Securing the Next Wave of Technology

Dr. Daniel W. Engels
Chief Technology Officer
Revere Security

© 2009-2011 Revere Security. All rights reserved.

In my Lifetime, Computers have…

Image source: Wikipedia Commons, German Federal Archive
IBM 360 circa 1973

© 2009-2011 Revere Security. All rights reserved.

Revere SECURITY

…become a Grain of Sand

Passive RFID Chip circa 2010

© 2009-2011 Revere Security. All rights reserved.

TODAY @ PCWORLD

Sony Makes it Official: PlayStation Network Hacked

By Keir Thomas, PCWorld Apr 23, 2011 7:35 AM

When Sony's PlayStation Network was taken offline three days ago, all eyes fell on the Anonymous group, who've taken a dislike to Sony over its treatment of hardware hacker George Hotz. The network allows online play between PlayStation 3 consoles and boasts 70 million users, so this is no small inconvenience.

Last night Sony confessed that an "external intrusion" caused the company to take-down the PlayStation Network and also Sony's Qriocity service in order "to verify the smooth and secure operation of our network services going forward". However, they're not saying anything more, or giving a time scale as to when gamers will be able to resume playing online.

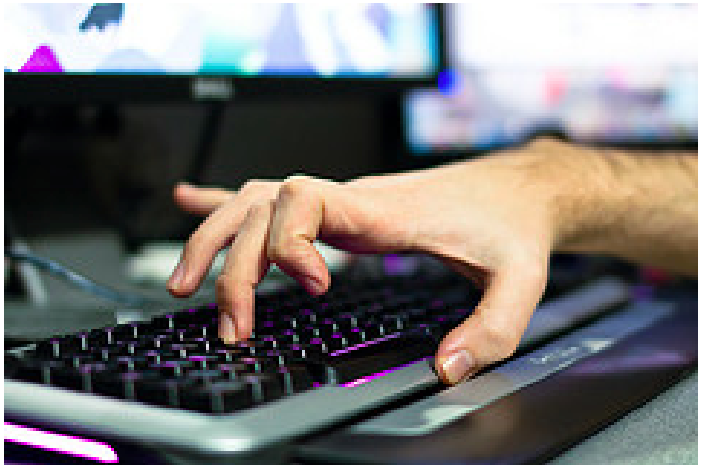
What makes it strange is that Anonymous has denied being involved, claiming "for once we didn't do it" and suggesting Sony was using rumors of an Anonymous attack as cover for an internal problem with their servers. As yet Anonymous hasn't responded to the latest update from Sony.

However, the decentralized nature of Anonymous means that individuals act alone with no governance, and Anonymous admitted that "it could be the case that other Anons have acted by themselves."

CITIBANK

How Hackers Stole 200,000+ Citi Accounts Just By Changing Numbers In The URL

By Ben Popken on June 14, 2011 3:00 PM The Consumerist



(Sebastian Anthony)

Details have emerged has to how hackers were able to steal over 200,000 Citi customer accounts, including names, credit card numbers, mailing addresses and email addresses. It turns out quite easily, in fact. All they had to do was log in as a customer and change around a few numbers into the browser's URL bar, NYT reports. Facepalm.

Basically after you logged into your account as a Citi customer, the URL contained a code identifying your account. All you had to do was change around the numbers and boom, you were in someone else's account.

So if the URL was something like citibank.com/user/12345, all you had to do was change it to citibank.com/user/123456 and you had access to all of their account information.

The hackers then used a simple script that automatically scraped all the account information, saved it, and then changed the numbers in the URL and repeated the process. Hundreds of thousands of times.

As someone who has been on the internet for a few years, this is a dead simple and common hack and Citi should have seen it and prevented against it. Seriously, this is kindergarten level stuff. Really, really stupid.

What Went Wrong?

- The **Internet** was designed to **SHARE** information
- The **World Wide Web** was designed to **SHARE** information
- Security was an **AFTERTHOUGHT**

  (and it continues to be an afterthought today)

Steal this barcode

Re-Code.com offers a do-it-yourself product repricing service. Wal-Mart is not amused.

By Katharine Mieszkowski

www.salon.com

Apr 10, 2003 | Is it social commentary, or shoplifting?

The Web site Re-Code.com parodies the design and chipper lingo of Priceline.com's "name your own price" shopping site. It invites shoppers to "recode your own price," by making their own barcodes using the site's barcode generator. The theory: There's just a 10-digit number standing between you and a better deal on anything that you want in a store, and this site will help you crack the code.

The site's creators call it satire. Wal-Mart's legal counsel calls it an incitement to theft and fraud.

Note: re-code.com is now the website for a weight loss product

Researchers Hack Cars via Wireless Tire Pressure Sensors

by **Caleb Johnson** on August 11, 2010 at 06:20 PM

FILED UNDER: security, transportation

courtesy: USC/Rutgers U.

59 tweets
retweet

Back in May, we told you about a study that proved it's fairly easy to remotely hack into a car's onboard computer. Now, according to Technology Review, researchers at the University of South Carolina and Rutgers University have figured out how to hack into the tire-pressure-monitoring systems (TPMS) featured on many vehicles. The researchers used easy-to-find equipment that cost about $1,500 -- including a programmable radio transmitter, a specialized circuit board and free software -- to remotely hack the TPMS. By doing so, they could trigger warning lights by altering wireless communications, and remotely track the vehicle wherever it went, due to the fact that each TPMS features a unique ID.

In and of themselves, these findings, which will be presented at a security conference in Washington, D.C. this week, don't pose a huge threat to drivers. The troubling part is the bigger picture; it appears that more and more evidence supports the idea that the wireless computer systems featured on most vehicles are greatly lacking in security. These built-in computer systems have made driving both more pleasurable and safer, but, as with any industry, technological change should never outpace security or safety. [From: Technology Review]

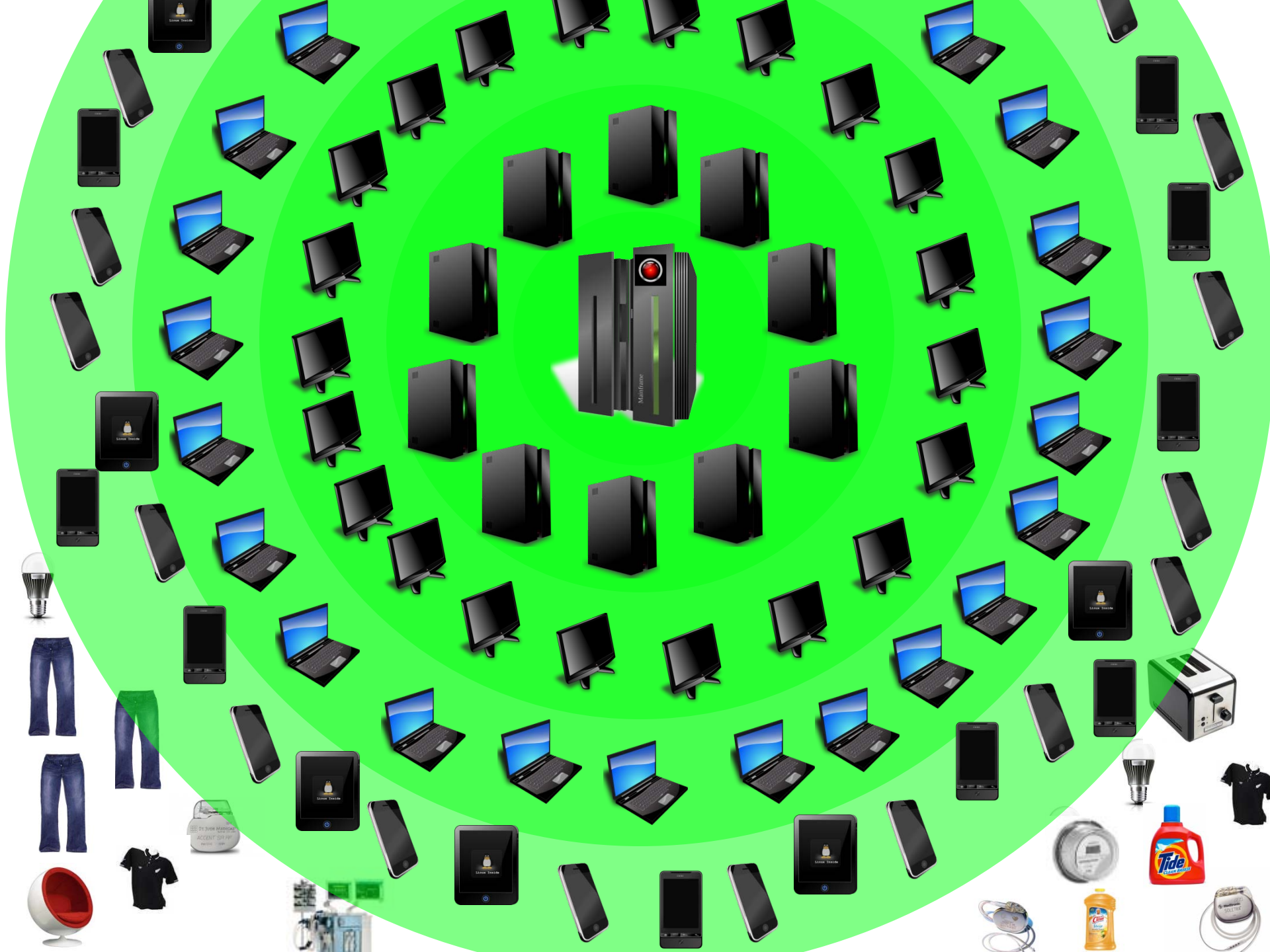
TAGS: CAR, CAR TECH, CARHACKING, CARTECH, HACK, RUTGERSUNIVERSITY, SECURITY, TOP, TPMS, UNIVERSITYOFSOUTHCAROLINA

source:
http://www.technologyreview.com/communications/25962/

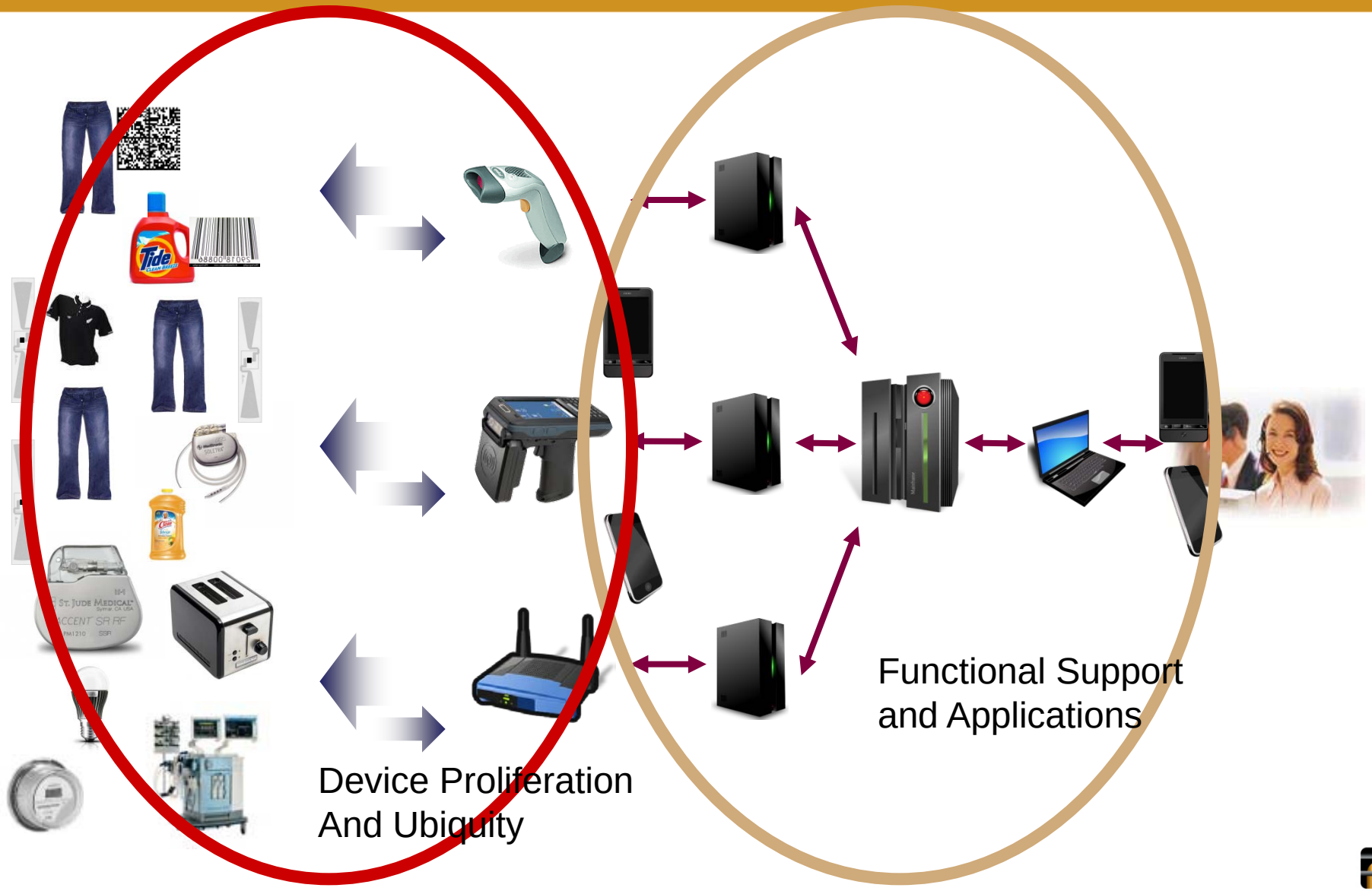
What Went Wrong?

- The **BARCODE** was designed to **SHARE** information
- The **RFID TAG** was designed to **SHARE** information
- Security was an **AFTERTHOUGHT**

  (and it continues to be an afterthought today)


Mainframe
Tide

The Next Wave of Technology



© 2009-2011 Revere Security. All rights reserved.

The Internet of Things is Here

Wal-Mart's EPC Garment Tracker System

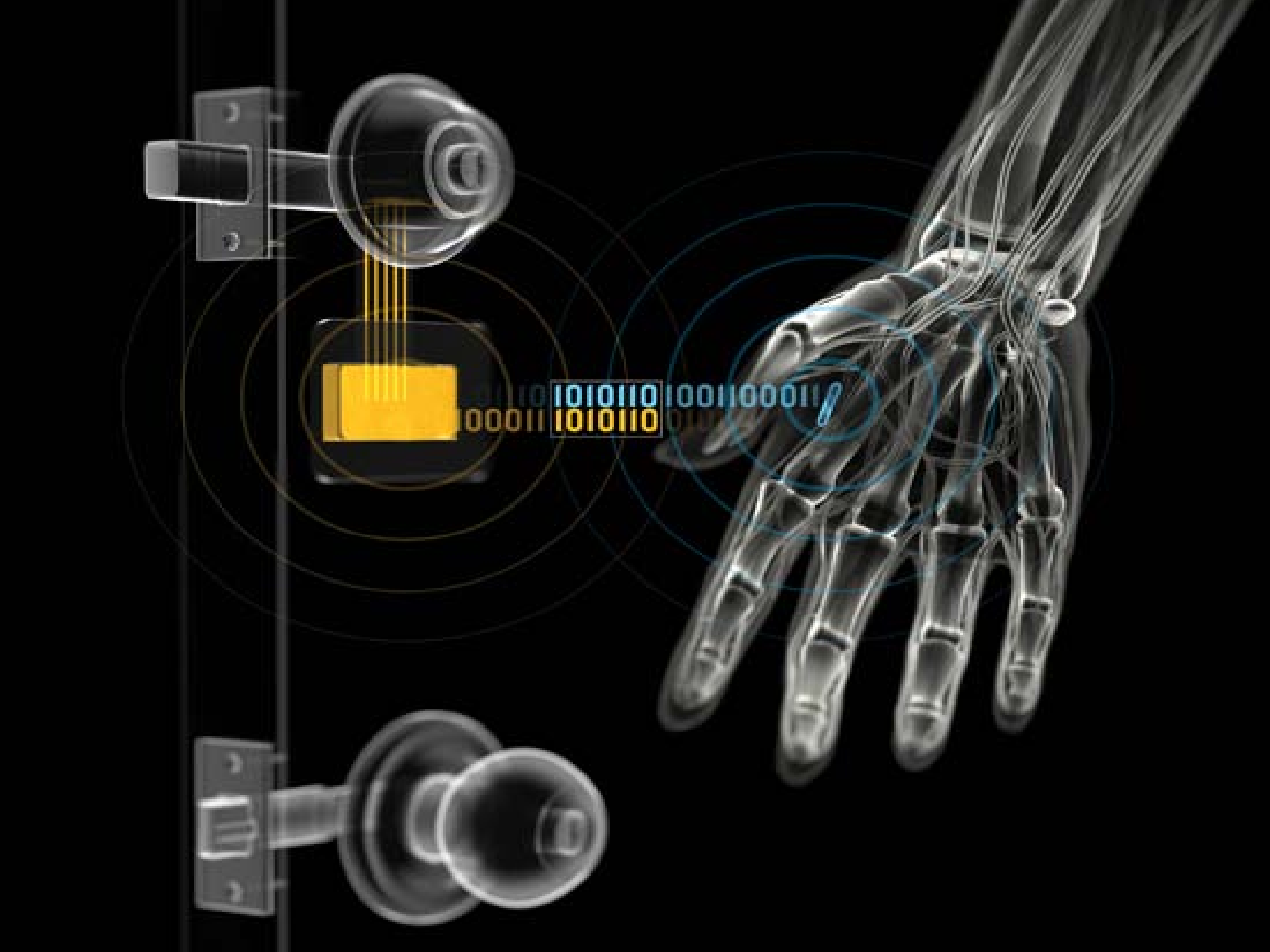
1 Tag

2 Track

3 Manage

4 Dispose

© 2009-2011 Revere Security. All rights reserved.


1010110
1010110

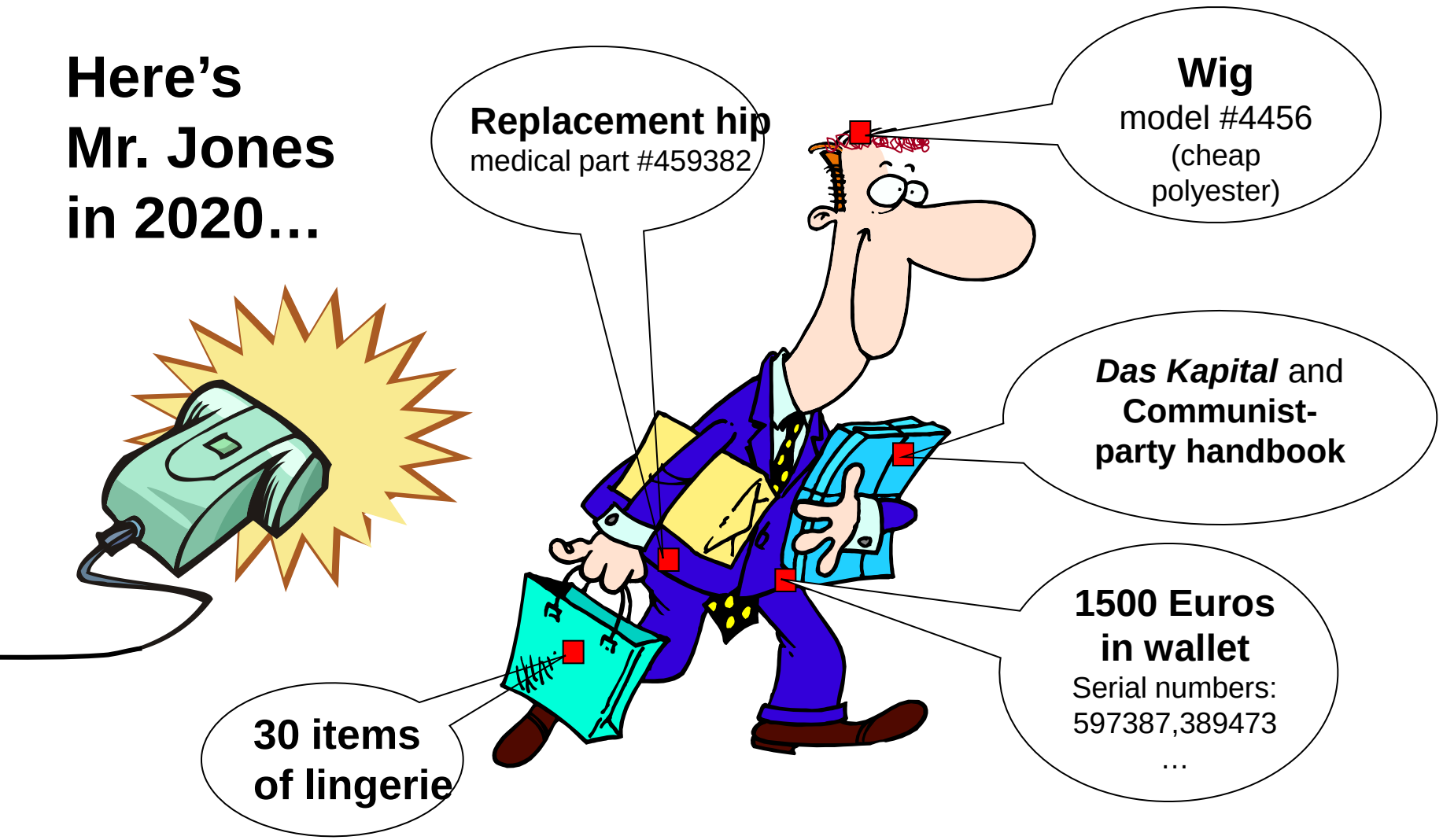
No Device is an Island

- Wireless Communications bypass all basic security mechanisms except Cryptography
- Every device is an entry point into your network
- No device is to be fully trusted by any other
- Every device is a city state to be protected

© 2009-2011 Revere Security. All rights reserved.

The Security Problem has Changed

Here's Mr. Jones in 2020…



Slide Courtesy of Ari Juels

© 2009-2011 Revere Security. All rights reserved.

Common Edge Device Attacks

Eavesdropping 	• Listen to a conversation without the participants' knowledge or consent
Snooping 	• Illicit reading of a device's identity and data
Tracking 	• Determine where a specific device is currently
Tracing	• Determine where a specific device has been
Replay 	• Repeat a recorded conversation
Counterfeit 	• Create a duplicate device
Spoofing 	• Masquerade as a tag, reader, or other device

© 2009-2011 Revere Security. All rights reserved.

Security Must be Designed into Every *Device*, Every Communication *Protocol*, and the *Network*

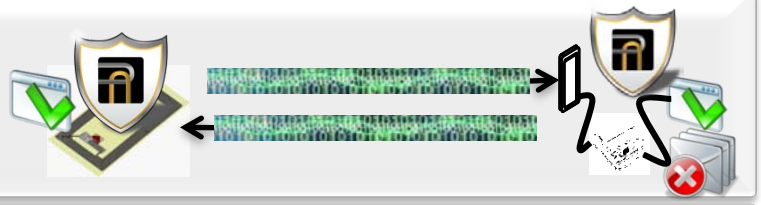
From the Beginning

© 2009-2011 Revere Security. All rights reserved.

Edge Device Security Mechanisms

Over the Air Encryption: over the air data and commands are encrypted with full data authentication (**secure communication channel**)

Device Authentication: validates devices as TRUSTED before data divulged or accepted. (**identity authentication**)



Secure Identification tags communicated identifier changes securely over time – identity never sent in the clear. (**secure identification**)

Pre-Authentication (Cloaking) enables device to determine whether it is SAFE to respond to a request or remain silent (**cloaking**)

Information Assurance authenticate data integrity and data origin. (**data authentication**)

© 2009-2011 Revere Security. All rights reserved.

Black

Cloaked Devices

Here's Mr. Jones in 2020…

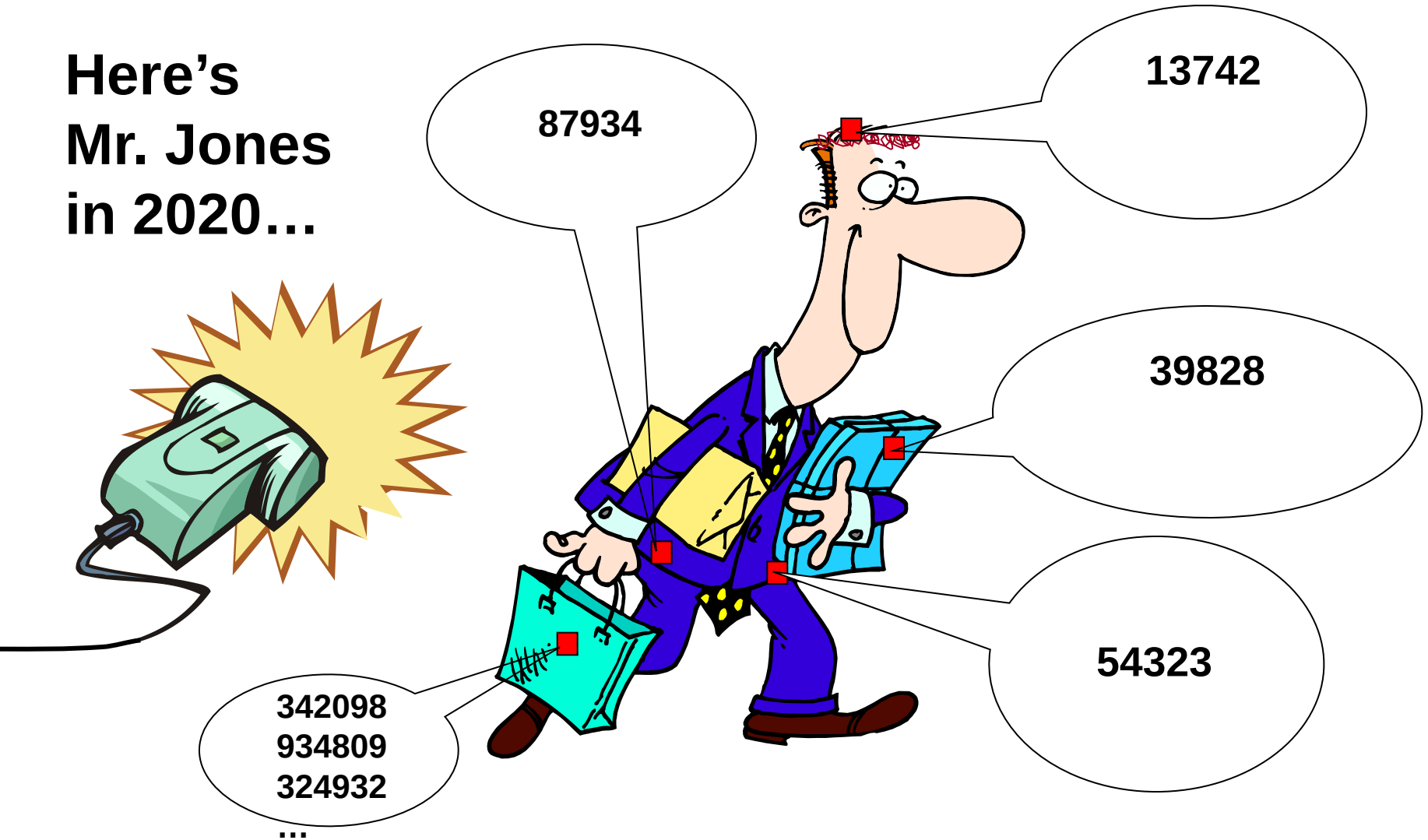
Slide Courtesy of Ari Juels

© 2009-2011 Revere Security. All rights reserved.

Secure IDs

Secure Identifiers

Here's Mr. Jones in 2020…



Slide Courtesy of Ari Juels

© 2009-2011 Revere Security. All rights reserved.

Limits of New Edge Devices

Size

- RFID tags have limited size
- Passive UHF tags have approximately 2000 GEs for security
- Microprocessor based tags and other devices have approximately 2 kB of ROM available for security

Speed

- Identification rate and data communication rates cannot be affected by security mechanisms
- Passive UHF tags have 10's to 100's of clock cycles
- Active microprocessor based tags and devices typically have 10's to 100's of microseconds for security

Power

- Power used for security affects range and battery life
- Passive UHF tags have 1 uW of power available for security without significant range reductions
- Battery powered devices have less than five thousand clock cycles per security computation without significant battery degradation

© 2009-2011 Revere Security. All rights reserved.

Standard Cryptography Doesn't Fit

AES	• Standard symmetric key block cipher • Designed for 32-bit microprocessors • Large, slow, and power inefficient on new edge devices with large block size • Not well suited for resource constrained environments of passive UHF RFID tags
ECC	• Standard asymmetric public key cipher • Requires significant time and space • Large, slow, and power inefficient • Not suited for resource constrained environments of RFID tags

© 2009-2011 Revere Security. All rights reserved.

AES and EAX Mode

(Brian Gladman Source Code)

HB2

(Eric Smith Source Code)

Hummingbird Equations

Encryption Process	Decryption Process	Initialization Process (Four Rounds Encryption)
$V12_t = E_{K1}(PT \boxplus RS1_t)$ $V23_t = E_{K2}(V12_t \boxplus RS2_t)$ $V34_t = E_{K1}(V23_t \boxplus RS3_t)$ $CT'_t = E_{K2}(V34_t \boxplus RS4_t)$ $CT_t = CT'_t \boxplus RS1_t$	$CT'_t = CT_t \boxminus RS1_t$ $V34_t = D_{K2}(CT'_t) \boxminus RS4_t$ $V23_t = D_{K1}(V34_t) \boxminus RS3_t$ $V12_t = D_{K2}(V23_t) \boxminus RS2_t$ $PT_t = D_{K1}(V12_t) \boxminus RS1_t$	$V12_t = E_{K1}(t \boxplus RS1_t)$ $V23_t = E_{K2}(V12_t \boxplus RS2_t)$ $V34_t = E_{K1}(V23_t \boxplus RS3_t)$ $TV_t = E_{K2}(V34_t \boxplus RS4_t)$
Internal State Updating		Internal State Updating
$RS1_{t+1} = RS1_t \boxplus V34_t$ $RS2_{t+1} = RS2_t \boxplus V12_t$ $RS3_{t+1} = RS3_t \boxplus V23_t$ $RS4_{t+1} = RS4_t \boxplus V12_t \boxplus RS1_{t+1}$ $ACC1_{t+1} = ACC1_t \oplus RS1_{t+1}$ $ACC2_{t+1} = ACC2_t \oplus RS2_{t+1}$ $ACC3_{t+1} = ACC3_t \oplus RS3_{t+1}$ $ACC4_{t+1} = ACC4_t \oplus RS4_{t+1}$		$RS1_{t+1} = (RS1_t \boxplus TV_t) \lll 3$ $RS2_{t+1} = (RS2_t \boxplus V12_t) \ggg 1$ $RS3_{t+1} = (RS3_t \boxplus V23_t) \lll 8$ $RS4_{t+1} = (RS4_t \boxplus V34_t) \lll 1$ $ACC1_{t+1} = ACC1_t \oplus RS1_{t+1}$ $ACC2_{t+1} = ACC2_t \oplus RS2_{t+1}$ $ACC3_{t+1} = ACC3_t \oplus RS3_{t+1}$ $ACC4_{t+1} = ACC4_t \oplus RS4_{t+1}$

Revere Security

Cipher Comparison (1)

Comparison of Smallest Published Implementations

Algorithm	Security	I_{mean} (uA@100kHz)	Chip Area (GE)	Clocks (Cycles)
AES-128*	128	3.0	3,400	1032
Grain**	128	1.28	1,857	(513) + 128
PRESENT***	128	3.67	2,332	64
HB2/HW20	128	1.44	2,159	(80) + 160
HB2/HW16	128	1.54	2,332	(80) + 128
HB2/HW4	128	1.60	3,220	(16) + 32

*M. Feldhofer, *"AES Implementation on a Grain of Sand"*
**T. Good & M. Benaissa, *"Hardware Results for Selected Stream Cipher Candidates"*
****A. Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a Pervasive World", PhD Thesis*

Cycles to encrypt 128 bits of plain text. Number in parenthesis are initialization clocks.
AES initialization is not reported. PRESENT initialization is not reported.
AES mode overhead is not reported. PRESENT mode overhead is not reported.

Revere Security

Cipher Comparison (2)

Cipher	Process [μm]	Key Size	Block Size	Cycles / Block	Datapath Width	GE	Init (Cycles)	Throughput (bits/cycle)	Power 10 MHz (μW)
HB2-ee4c [1]	0.13	128	16	4	16	3220	16	4	163.1
HB2-ee16c [1]	0.13	128	16	16	16	2332	80	1	156.8
HB2-ee20c [1]	0.13	128	16	20	16	2159	80	0.8	149.1
Grain-128x1 [2]	0.13	128	1	1	1	1857	513	1	167.7
Grain-128ax2 [3]	0.13	128	1	1	1	2867	160	1	258.9
AES-128 [4]	0.13	128	128	160	8	3200	NA	0.8	300

1. Daniel Engels, Markku-Juhani O. Saarinen and Eric M. Smith. “The Hummingbird-2 Lightweight Authenticated Encryption Algorithm.” RFIDSec 2011
2. T. Good and M. Benaissa, “Hardware Results for Selected Stream Cipher Candidates,” eSTREAM http://www.ecrypt.eu.org/stream/papersdir/2007/023.pdf)
3. M. Agren, M. Hell, T. Johansson, and W. Meier, “A New Version of Grain-128 with Authentication.” SKEW 2011
4. Panu H¨am¨al¨ainen, Timo Alho,Marko H¨annik¨ainen, Timo D. H¨am¨al¨ainen, *Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core*, Ninth Euromicro Conference on Digital System Design: Architectures, Methods and Tools, IEEE Computer Society, 2006.

©2009-2010 Revere Security. All rights reserved.

Clocks Per Bit

Table 5. Clocks Per Bit.

Cipher	Block Size (bits)	Key Size (bits)	Clocks Per Bit
HB2	16	128	0.25
Grain-128	1	128	1
Trivium	1	128	1
Present-80	64	80	0.5
Present-128	64	128	0.5
Katan32	32	80	8
Katan48	48	80	5.31
Katan64	64	80	3.98
Iceberg	64	128	0.25
AES-128	128	128	1.25

Daniel Engels, Markku-Juhani O. Saarinen and Eric M. Smith.
“The Hummingbird-2 Lightweight Authenticated Encryption Algorithm.”
RFIDSec 2011

Revere Security

Clock Cycles to Encrypt

Table 6. Comparison of Clock Cycles to Encrypt. Note that most block ciphers require initialization every time key is changed.

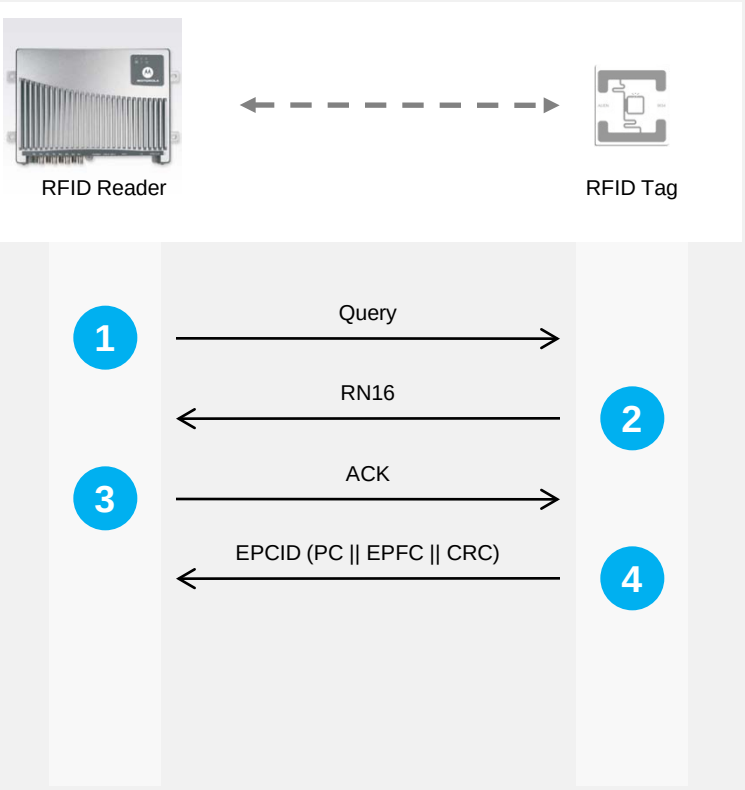
Cipher	Init	16 bits	32 bits	48 bits	64 bits	96 bits	128 bits
HB2	16	4	8	12	16	24	32
Grain-128	513	16	32	48	68	96	128
Trivium	1333	16	32	48	68	96	128
Present-80	0*	32	32	32	32	64	64
Present-128	0*	32	32	32	32	64	64
Katan32	0*	256	256	512	512	768	1024
Katan48	0*	255	255	255	510	510	765
Katan64	0*	255	255	255	255	510	510
Iceberg	0*	16	16	16	16	32	32
AES-128	0*	160	160	160	160	160	160

Daniel Engels, Markku-Juhani O. Saarinen and Eric M. Smith.
“The Hummingbird-2 Lightweight Authenticated Encryption Algorithm.”
RFIDSec 2011

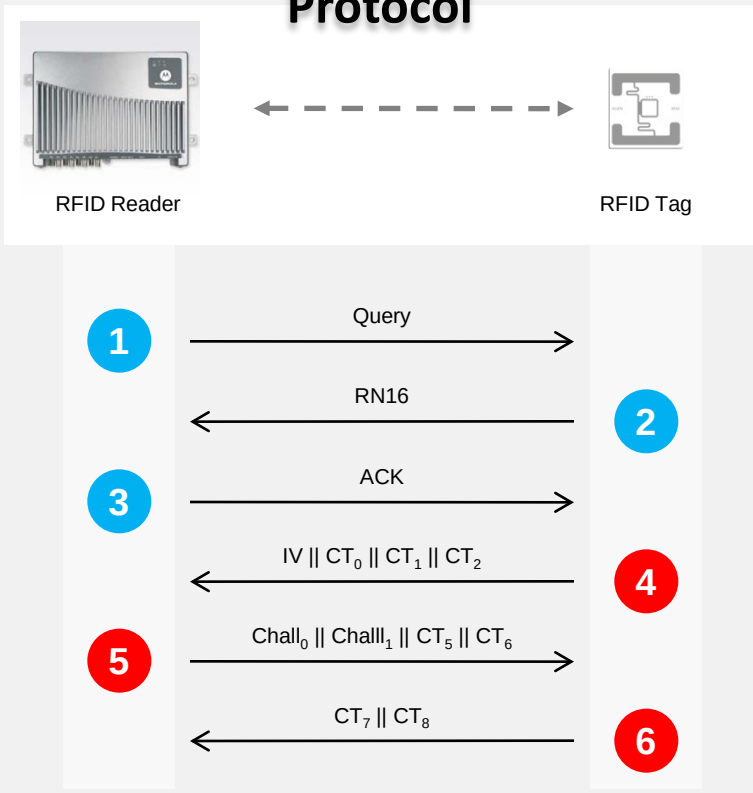
Revere SECURITY

Secure ID & Mutual Authentication

Standard EPC Gen 2 Protocol



Hummingbird Secure EPC Gen 2 Protocol



n **Secure Communication**

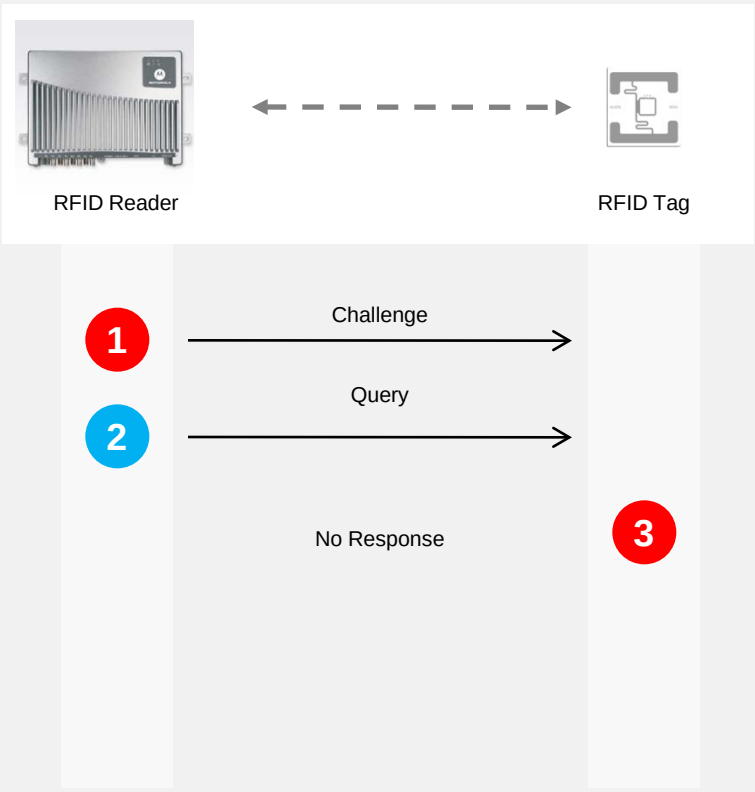
n **Unsecure Communication**

© 2009-2011 Revere Security. All rights reserved.

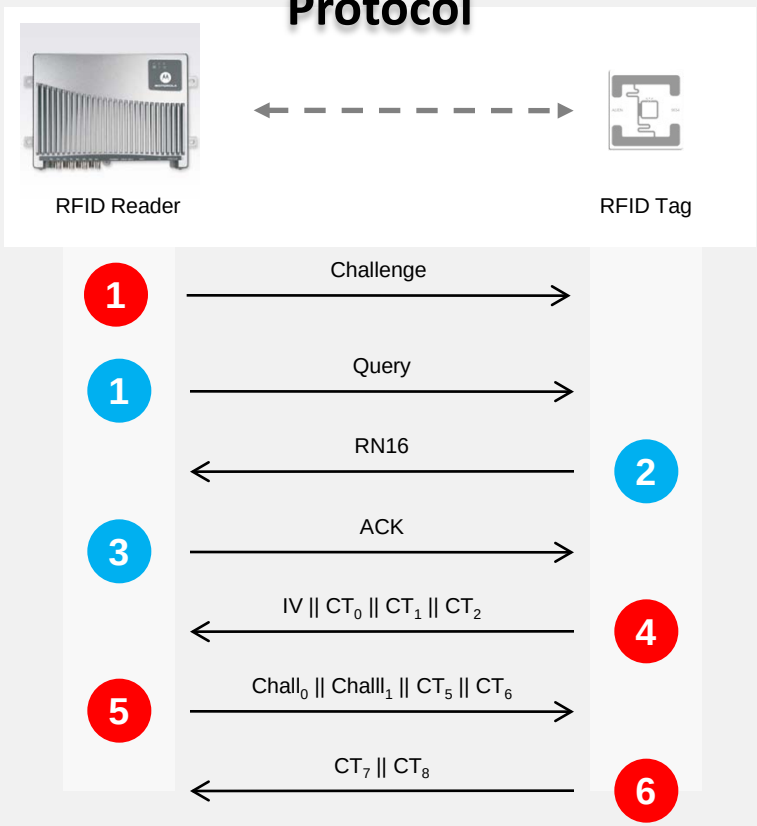
Revere SECURITY

Tag Cloaking, Secure ID & MA

Standard EPC Gen 2 Protocol



Hummingbird Secure EPC Gen 2 Protocol



n **Secure Communication**

n **Unsecure Communication**

© 2009-2011 Revere Security. All rights reserved.

Revere SECURITY

Summary

- The next wave of networked technology has already begun to be deployed (largely without security)
- Personal mobile devices pose new security threats
- Security must be designed into the communication protocols
- Wireless communications require cryptographic security
- Resource constraints require the use of new cryptographic ciphers such as HB2

© 2009-2011 Revere Security. All rights reserved.

Protecting your Privacy by Securing the Insecurable

www.reveresecurity.com