IQRF OS 4.0, security and some news

Vladimír Šulc, Ph.D.
MICRORISC s.r.o., CEO
Jičín, Czech Republic

IQRF® conference 2016
May 25, 2016, Prague

IQRF OS – few new features released 2015 / 2016

IQRF OS 3.06

IQRF OS + IQRF HWP (DPA) + IQRF IDE working together

Remote bonding support

FRC extensions: advanced, selective modes

LP support – bonding, discovery

IQRF OS – few new features released 2015 / 2016

IQRF OS 3.07

Extended support for TR-7xD modules

Extended control over built-in HW

FRC extensions: 2B, selective, indications

IQRF OS – few new features released 2015 / 2016

IQRF OS 3.08

Optimizations and minor bugs fixes

Support for 433 MHz and 915 MHz bands + -IL version

IQRF OS – few new features released 2015 / 2016

IQRF OS 4.00

Deep system optimizations

Complex security features

Redesigned packets structure

New bonding mechanisms

It is wireless. Everybody can listen and forge packets!

No physical protection.

Security concept should consider more threats.

Security – previous versions of IQRF

From the same begin we understood IT IS A MUST:

Consistency protection

Automatic encryption of network communication

Bonding security dependent on an application layer

COMPLEXITY

ADEQUACY

SIMPLICITY

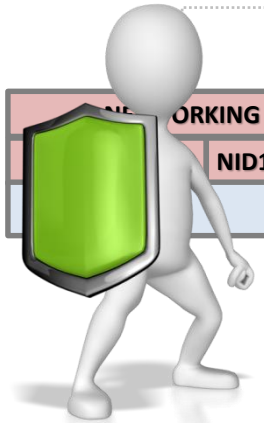
UNDERSTANDABILITY

PREDICTABILITY

Security concept – start at basic protection

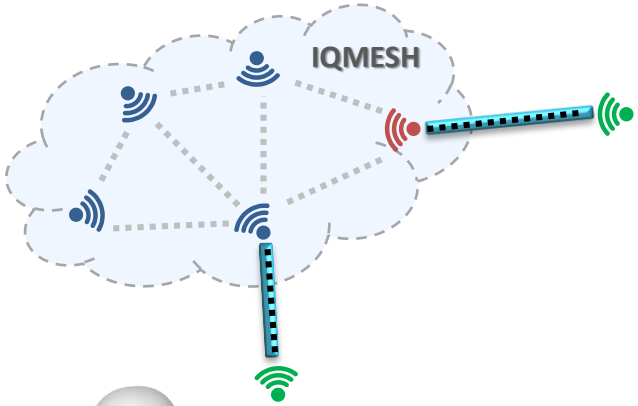
HEADER			[NETWORKING AND SYSTEM]		DATA			SYNC		CRC-16
PIN	DLEN	CSH	NETWORKING AND SYSTEM	CSN	DATA-whitened	CSD0	CSD1	SYNC	CSS	

PIN							
NTWF	ACKF	ROUTEF	CRYPTF	DPAF	SYSPF	AUXF0	AUXF1



ORKING			ROUTING						DPA			SYSTEM	A0	A1	ENCRYPTING					CSN
	NID1	PID	RTOTX	RTDEF	RTHOPS	RTSLOT	RTDID	RTAUX	PNUM	PCOM	PPAR	SCMD	---	---	ECFG	CNT0	CNT1	CNT2	CNT3	
[NETWORKING AND SYSTEM]																				

Security concept – JOINING THE NETWORK



WHY?

Bonding is a process during which devices exchange sensitive information (e.g. network passsword, addresses, …)

HOW?

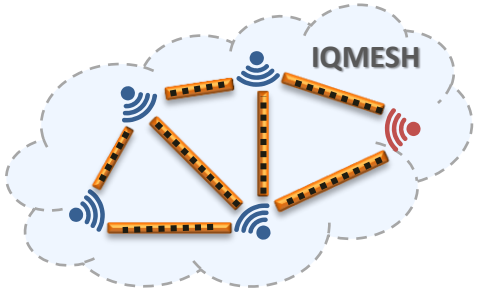
Bonding password (128 b)

Its knowledge entitles new device to join the network

Bonding keys + AES 128 b → **ENCRYPTION** → **BONDING DATA**

Packets consistency check

Security concept – NETWORK COMMUNICATION



WHY?

Network communication is continous process during which some sensitive data or commands may be transmitted.

HOW?

Network password (192 b)

Its knowledge entitles devices to decrypt and process packets

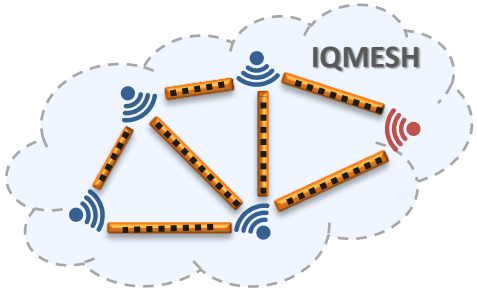
Network keys + AES 128 b → **ENCRYPTION** → **NETWORK PACKET**

+ Packets consistency check

+ Forged packets check / drop

+ Dynamic keys change

Security concept – user's encryption



WHY?

Users may use additional encryption shield for data. Thus, data not necessarily should be processed by the IQRF network.

HOW?

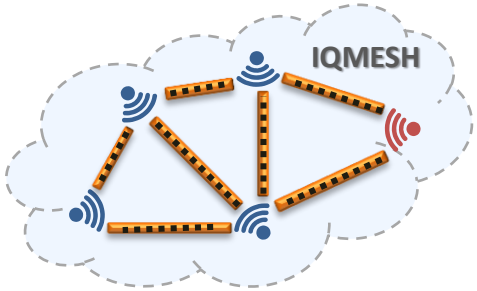
User's key (128 b)

Its knowledge entitles application to decrypt data

User's key + AES 128 b → **ENCRYPTION** → DATA

It enables data isolation from the IQRF platform.

Security concept – potential future problems



WHY?

In the future, new vulnarabilities (e.g. in AES) may be found and running system should be patched.

HOW?

Application upgrade: SPIPGM, RFPGM, IQMESH OTA

HWP upgrade: SPIPGM, RFPGM, IQMESH OTA

Secure IQRF OS upgrade: SPIPGM, RFPGM, IQMESH OTA

Security concept – simplicity and understandability

encryptBufferRF(x)

decryptBufferRF(x)

setUserKey()

setBondingPassword()

WHY?

If security is not understandable or brings technical difficulties users will *usually* will not use it.

HOW?

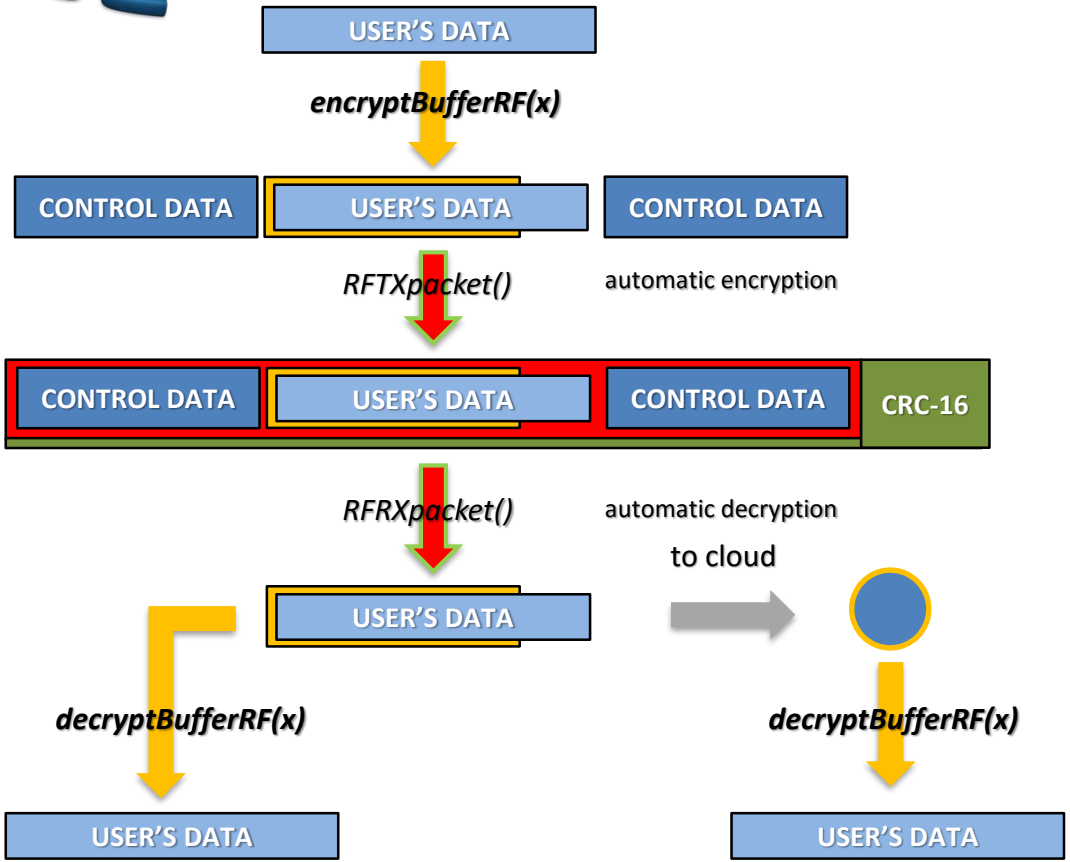
All discussed features related to network security are automatic.

Random Network password (192 b) is set during manufacturing.

Dynamic network keys exchange realized by the IQRF OS.

Easy to understand API.

Security concept – network communication



User's encryption AES 128 b CBC + user's key

network password 192 b

Network encryption AES 128 b + CDC + CP + network keys

Cipher Data Chaining + Consistency protection

network password 192 b

Network decryption AES 128 b + CDC + CP + network keys

Cipher Data Chaining + Consistency protection

User's decryption AES 128 b CBC + user's key

Security concept – features

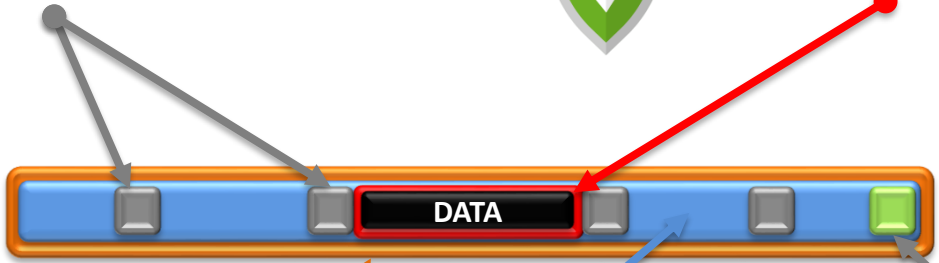
Keys + passwords management

SPIPGM
RFPGM
OTA

FUTURE PROTECTION

Block checksums

User's encryption shield



PACKET

CRC-16

Network encryption shield
Forged packets protection
Packet's consistency protection

Security concept – few security layers

Prevention is always better than elimination of the problem .