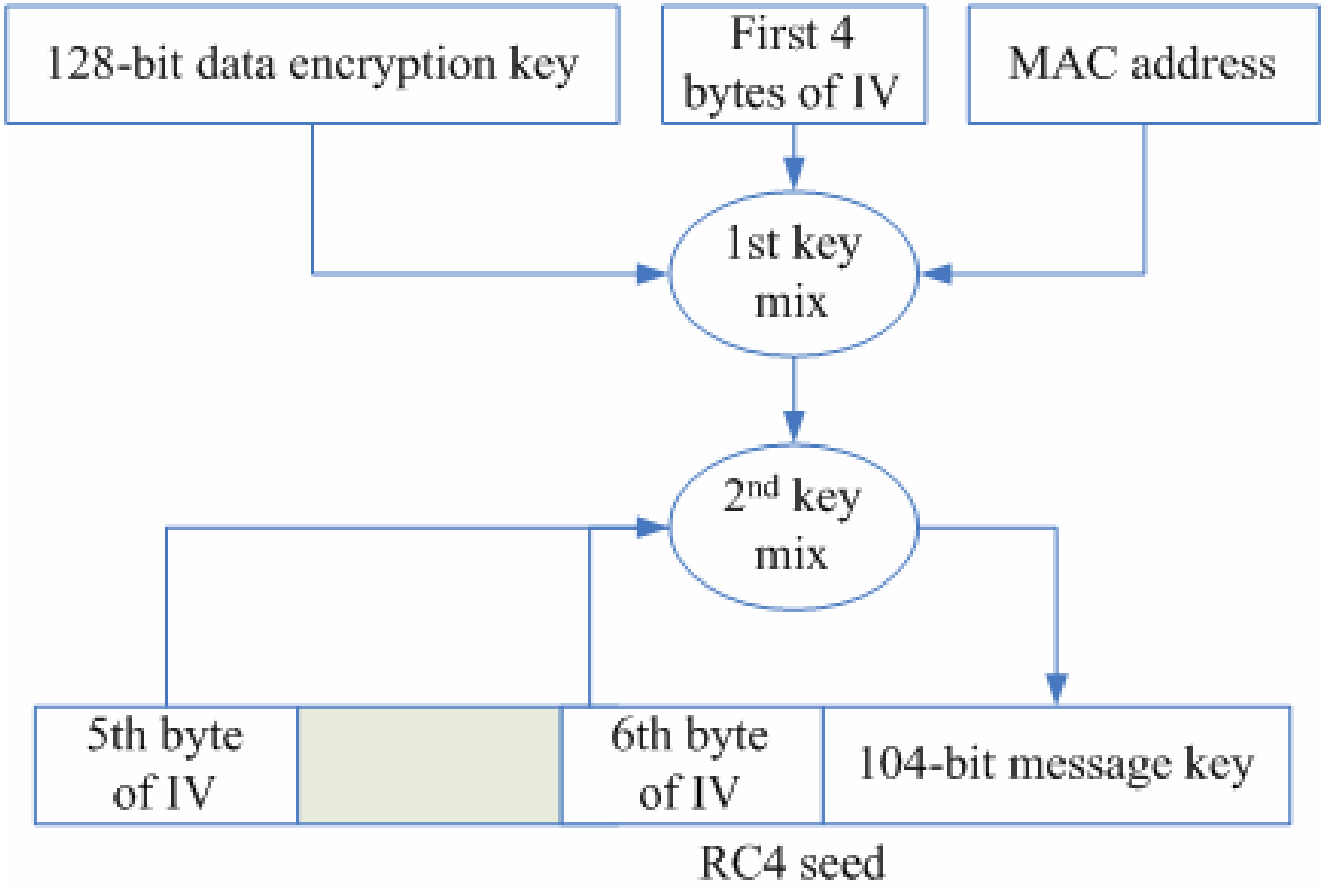
Recent WiFi Development

- Encryption key establishment uses asymmetric key-based techniques
- WiFi Protected Access (WPA)
  - Temporal Key Integrity Protocol (TKIP): RC4 with longer non reused keys
- 802.11i
  - Advanced Encryption Standard (AES)

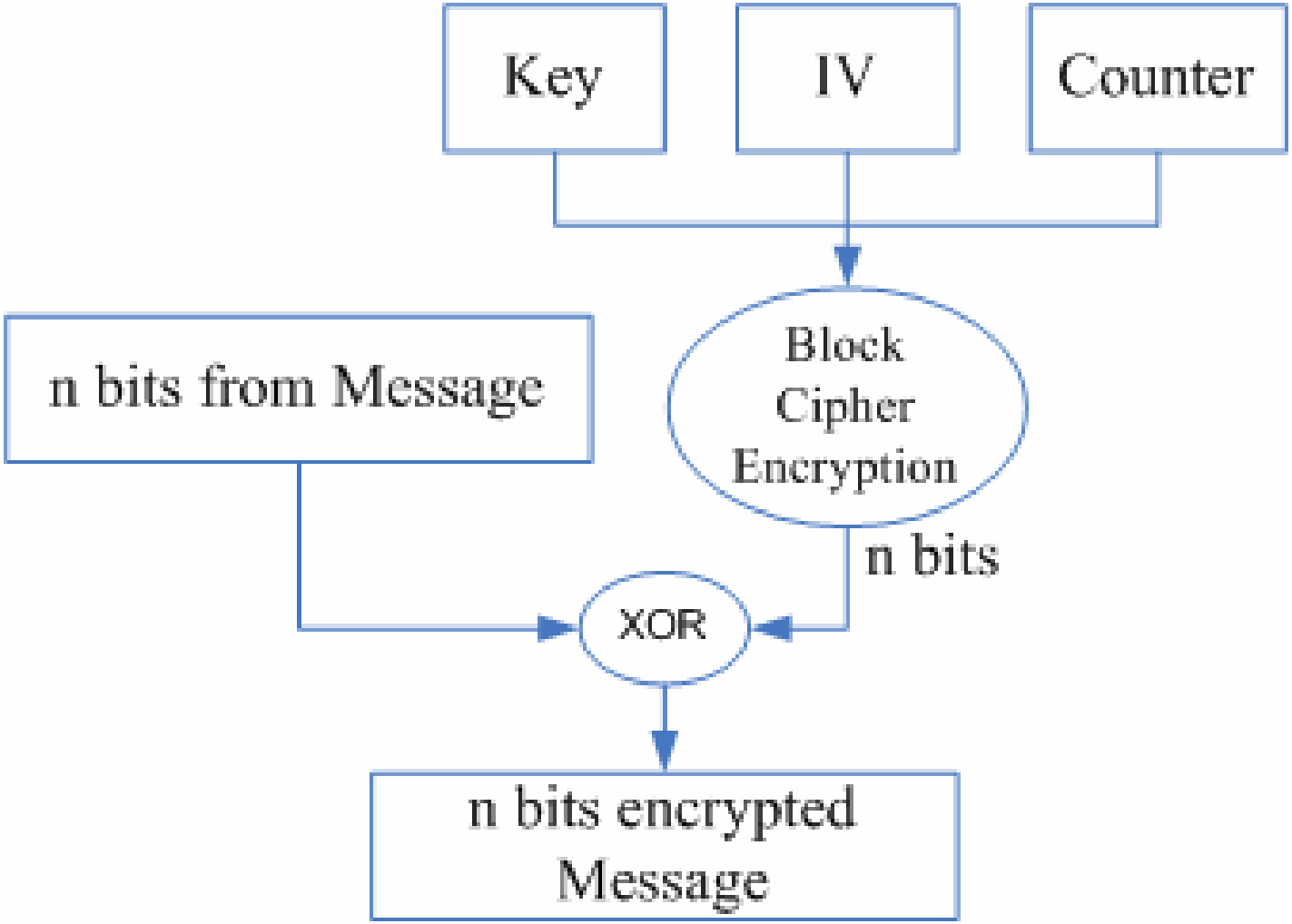
IEEE 802.11i

Protocol	Authentication and access control	Confidentiality and Integrity
WiFi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP)	802.1X-based	Per-packet RC4 encryption key Message Integrity Code (64-bit hash) Replay protection (48-bit sequence num.)
WiFi Protected Access 2 (WPA2)/Robust Security Network (RSN)/Counter-Mode-CBC-MAC Protocol (CCMP)	802.1X-based	AES 128-bit encryption Message Authentication Code(64-bit hash) Replay protection (48-bit sequence num.)

TKIP



Counter Mode

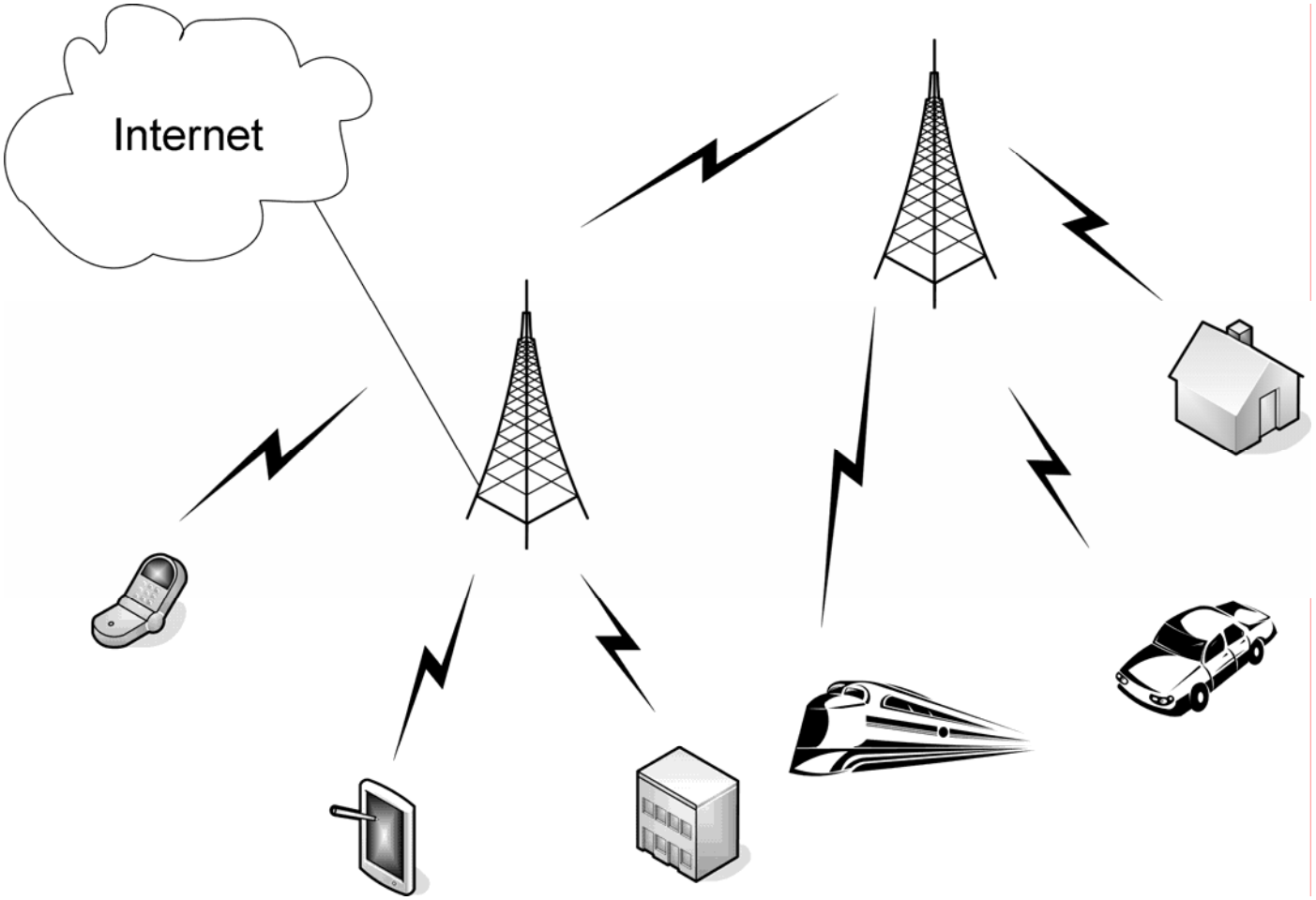


WiFi/802.11 Threat Analysis

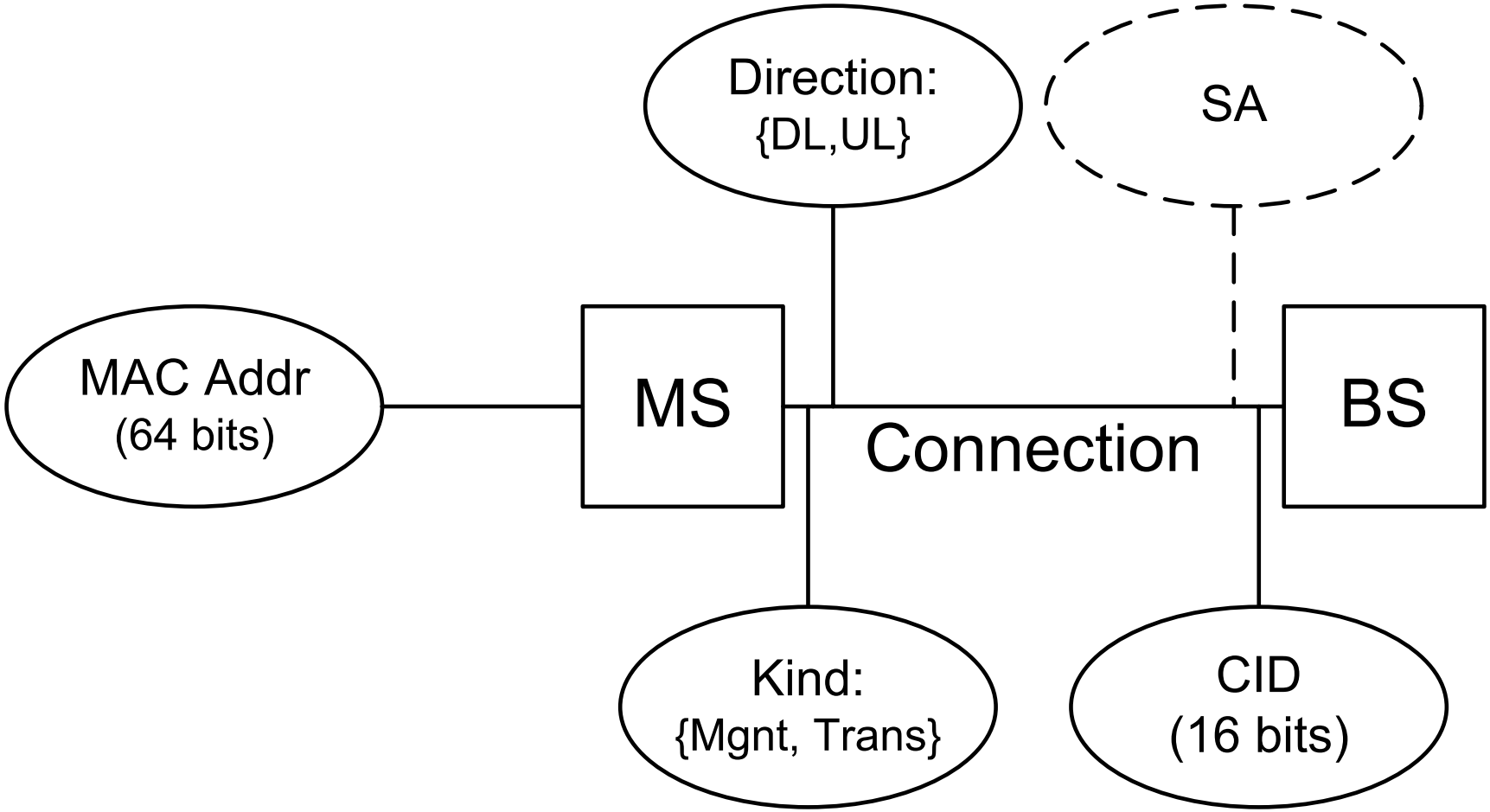
Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping Data Traffic Msgs	WEP (before 2001)	Unlikely	High	Minor
	WEP (before 2002)	Possible	High	Major
	WEP (2002-)	Likely	High	Critical
	WPA 802.11i	Unlikely	High	Minor
Eavesdropping Management Msgs	None	Likely	Medium	Major

Threats to Confidentiality
The WiMAX/802.16 Case

A WiMAX/802.16 PMP Network



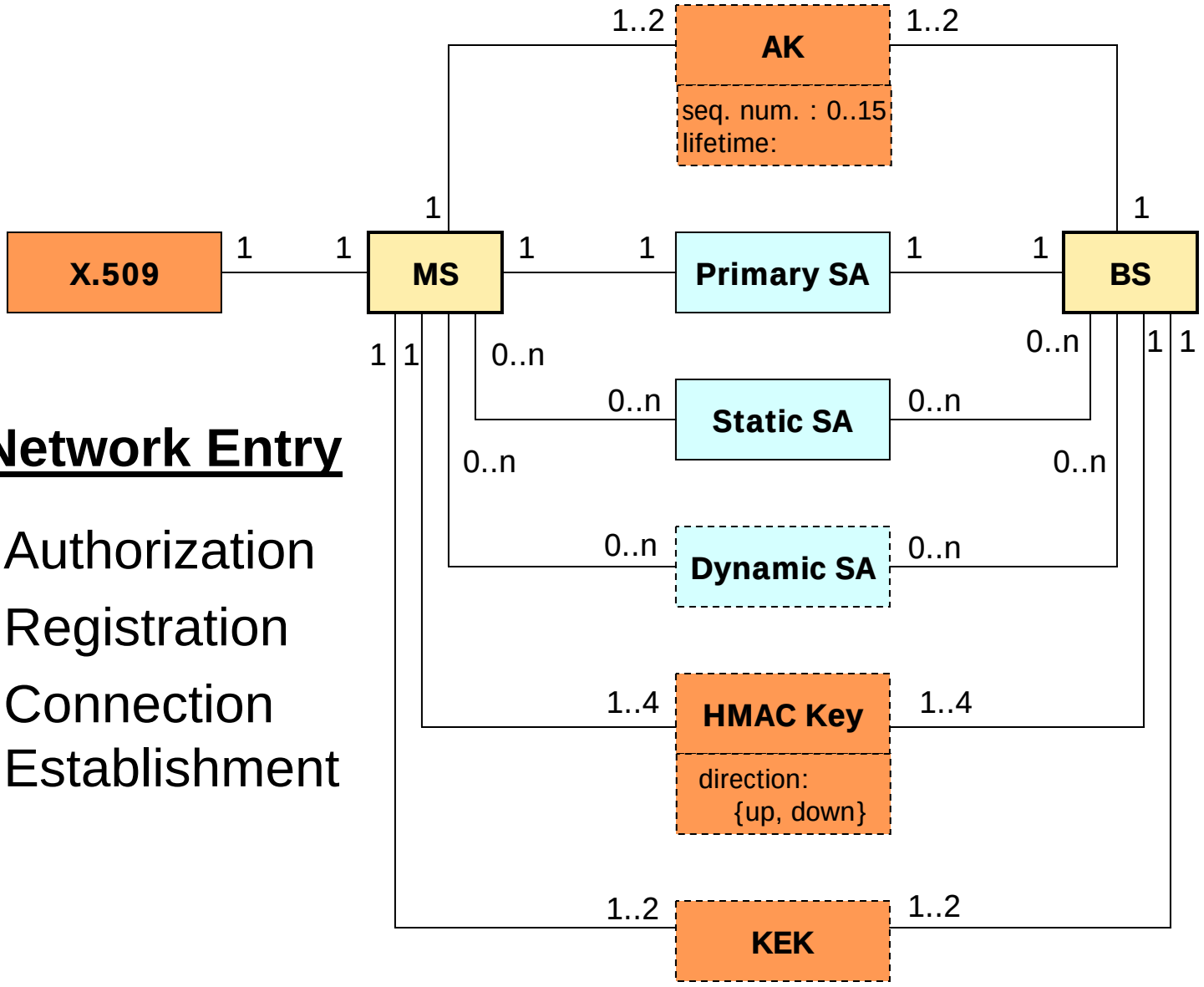
MAC Layer Concepts



Management Connections

<table>
<tr><th>Type</th><th>Usage</th><th>When</th><th>SA</th></tr>
<tr><td>DL Basic</td><td rowspan="2">Short & urgent mgnt msgs</td><td rowspan="4">MS init time</td><td rowspan="4">None</td></tr>
<tr><td>UL Basic</td></tr>
<tr><td>DL Primary</td><td rowspan="2">Delay tolerant mgnt msgs</td></tr>
<tr><td>UL Primary</td></tr>
<tr><td>DL Secondary</td><td rowspan="2">IP encap mgnt msgs (e.g. DHCP, SNMP, TFP)</td><td rowspan="2">MS init time (optional)</td><td rowspan="2">Primary</td></tr>
<tr><td>UL Secondary</td></tr>
</table>

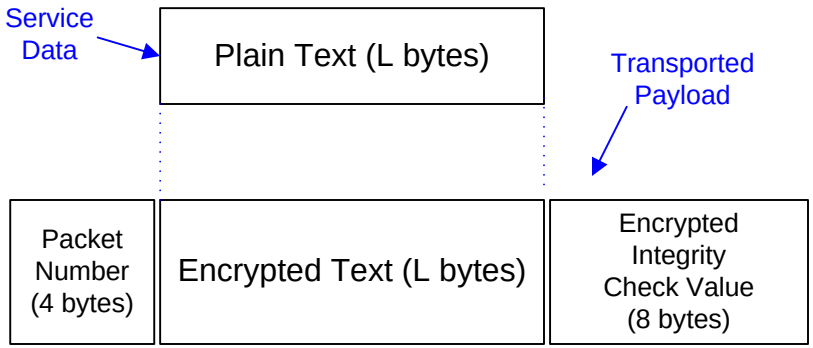
WiMAX/802.16 Security Model



Network Entry

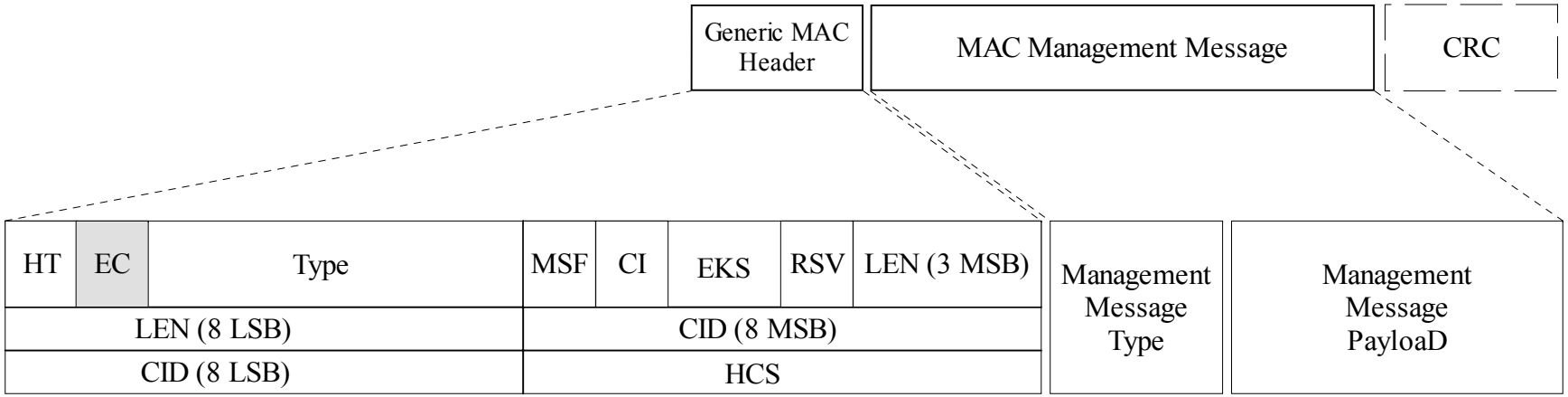
- Authorization
- Registration
- Connection Establishment

Encryption

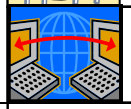


IEEE 802.16d/e standard (Section 7.1.1) states:

- generic MAC header is not encrypted
- all MAC management messages shall be sent in the clear
  this for facilitating registration, ranging and normal operation of the MAC.



WiMAX/802.16 Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping Management Msgs	None	Likely	 Medium	 Major
			 High	 Critical
Eavesdropping Data Traffic Msgs	DES-CBC, AES-CCM	Unlikely	High	Minor

Insider Threats to Vehicular Communications

- Malicious Insiders
- Vehicular Communications Security
- Insider Threat Analysis

Malicious Insiders

- Wireless networks use an open medium
- Security measures are necessary

- Problem:
  - Most measures secure against outsider threats
  - Few secure against malicious insiders

Telegraph.co.uk

Schoolboy hacks into city's tram system

By Graeme Baker
Last Updated: 2:27AM GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.

The teenager, who was not named by police, told them he had changed the points for a prank.

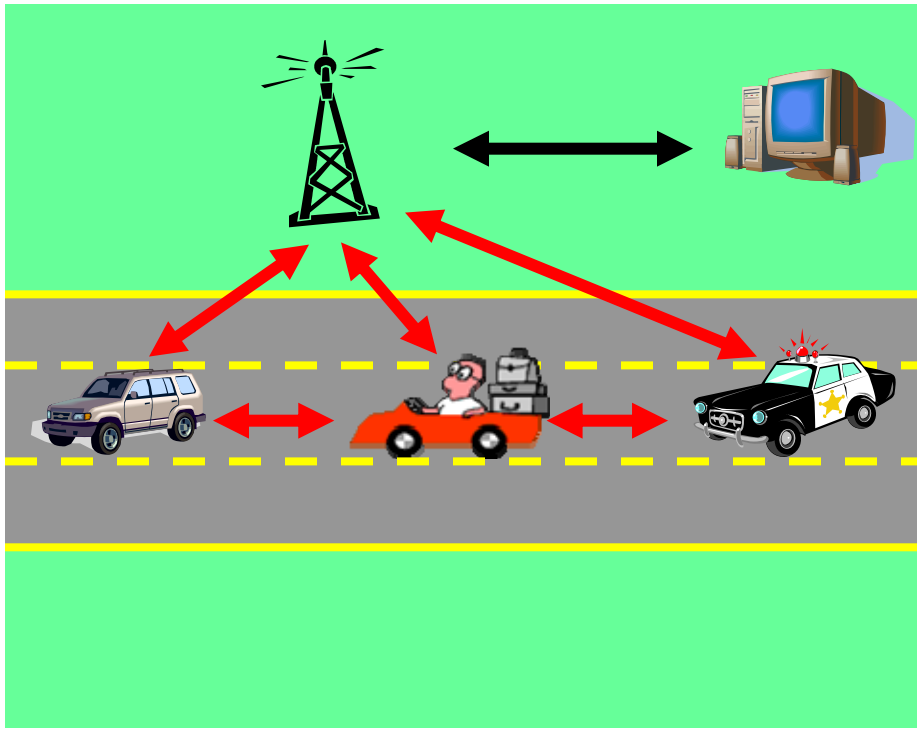
The boy, described as a 'genius'and some of the equipment he used

Example of Insider Attack

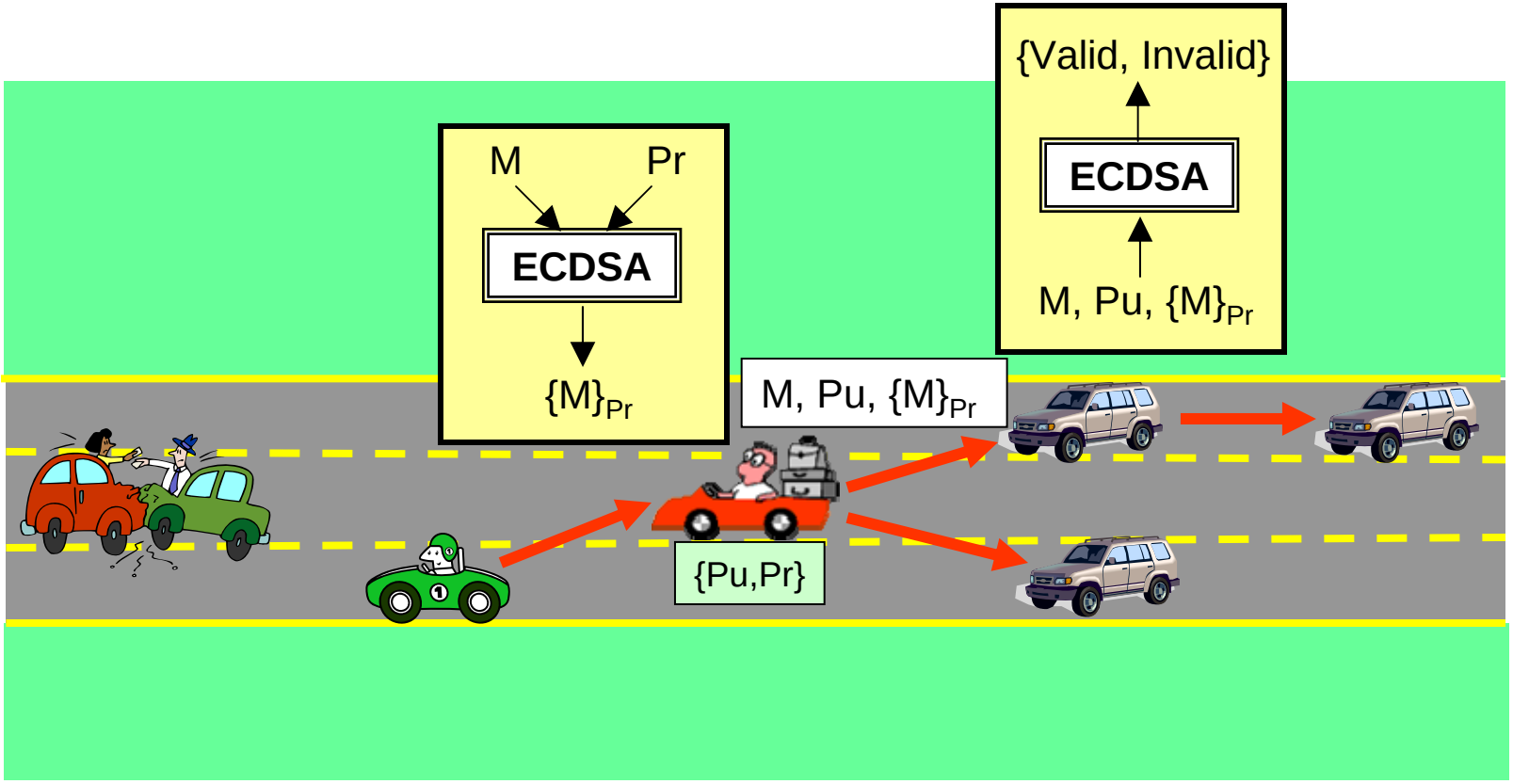
- Sequence from “Live Free or Die Hard,” Stage One

Vehicular Communications Security

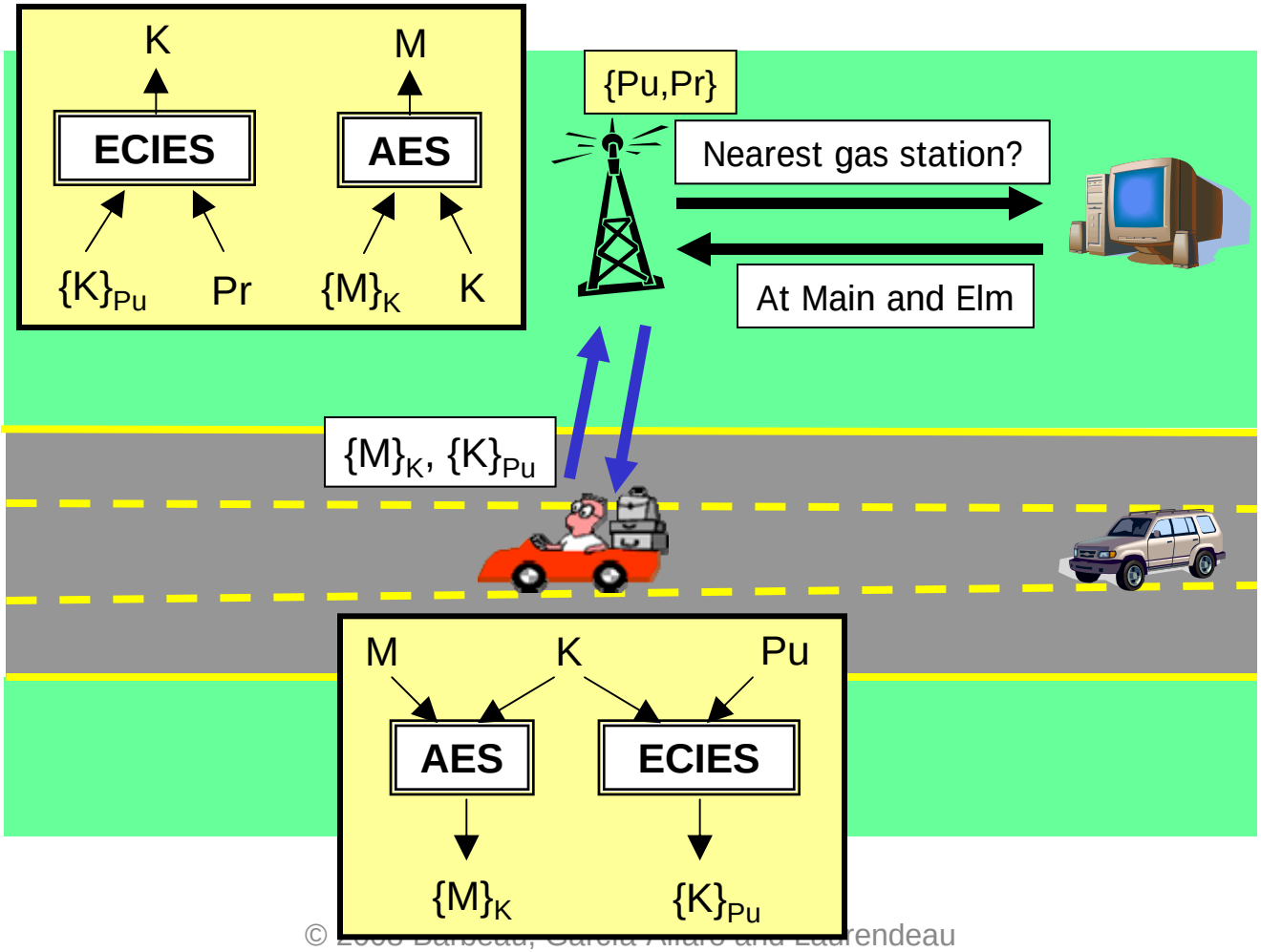
- **Broadcast Applications**
  - E.g. traffic updates, hazards, collision warnings
  - Digital signatures
- **Transaction Applications**
  - E.g. navigation, location-based services, toll payment
  - Encryption



Example of Broadcast Application



Example of Transaction Application

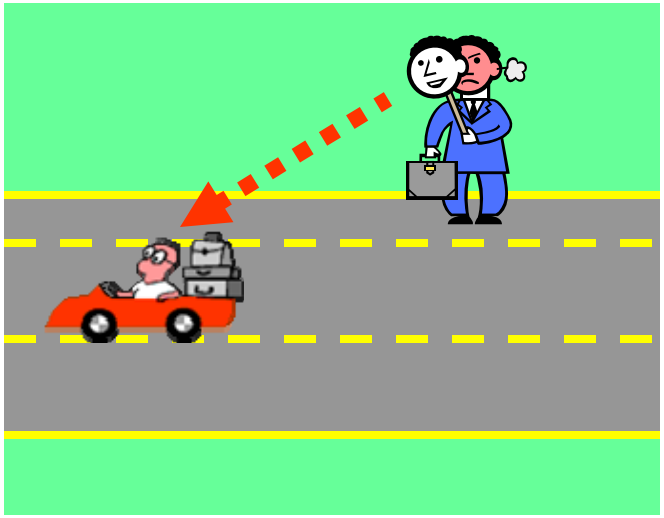


Insider Threat Analysis

- Threats to broadcast and transaction messages
  - Masquerading
  - Eavesdropping
  - Tampering
- Motivation = High
  - Nothing is secret anymore
- Technical Difficulty = None
  - Insider access to secret keys
- Likely threats

Masquerading

- Motivation
  - Evading retribution
- Technical Difficulty
  - Victim's private key used to sign messages
  - Credentials untraceable to malicious insider
- Impact
  - Wide scope due to lack of accountability

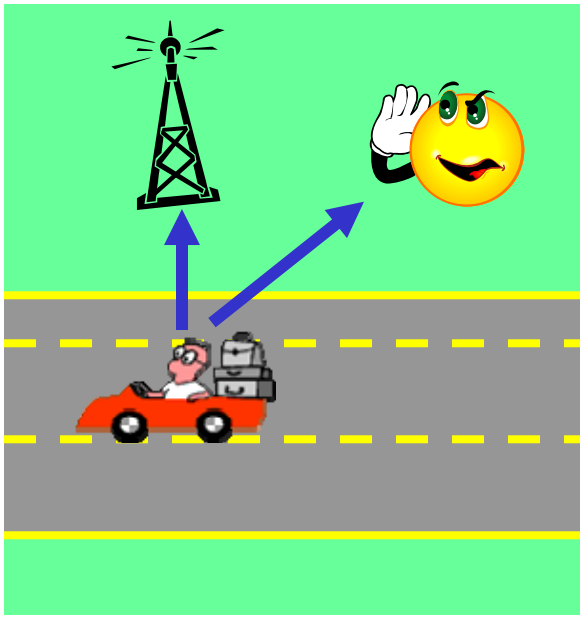


Masquerading Analysis

Threat	Messages	Likelihood	Impact	Risk
Masquerading	All	Likely	High	Critical

Eavesdropping
Transaction Messages

- Motivation
  - Access to victim's personal and financial information
- Technical Difficulty
  - Victim's private key used to decrypt messages
- Impact
  - Scope limited to victim



Eavesdropping Analysis

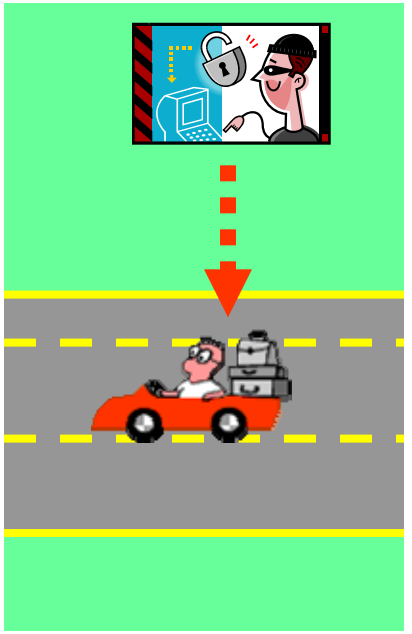
Threat	Messages	Likelihood	Impact	Risk
Eavesdropping	Broadcast	Unlikely	Low	Minor
	Transaction	Likely	Medium	Major

Example of Tampering
Broadcast Messages

- Sequence from “Live Free or Die Hard,” Tunnel

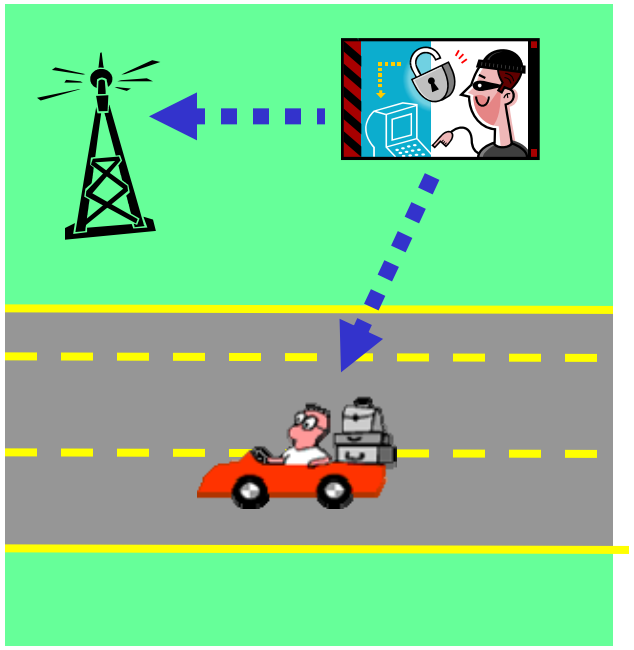
Tampering
Broadcast Messages

- Motivation
  - Manipulate vehicular traffic
- Technical Difficulty
  - Valid key pair used to sign messages
- Impact
  - All vehicles within radio range are vulnerable



Tampering
Transaction Messages

- Motivation
  - Manipulate information to/from victim
- Technical Difficulty
  - Victim's private key used to sign messages
- Impact
  - Scope limited to victim



Tampering Analysis

Threat	Messages	Likelihood	Impact	Risk
Tampering	Broadcast	Likely	High	Critical
	Transaction	Likely	Medium	Major

Threats to EPC/RFID

- Background
- Threats
- Countermeasures

Electronic Product Code (EPC)

- Evolution of optical barcodes
- Based on RFID technologies
- Still an evolving standard
  - Started in 1999 at MIT's Auto-ID Labs
    - academic research project
    - supported by industrial partners
  - Since 2003, transferred to EPCglobal Inc.

EPCglobal

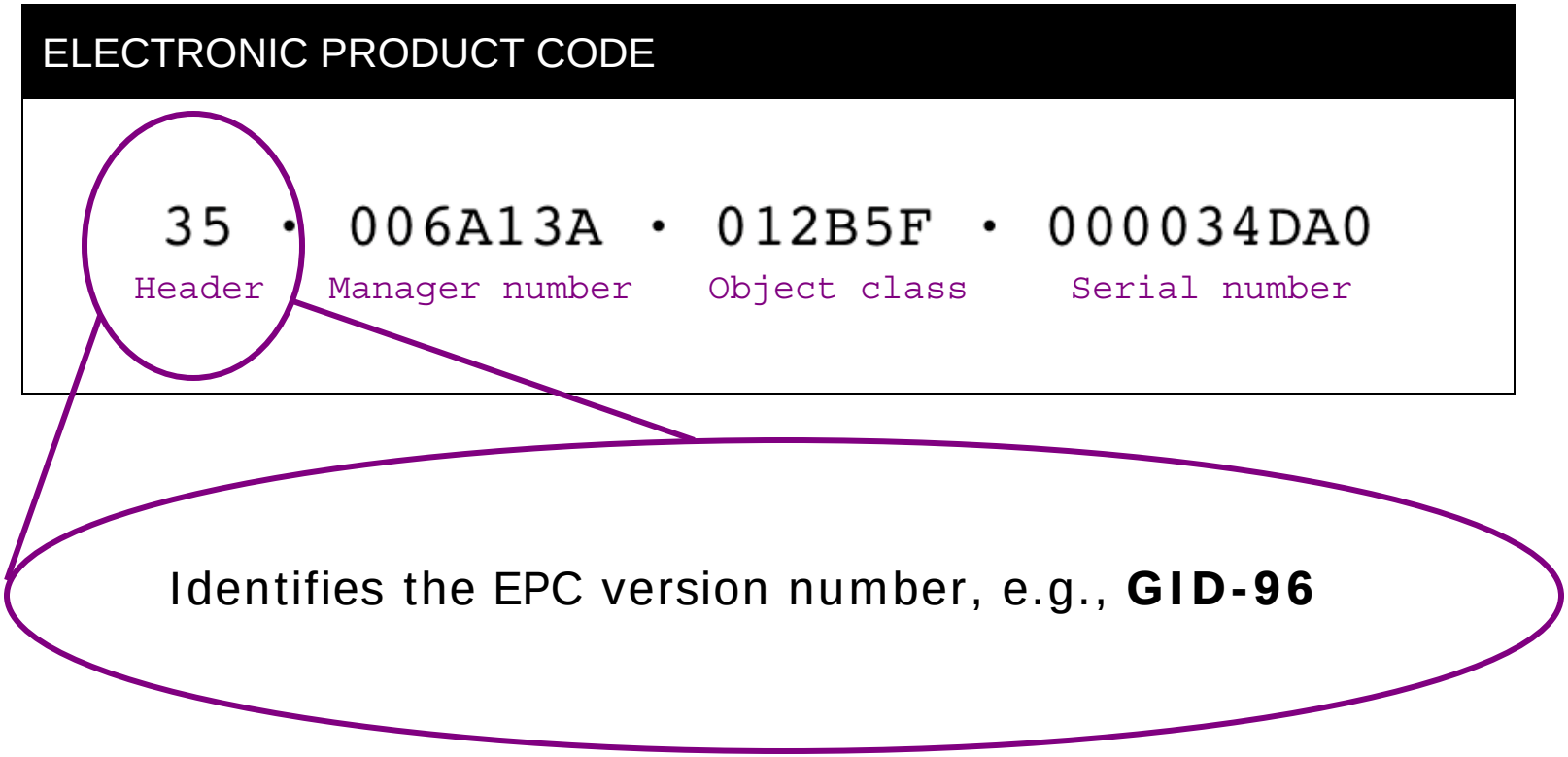
- Joint project of the organizations that regulate:
  - The Universal Product Code (UPC)
  - The European Article Number (EAN)
  - The Japanese Article Number (JAN)

- Main goal of EPCglobal
  - World-wide adoption and standardization of EPC technology

- Other issues of concern for EPCglobal:
    - Intellectual property
    - Frequency bands in the different world regions
    - Hardware/application standards
    - …

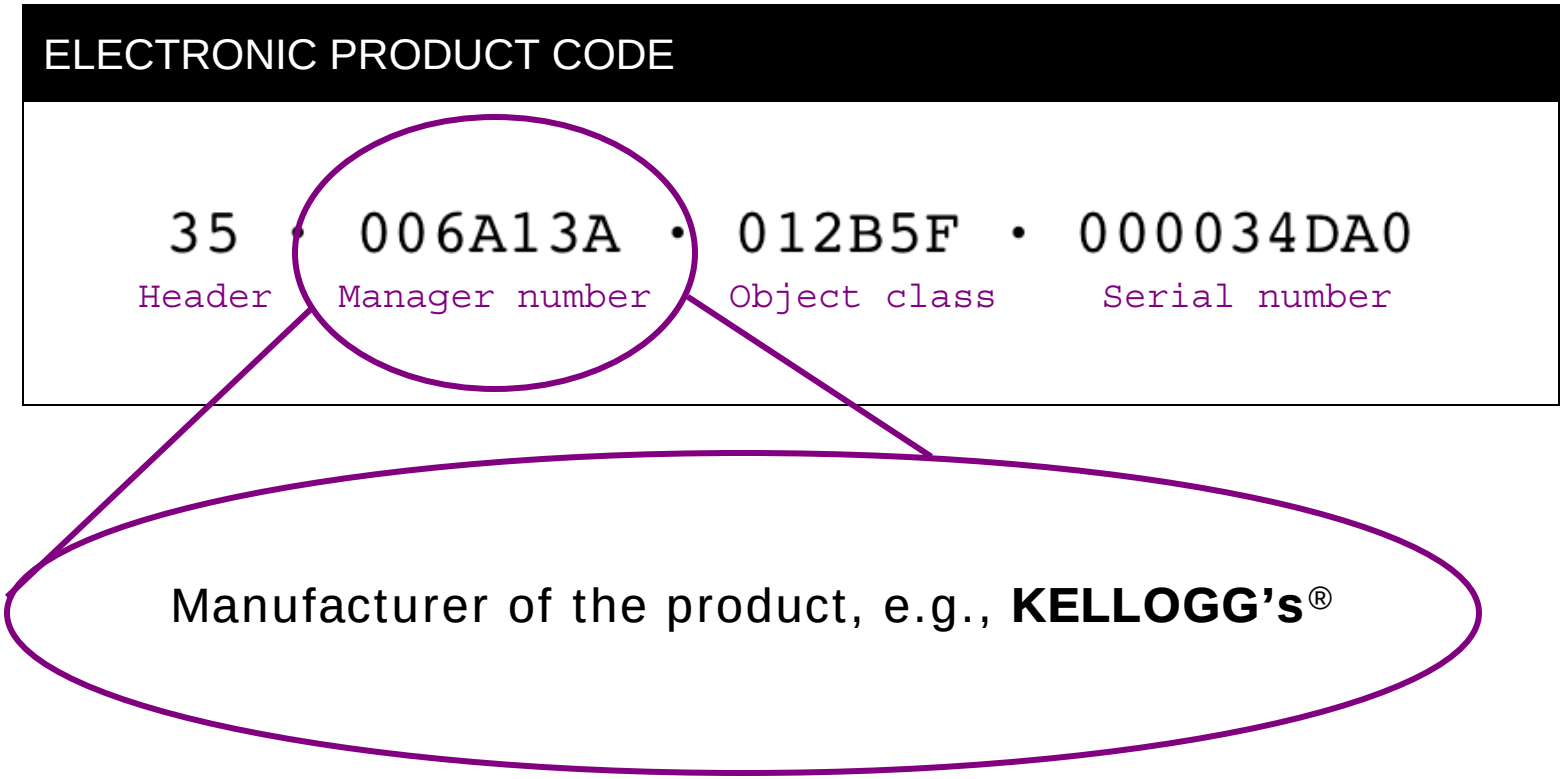
Structure of the EPC

- It support codes widely-used today or self defined conventions
- E.g., representation of an EPC general identifier (GID) of 96 bits:



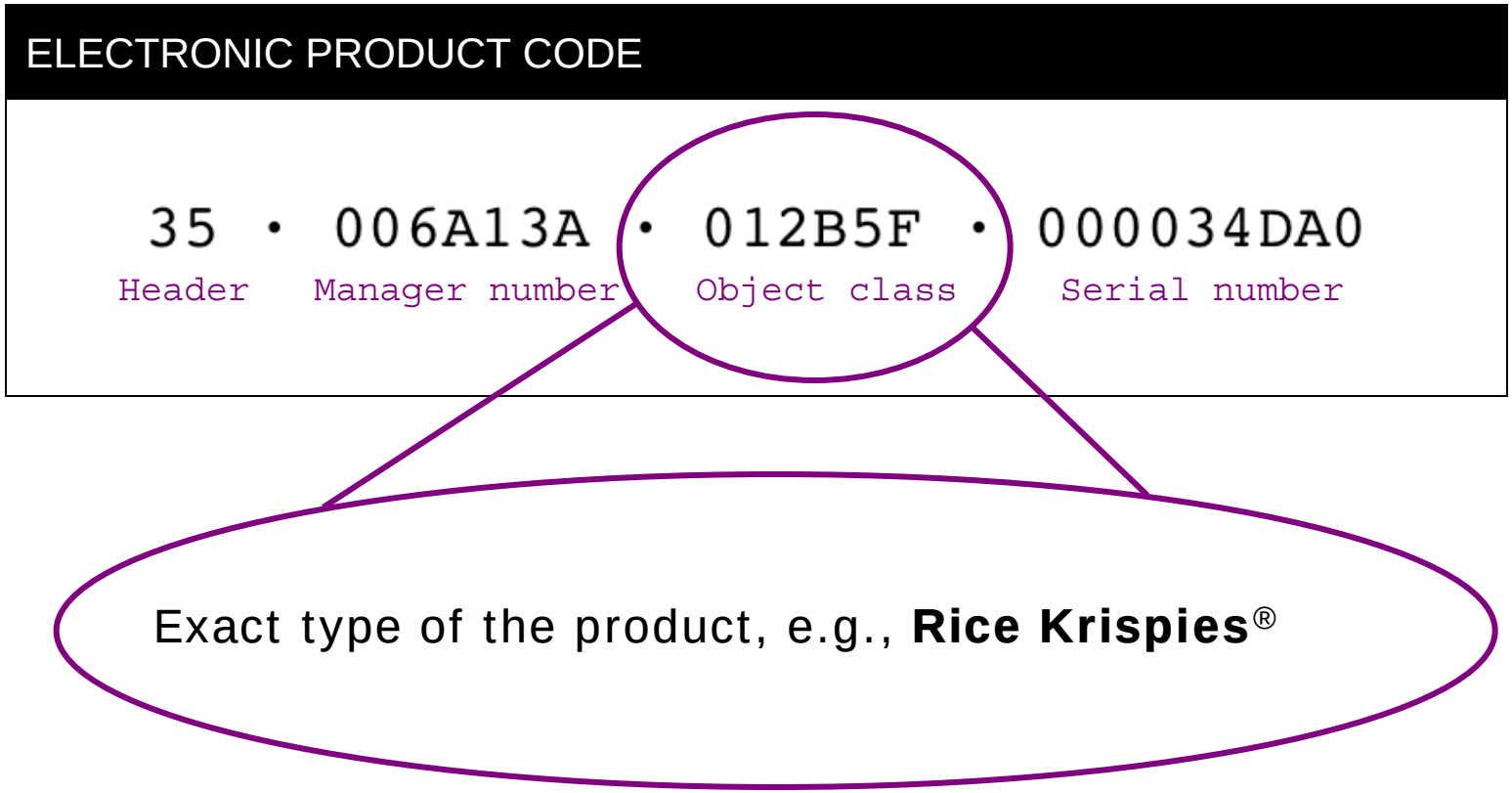
Structure of the EPC

- It support codes widely-used today or self defined conventions
- E.g., representation of an EPC general identifier (GID) of 96 bits:



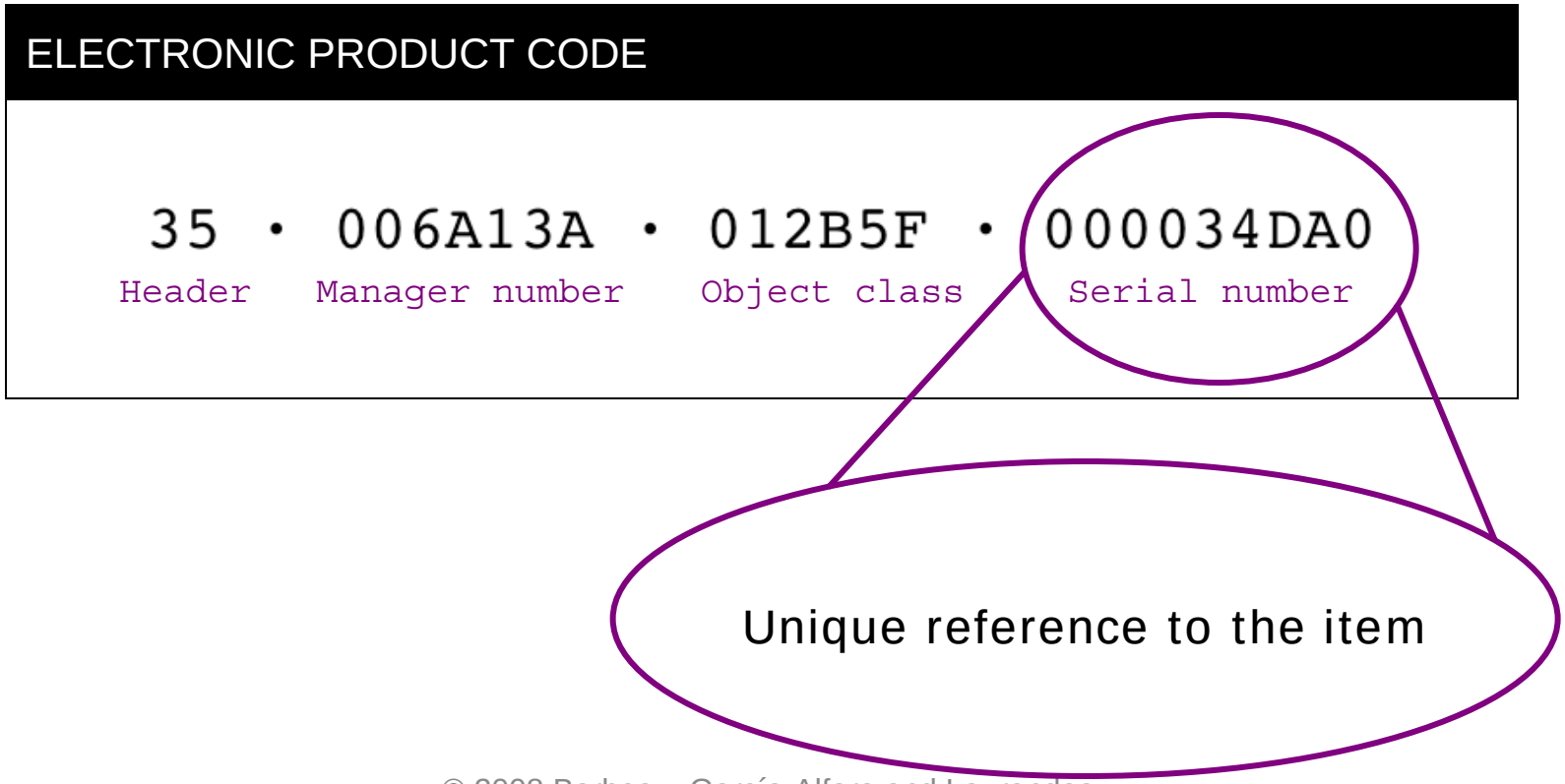
Structure of the EPC

- It support codes widely-used today or self defined conventions
- E.g., representation of an EPC general identifier (GID) of 96 bits:



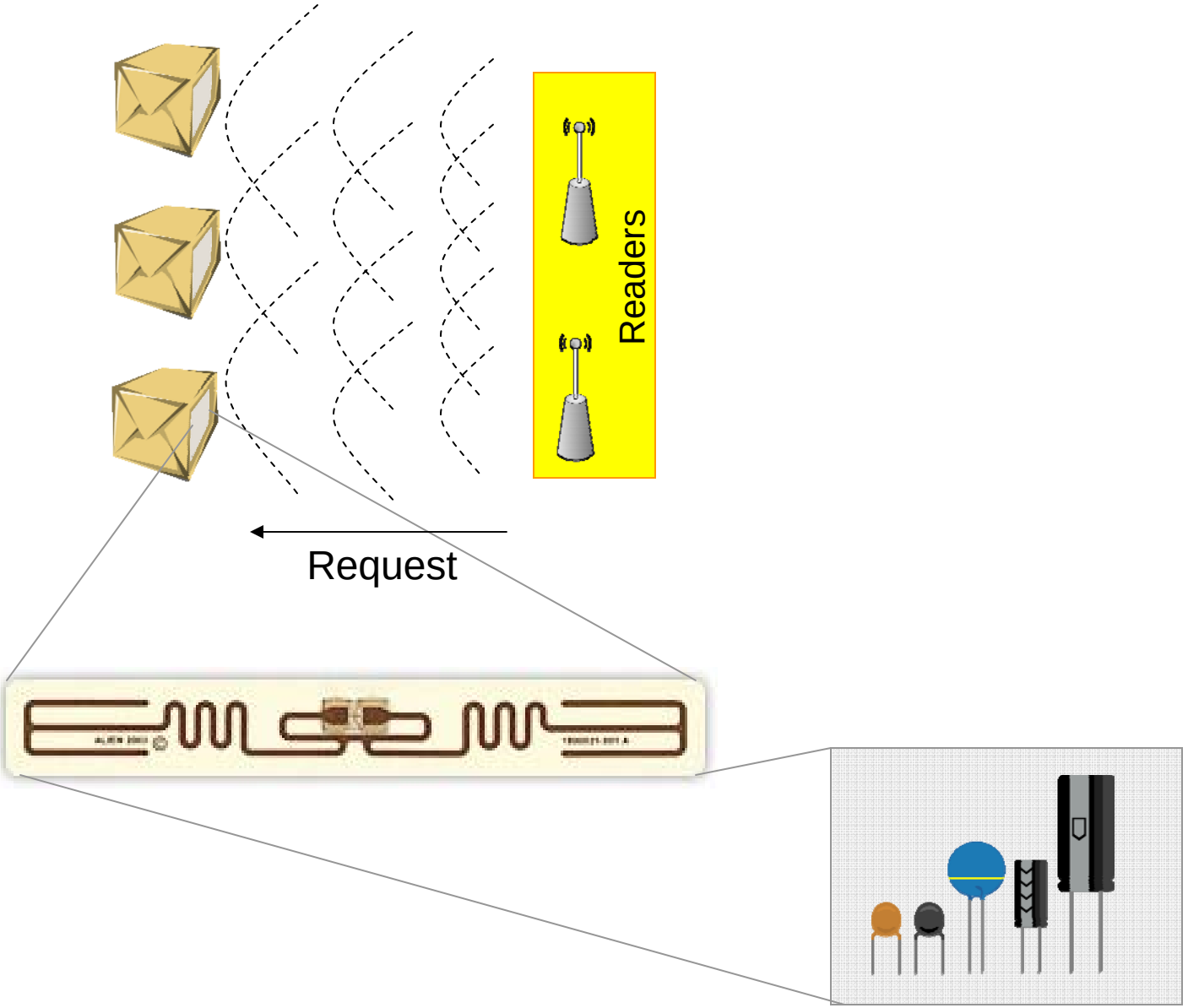
Structure of the EPC

- It support codes widely-used today or self defined conventions
- E.g., representation of an EPC general identifier (GID) of 96 bits:

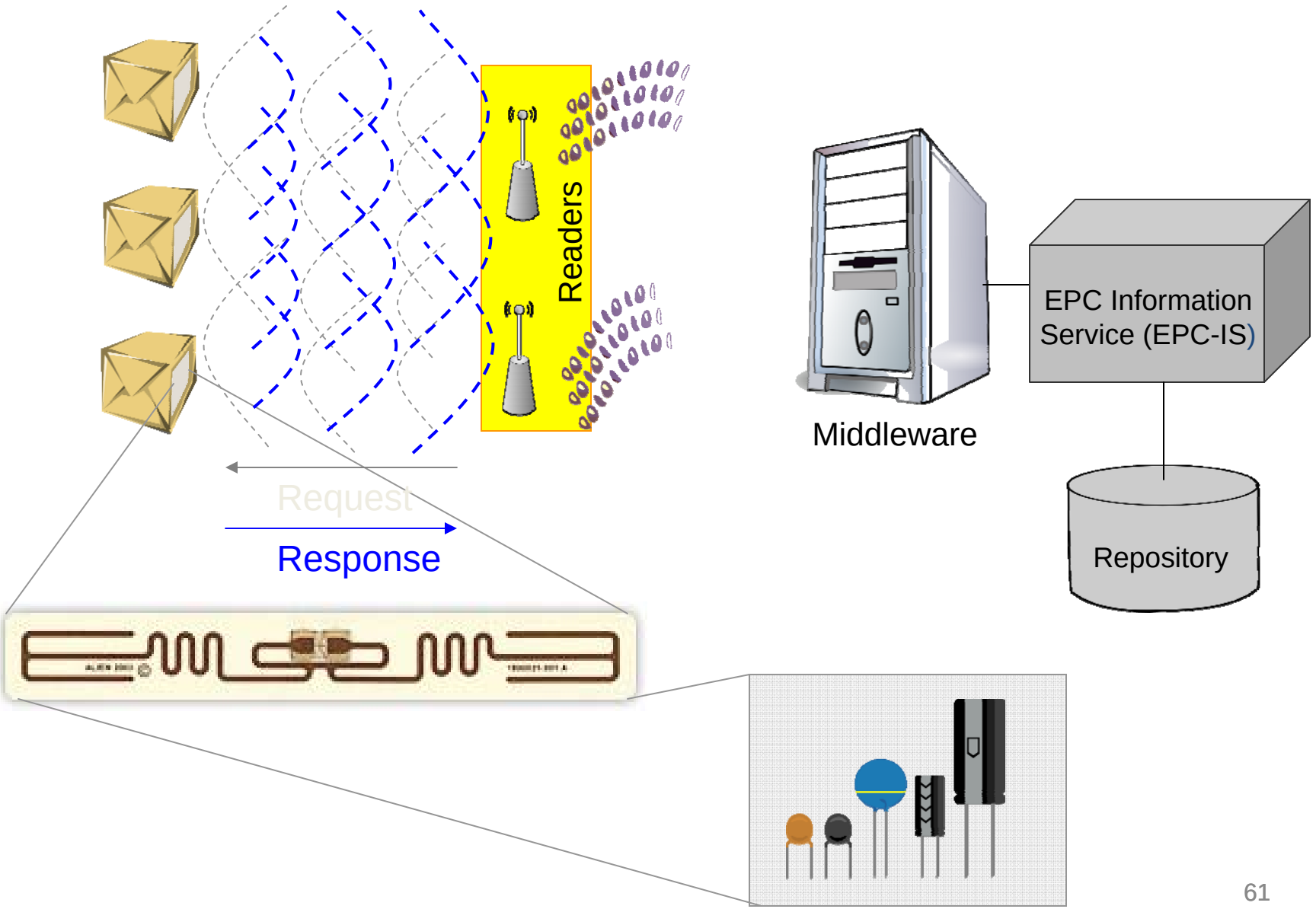


RFID tags & readers

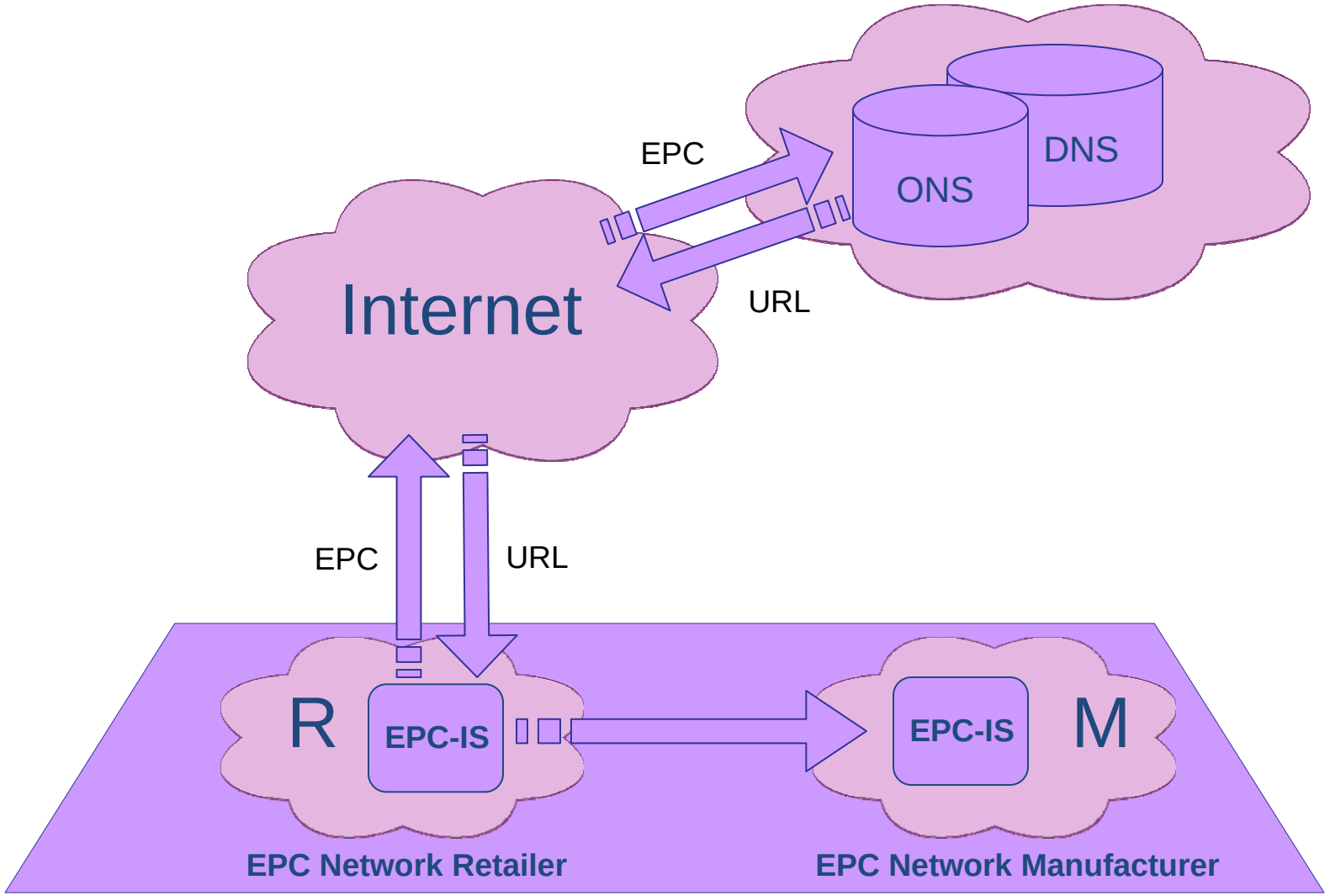
Sample EPC network



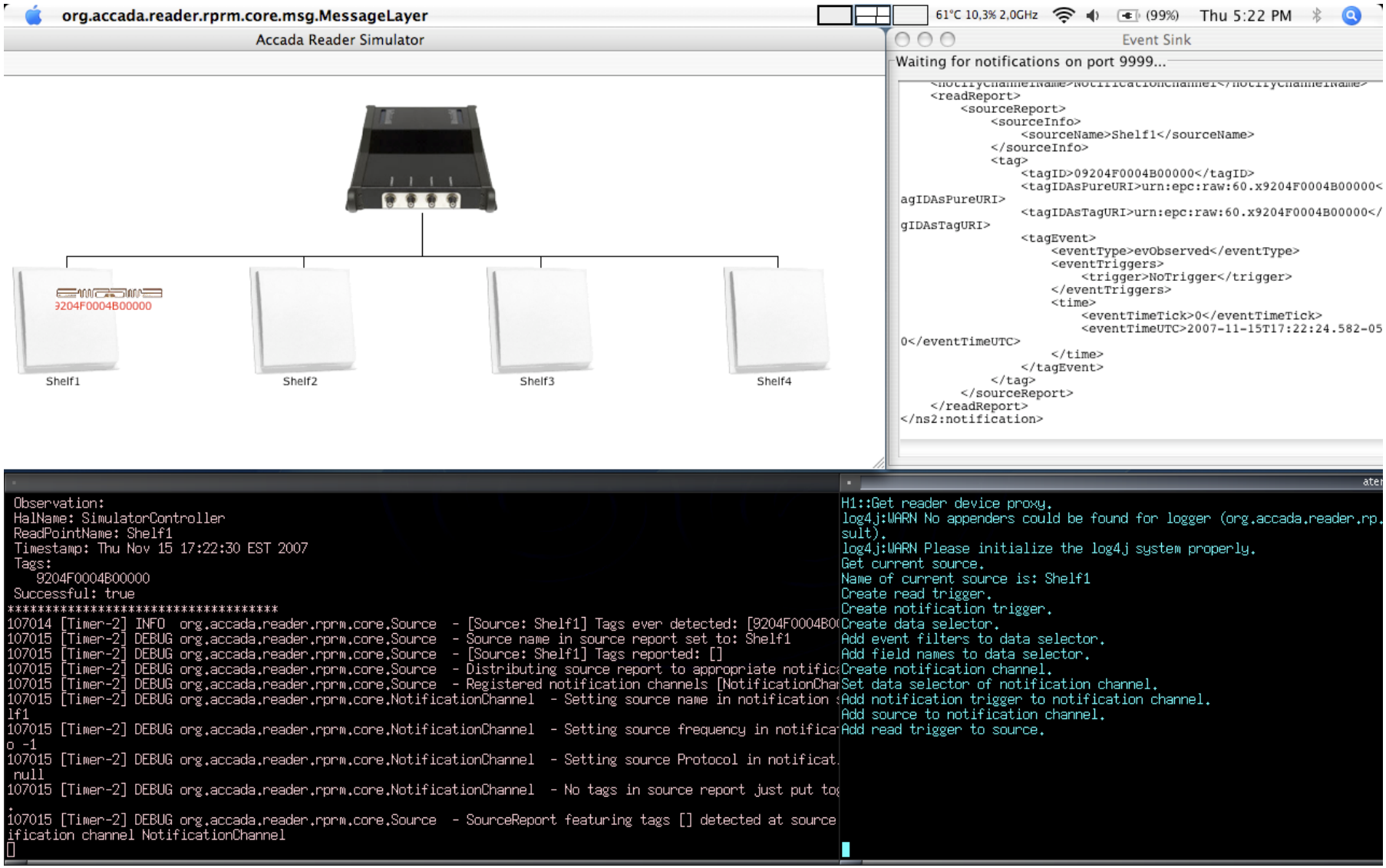
Sample EPC network



Interoperability between EPC Networks



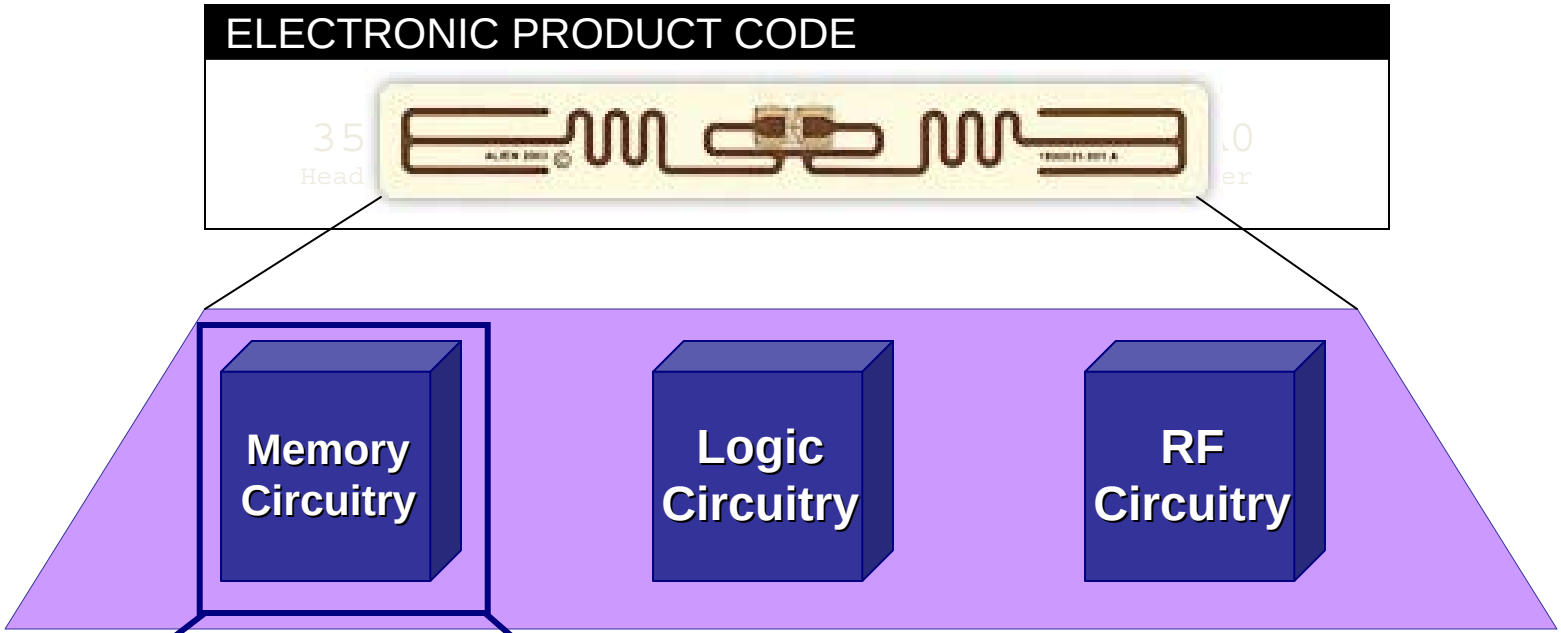
Simulation


org.accada.reader.rprm.core.msg.MessageLayer
61°C 10,3% 2,0GHz
(99%)
Thu 5:22 PM
Accada Reader Simulator
Event Sink
Waiting for notifications on port 9999...
<readReport>
<sourceReport>
<sourceInfo>
<sourceName>Shelf1</sourceName>
</sourceInfo>
<tag>
<tagID>09204F0004B00000</tagID>
<eventType>evObserved</eventType>
<eventTriggers>
<trigger>NoTrigger</trigger>
</eventTriggers>
<eventTimeTick>0</eventTimeTick>
</readReport>
</ns2:notification>
9204F0004B00000
Shelf1
Shelf2
Shelf3
Shelf4
Observation:
HalName: SimulatorController
ReadPointName: Shelf1
Timestamp: Thu Nov 15 17:22:30 EST 2007
Tags:
9204F0004B00000
Successful: true
107014 [Timer-2] INFO org.accada.reader.rprm.core.Source - [Source: Shelf1] Tags ever detected: [9204F0004B0
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.Source - Source name in source report set to: Shelf1
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.Source - [Source: Shelf1] Tags reported: []
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.Source - Distributing source report to appropriate notific
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.Source - Registered notification channels [NotificationChar
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.NotificationChannel - Setting source name in notification
lf1
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.NotificationChannel - Setting source frequency in notifica
o -1
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.NotificationChannel - Setting source Protocol in notificat
null
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.NotificationChannel - No tags in source report just put to
.
107015 [Timer-2] DEBUG org.accada.reader.rprm.core.Source - SourceReport featuring tags [] detected at source
ification channel NotificationChannel
H1::Get reader device proxy.
log4j:WARN No appenders could be found for logger (org.accada.reader.rp.
sult).
log4j:WARN Please initialize the log4j system properly.
Get current source.
Name of current source is: Shelf1
Create read trigger.
Create notification trigger.
Create data selector.
Add event filters to data selector.
Add field names to data selector.
Create notification channel.
Set data selector of notification channel.
Add notification trigger to notification channel.
Add source to notification channel.
Add read trigger to source.

Security threats to EPC networks

- Can target the different services of the EPC network
- In this talk, we focus on threats targeting the wireless channel used for the exchange of information between readers and tags

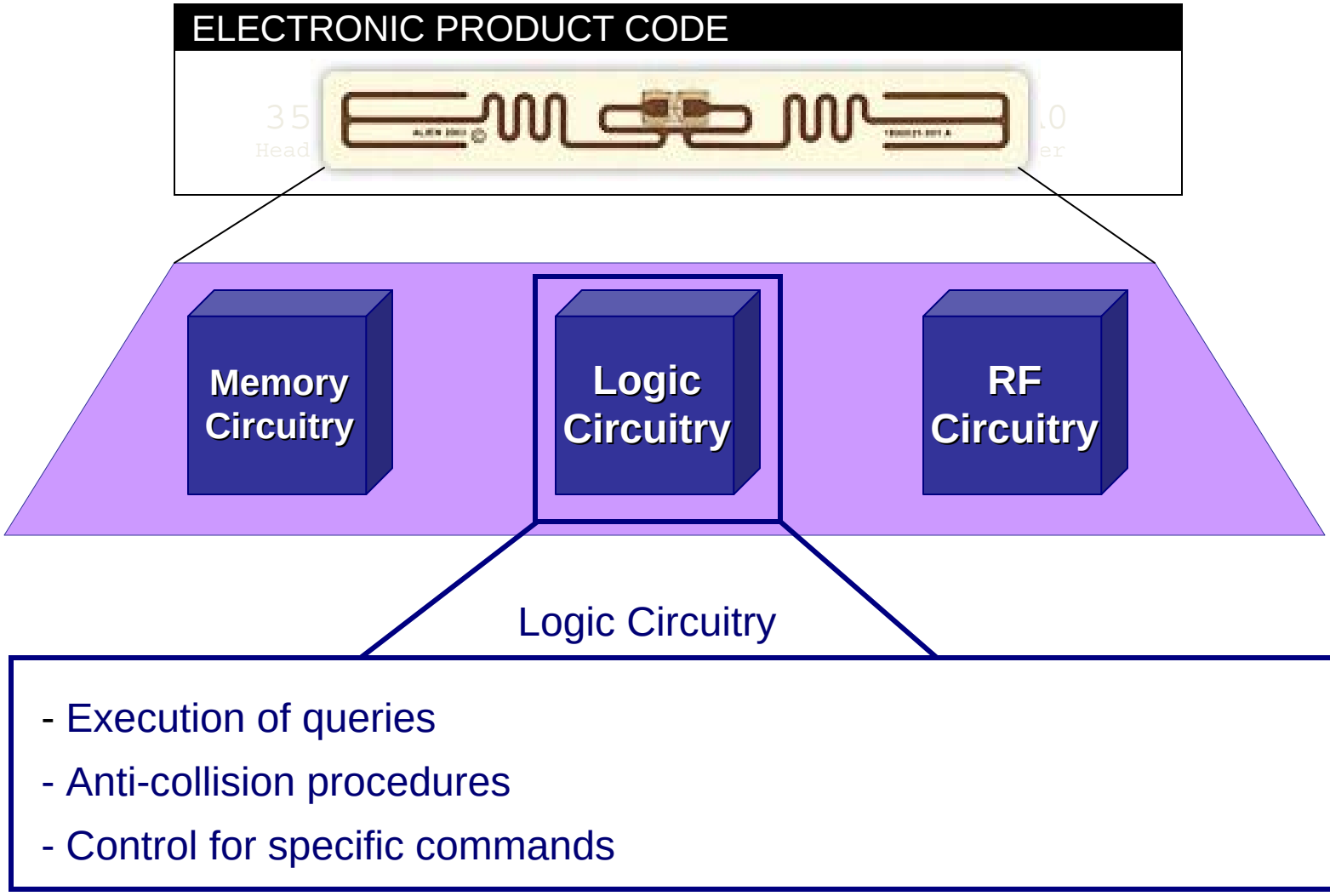
Characteristics of EPC tags



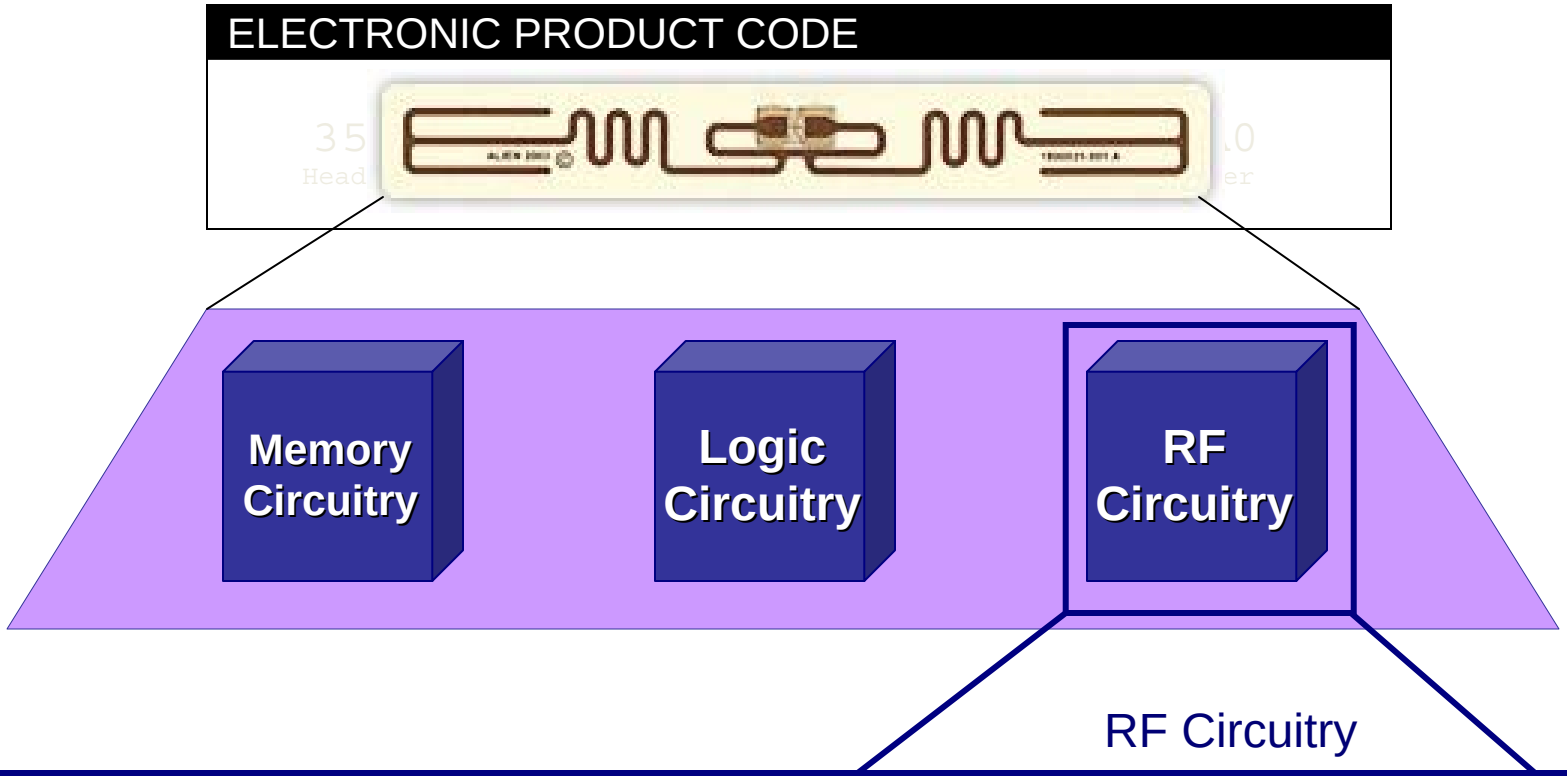
Memory Circuitry

- Very limited (generally few bytes)
- One part stores the EPC number; the rest is available to the user
- Read only write-once or Read/write

Characteristics of EPC tags



Characteristics of EPC tags



- Antenna pads
- Demodulation/Modulation circuits
- Capacitor/rectifier for storing energy and power the circuits

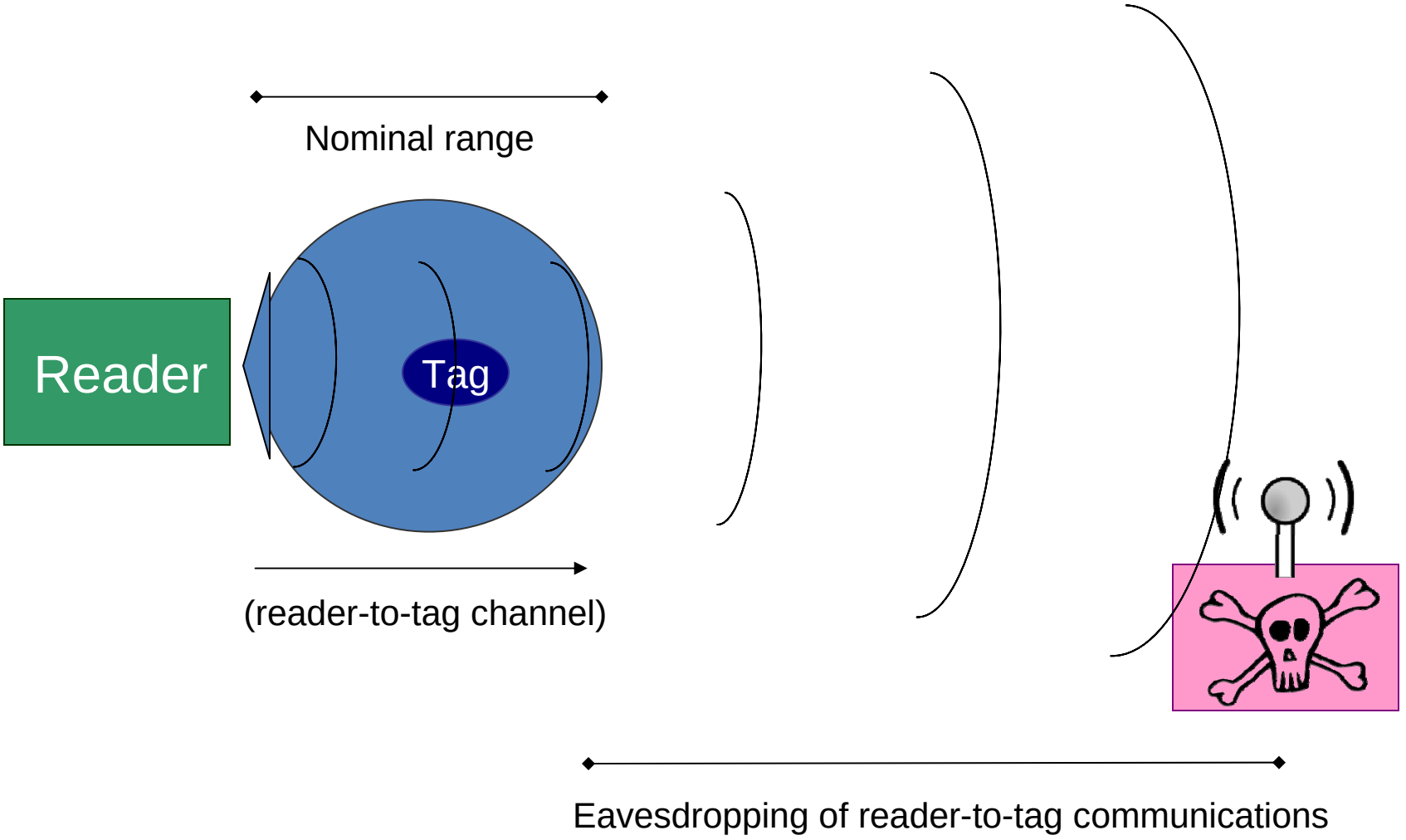
Security features of EPC tags

- Security features are minimalist
  - Kill & Access command

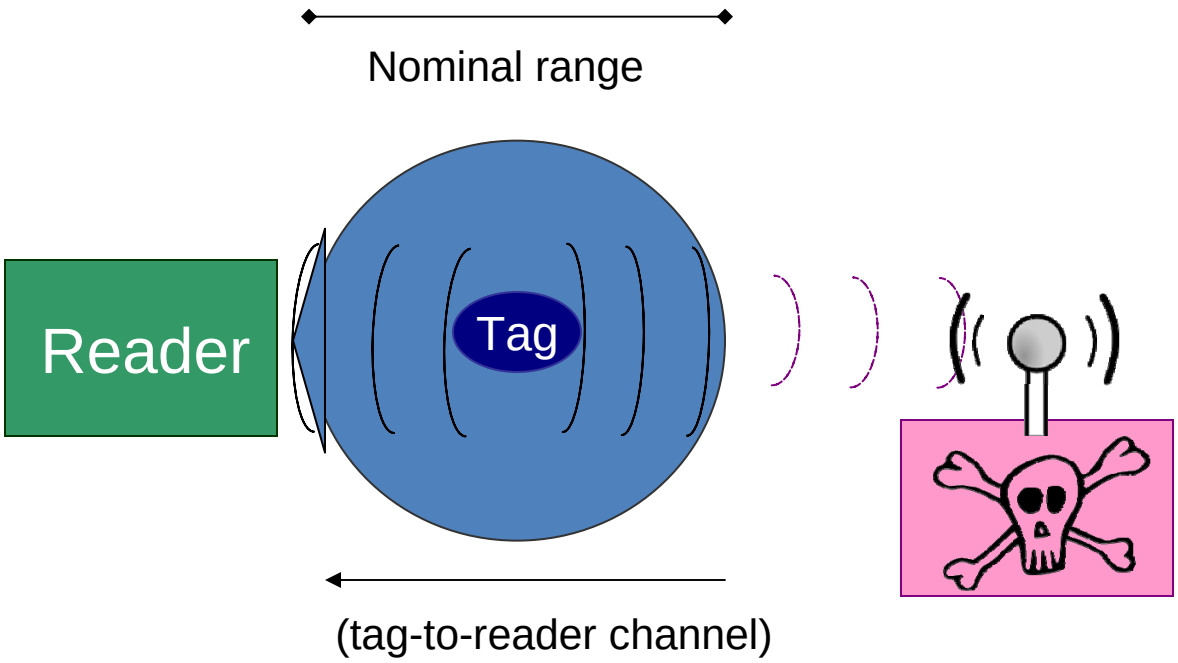
Security features of EPC tags

- Security features are minimalist
  - Kill & Access command
- Communication over insecure channel
  - Lack of authentication & confidentiality

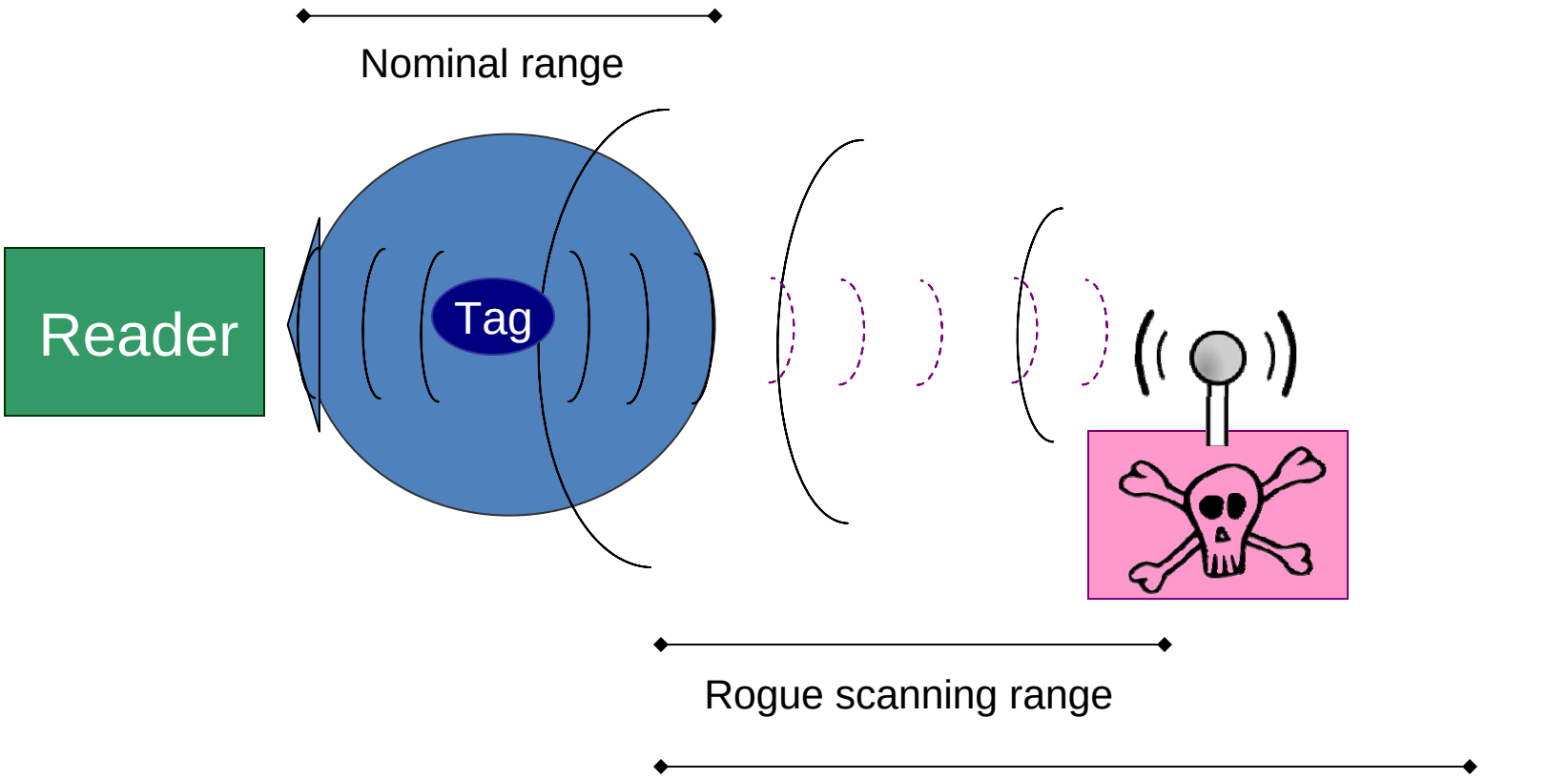
Eavesdropping reader channel



Eavesdropping tag channel

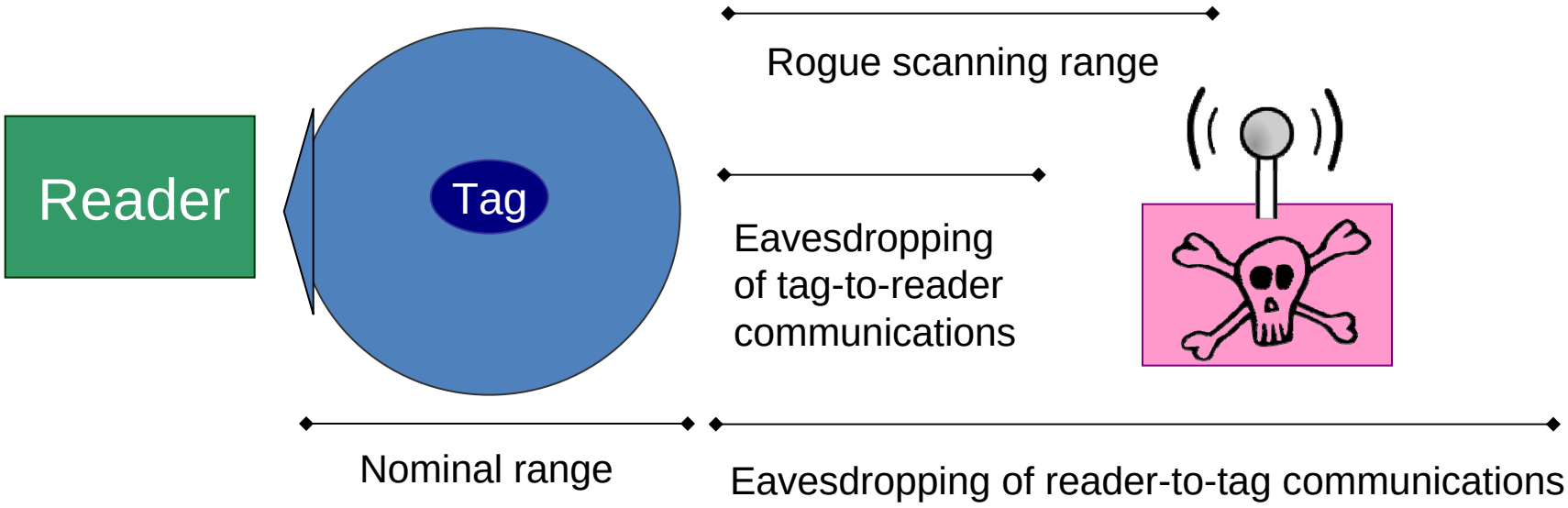


Rogue scanning



Motivation

- Are read-range distances sufficient to allow for it?
  - If we consider a dishonest third party using highly sensitive receivers, special antenna, … yes, it might be possible

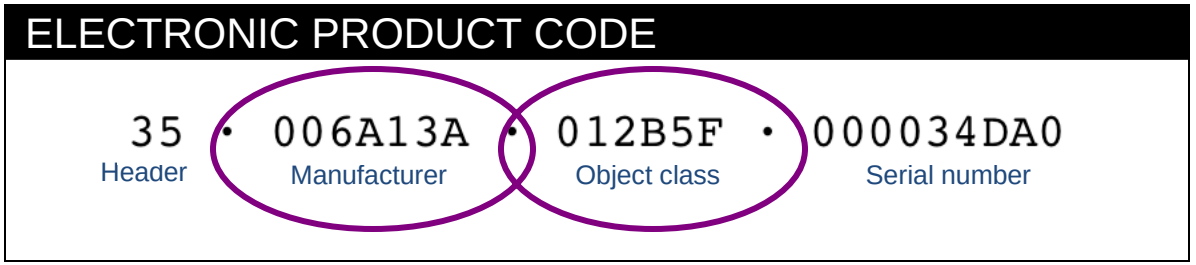


Consequences … replay attacks

- Eavesdropping the exchange of data between readers and tags, attackers can store the data, manipulate it, and retransmit modifications to illicitly request specific actions

Consequences … disclosure of information

- Which information could be disclosed? the EPC number associated to a tagged object



- It can lead to clandestine inventory, espionage of the organization, …
  - For retailers, impact might be rated as medium
  - For the management of materiel on health care or military scenarios, impact might be rated as high

EPC/RFID Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping	None	Likely	Medium	Major
			High	Critical
Rogue Scanning	None	Likely	Medium	Major
			High	Critical

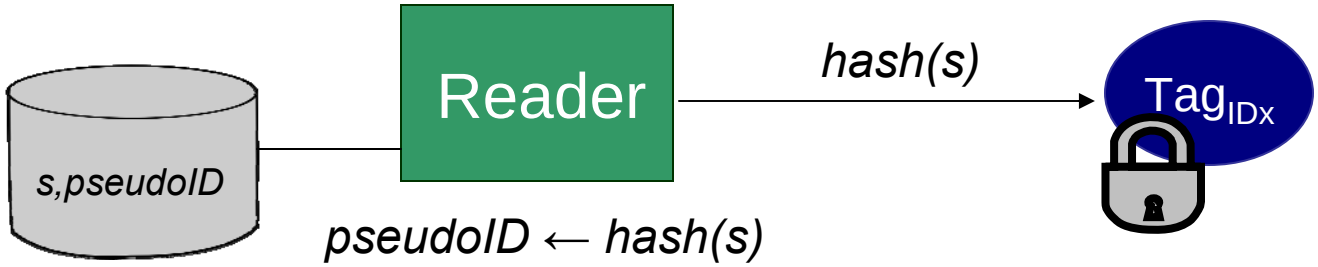
How to deal with these threats ?

- Shielding, jamming, blockers, guardians, …
  - It may work on some other RFID scenarios
  - Requires the management of new components

How to deal with these threats ?

- Shielding, jamming, blockers, guardians, …
  - It may work on some other RFID scenarios
  - Requires the management of new components
- Use of lightweight cryptography
  - E.g., implementation of XOR-based authentication protocols

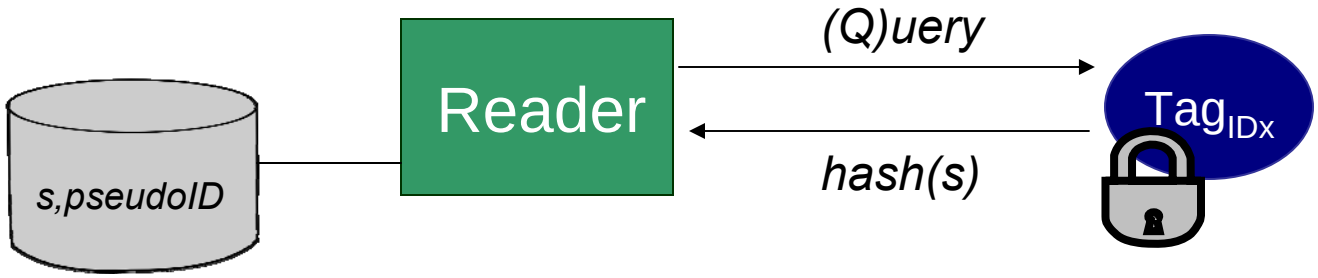
Hash-based AC



Locking the tag

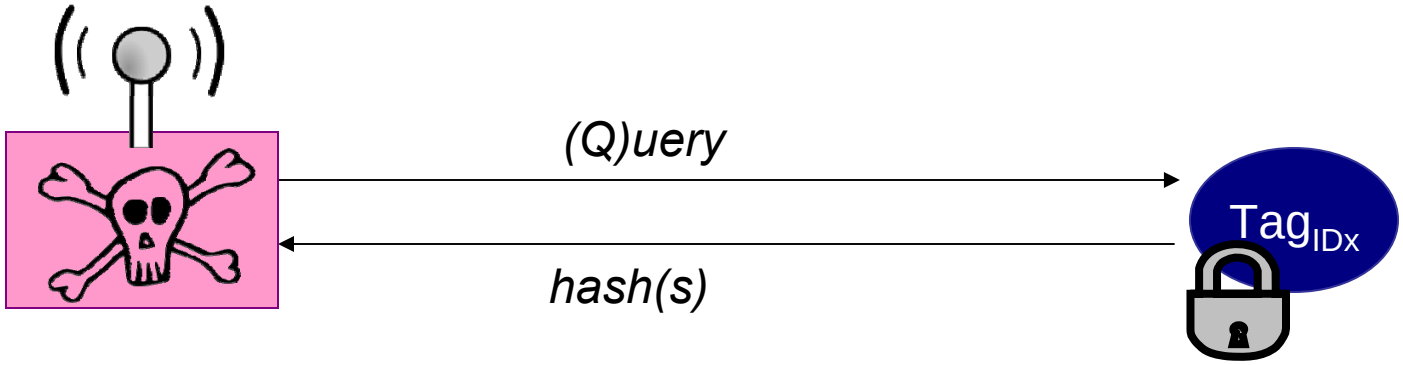
- Hash-lock approach:
  - Readers and tags must share a common secret (s)
  - When tag receives pseudoID = hash(s), it locks itself
    → when interrogated, it only answers with pseudoID
  - Tag unlocks itself when it receives the secret

Hash-based AC



Querying a locked tag

Hash-based AC



Querying a locked tag

EPC/RFID Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping	None	Likely	Medium	Major
			High	Critical
Rogue Scanning	None	Likely	Medium	Major
			High	Critical

EPC/RFID Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping	None	Likely	Medium	Major
			High	Critical
Rogue Scanning	None	Likely	Medium	Major
			High	Critical
Eavesdropping	Hash-based AC	Unlikely	Medium	Minor
			High	Minor
Rogue Scanning	Hash-based AC	Unlikely	Medium	Minor
			High	Minor

Activity 1: XOR-based hash

Given the following function:

```
hash(s:array of symbol){
    symbol H = 0000 0000;
    for (int i = 0; i < length(s); i++){
      H = H XOR s_i;
    }
    return H;
}
```

and the following table of symbols:

! = 0001 0000	$ = 0001 0001	% = 0001 1100	? = 0001 1111	. = 0010 1110
0 = 0011 0000	1 = 0011 0001	2 = 0011 0010	3 = 0011 0011	5 = 0011 0101
6 = 0011 0110	7 = 0011 0111	8 = 0011 1000	9 = 0011 1001	& = 0100 0000
A = 0100 0001	B = 0100 0010	C = 0100 0011	D = 0100 0100	F = 0100 0110

Activity 1: XOR-based hash

Compute the following operations:

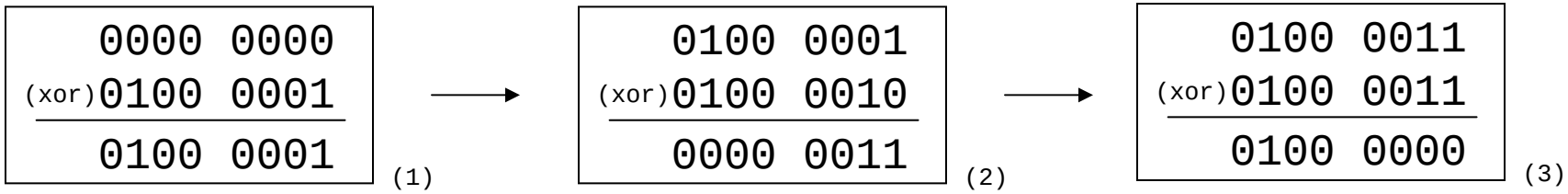
1) `hash("ABC")`
2) `hash("BCA")`
3) `hash("35.006A13A")`

Activity 1: XOR-based hash

Solution:

1) hash("ABC") → "&" (0100 0000)

Iterations:



Activity 1: XOR-based hash

Solution:

2) hash (“BCA”) → “&” (0100 0000)

Iterations:

Activity 1: XOR-based hash

Solution:

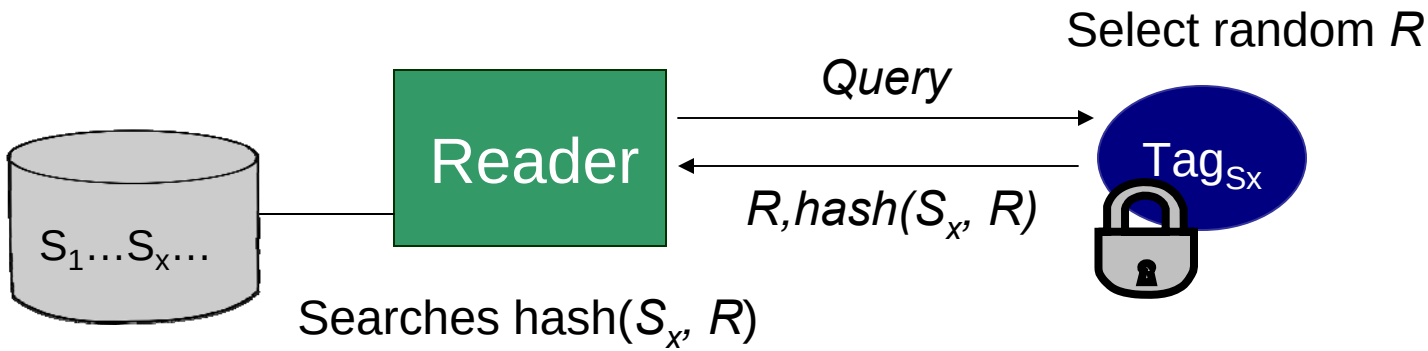
`3) hash (“35.006A13A”) → “%” (0001 1100)`

Iterations:

EPC/RFID Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping	Hash-based AC	Unlikely	Medium	Minor
			High	Minor
Rogue Scanning	Hash-based AC	Unlikely	Medium	Minor
			High	Minor
Tracking	Hash-based AC	Likely	Medium	Major
			High	Critical

Randomized Hash-based AC



EPC/RFID Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping	Hash-based AC	Unlikely	Medium	Minor
			High	Minor
Rogue Scanning	Hash-based AC	Unlikely	Medium	Minor
			High	Minor
Tracking	Randomized Hash-based AC	Unlikely	Medium	Minor
			High	Minor

Activity 2: keyed-hash

Given these two functions:

```
hash(s:array of symbol){
 symbol H = 0000 0000;
 for (int i=0;i<length(s);i++){
   H = H XOR s_i;
 }
 return H;
}
```

```
k_hash(m:array of symbol,k:symbol){
    symbol H = NULL;
    symbol I = 0010 1001;
    symbol O = 0110 0101;

    I = I XOR k;
    H = hash( [I, m ])
    return hash( [H, O ]);
}
```

and the following table of symbols:

! = 0001 0000	$ = 0001 0001	% = 0001 1100	? = 0001 1111	. = 0010 1110
0 = 0011 0000	1 = 0011 0001	2 = 0011 0010	3 = 0011 0011	5 = 0011 0101
6 = 0011 0110	7 = 0011 0111	8 = 0011 1000	9 = 0011 1001	& = 0100 0000
A = 0100 0001	B = 0100 0010	C = 0100 0011	D = 0100 0100	F = 0100 0110

Activity 2: keyed-hash

Compute the following operations:

```
1) k_hash(“ABC”, “!”)
2) k_hash(“ABC”, “5”)
```

Activity 2: keyed-hash

Solution:

1) k_hash(“ABC”, “!”) → “%” (0001 1100)

Iterations:

Activity 2: keyed-hash

Solution:

2) k_hash(“ABC”, “5”) → “9” (0011 1001)

Iterations:

References

- M. Barbeau and C. Laurendeau, "Analysis of Threats to WiMAX/802.16 Security", in: Y. Zhang and H.-H. Chen (Editors), *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks,* CRC Press, 2008.
- J. Garcia-Alfaro, M. Barbeau and E. Kranakis, *Analysis of Threats to the Security of EPC Networks,* Sixth Annual Communication Networks and Services Research (CNSR) Conference, Halifax, Nova Scotia, Canada, 2008.
- M. Barbeau and E. Kranakis. *Principles of Ad Hoc Networking*. John Wiley & Sons Ltd, West Sussex, England, 2007.
- M. Barbeau and C. Laurendeau, “Tilting at Giants: Avoiding Quixotic Pursuits in Understanding the Threats to Wireless Network Security,” MITACS e-newsletter, *Connections*, September 2007.
- C. Laurendeau and M. Barbeau, *Threats to Security in DSRC/WAVE,* 5th International Conference on Ad-hoc Networks, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 4104, 2006, pp. 266-279.

URLs: **http://www.scs.carleton.ca/~barbeau/**
http://www.scs.carleton.ca/~claurend/
http://www.scs.carleton.ca/~joaquin/