FORTECHO SOLUTIONS

Encoded versus Encrypted

In this white paper, we discuss the difference between encoded and encrypted communication, perceived shortcomings and how the two relate to an Active RFID monitoring system in practise.

+ In cryptography, encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can.

+ Fortecho Solutions / Wavetrend RFID Tags are only capable of data transmission; they have no data reception capability. Their operation is completely autonomous and cannot be altered by any external radio transmission. Therefore, given tag movement, there is no outside influence that can stop a tag generating “alarm” transmissions. Were the air interface to be properly encrypted the tags would need to be transceivers, the tag packet would be much longer and hence the battery life would be much shorter at fast heartbeat rates (30 second intervals). This would defeat the point of having long-life, regular supervision tags in the art market where tag swapping and battery changing is time-consuming and costly. The market has indicated to our reseller Fortecho Solutions that the less frequently clients have to change tags the better, yet they still want fast transmitting tags (30 seconds) in case the tag is physically compromised.

+ To be able to intercept a specific tag’s message, make sense of it and re-transmit something that looks like that tag’s message requires inside knowledge. This is what we have described by Encoded. A 3rd party does not have access exclusively to one known tag. Tags are spread geographically and transmit each 30 seconds. They transmit for only a few milliseconds on very low power and go silent again. There are typically hundreds of tags all doing the same, so pulling one tag’s messages out of the traffic is exceedingly difficult and the 3rd-party has no knowledge of where this tag is specifically located. Tags in motion send many messages per second. No one can predict when that same tag will transmit next time as the period is randomised.

+ Even if a message is encrypted it can be copied and resent. However the host software will reject such a message as it does not fit the flow of numbers expected from the tags. It will also reject an unencrypted message that does not fit the flow and copying a message does not stop the original tag from transmitting. So the system will always react to legitimate tag alarm states and will be alerted to the presence of an erroneous message and ignore it. Message traffic is exclusively from tag to reader so there is no possibility of passing updated keys and so any encryption would be static and easily defeated anyway.

+ Encrypted or not, no amount of expertise can cause the host software not to give an alarm if the original tag sends its motion messages. A 3rd-party CAN NOT stop that from happening without physical access to the tag. If someone wished to defeat the system there are more straight forward methods such as radio jamming, however the host software gives warnings when receivers are not receiving normal tag radio traffic. This also requires proximity to the tags and receivers and assumes that the 3rd-party has unchallenged access to the area.

+ An alarm condition is signalled by the presence of an alarm transmission, rather than the absence of a steady-state transmission. The protocol used does not have a concept of a transmission that can cancel an alarm transmission. There is therefore no external transmission that can override an alarm transmission.

+ There is no plain text in a tag message, there is no artwork or other confidential information in a tag message. The tag message only has meaning to the software because of the database it is attached to. There are only numbers that are encoded and these numbers are meaningless in isolation. Thus reading a message has no benefit to a third party in discovering anything of any value.

+ Given the above, there is no advantage to be gained if an individual were to try and sniff and reproduce a valid tag transmission. However, for completeness, if a potential attacker were to try to understand the tag-to-reader RF link, they would need extremely specialist tools and knowledge to:

    - Discover the specific type and variant of carrier modulation used.

    - Sniff and capture a packet, particularly given the milli-second level transmission duration.

    - Decode the packet into its constituent fields and understand their contents, particularly as up to 45% of the transmission from a tag changes on a transmission-by-transmission basis.

+ Having taken the time and trouble to understand tag packet construction the dynamic construction and injection of a tag packet serves no purpose as it

can't prevent or cancel an alarm state. Additionally, as an injected packet would unavoidably be a duplicate of a valid packet, injection would cause an alarm to be generated in the host software, solely serving to make the system user aware of an attempted attack without compromising the proper operation of the system.

- As per the specification of the RFID Artefact Protection System the following statements are true:

- The tags shall be capable of being uniquely identified to this project. Thus, they should have a unique code or site code with sufficient permutations for this (more than 10 million possible codes are expected).

- The Tags shall have the ability to be programmed with up to 2 billion unique IDs.

- No other person other than the original hardware manufacturer shall have the ability to produce tags that could be detected by the proposed system.

- The Tag to Receiver message structure is such as to prevent cloning of messages for the purpose of subversion. The software monitors the integrity of each message and discards anomalous or potentially cloned messages.

- The system reports any attempts to block or jam the radio transmissions between tag and receiver or the electrical communication signals between receiver and software.

In summary, we believe the only practical way to defeat the RFID subsystem would be to jam, however this would equally defeat an encrypted RF link and would cause a general alarm at an application level anyway.

We have never heard of a 3rd party ever cloning a Wavetrend tag message in over 17 years of RFID experience.

We fully understand why public systems that do send sensitive data on the carrier wave require encryption, and also why tag systems such as access control system also encrypt (as the card's presence opens doors).

We hope the above alleviates any concerns regarding the debate on encryption and encoding.