

# **ON TREE CREEPERS AND THEIR CONTROL**

*Contribution to the RFID Security debate by Peter Hawkes, BTG plc and Chris Turner, RFIP Solutions Ltd, London UK*

## **Introduction**

No, we have not given up on RFID and become ornithologists. "Tree Creepers" is our alternative name for "Silent Tree Walkers" a name coined by Juels, Rivest and Szydlo of RSA Laboratories (USA) and MIT's Laboratory for Computer Science (Cambridge USA). They describe the Tree Walking attack on RFID tag systems in a recent paper entitled "The Blocker Tag" posted on <http://www.rsasecurity.com>. In this article we consider Tree Walking (also known as binary tree search or tree splitting) in the context of the draft ISO/IEC 18000-6 Standard for UHF item tagging in open systems. We also show how alternative systems protect against attack.

## **Eavesdropping on RFID Tag Readers**

Silent Tree Walking or Creeping refers to a class of "bugging" device that might be deployed by criminals to attack RFID tag reading operations for gain or to disrupt a business (e-vandalism) using this device to discover RFID tag numbers. The Silent Tree Walking device acts by covertly monitoring the dialogue between the authorised Reader and tags present. The Juels paper is mainly about such security weaknesses in "open" systems that use Tree Walking (binary tree search or tree splitting) arbitration schemes. It also covers some possible solutions.

They use as an example, the strengths and weaknesses of the MIT Auto ID Center's "Kill" command in the current EPC Class 1 draft specification. "Kill" causes tags to be permanently deactivated as the tagged item goes through a

Retail Point of Sale (PoS) terminal when the item is sold to a retail customer. "Dead Tags don't Talk" so the item ID remains unknown to all including the owner and any eavesdropper.

Juels includes a lucid and scholarly review of some of the other possible future threats to consumer privacy if and when supermarkets and other retailers deploy RFID Tags on consumer items such as clothes. The "Blocker tag" of the paper's title is proposed as a key component of solutions to counter the perceived threat to individual anonymity in public places. The threat could possibly come about when the purchaser subsequently wears a garment with the tag still functional ("alive") and unauthorised persons or organisations covertly reading the unique ID (EPC™) number of the tagged item and associating it with the person who purchased it. They assume that the purchaser's personal details have been obtained by other means and linked to the garment ID.

One obvious way to attempt to discover the unique ID's of purchased items is by monitoring retail purchase transactions in the Retailer's Point of Sale terminal. Even if said terminal and network are secure from eavesdropping there is another weakness. The terminal is assumed to have a secondary and unauthorized reader hidden nearby that practices the "Silent Tree Walking" routine. This unobtrusive and hard to detect "bugging" device receives and decodes single or multi-bit command queries sent by the reader's transmitter to all tags in the sphere of influence of the adjacent authorised Reader.

In all passive RFID tag systems the Reader's transmitter sends out much stronger signals than the tags' response messages. Therefore, a "Tree Walking" listening receiver can collect all the queries put to a group of tags at long range and then by "tree searching", the owner of the bugging device can deduce the list of the tagged items purchased or of the tag ID's present, depending on the system design. However it would be difficult to screen readers to stop signals

reaching the "Silent Tree Walker" receiver because it would make the reader ineffective for some legitimate reading operations. Silent Reading of the ID of tags using protocols based on the "anonymous but distinguishable" principle discussed below is however almost impossible.

For economic reasons, RFID tagging of Retail items is still in the future; therefore, we think that Personal Data Privacy concerns are premature. However the security weaknesses and countermeasure scenarios in the Juels paper are very applicable to Corporate Data Security.

The threats to business operations from "non-paying wholesale" Customers otherwise known as organised criminals, may soon materialise.

### **Countermeasures**

It should be noted that Tree Walking breach of security is only possible with those tag singulation methods employing tree walking also known as "tree-splitting" or binary tree search. We describe later alternative singulation (anti-collision) methods, which are able to frustrate Silent Tree Walkers. At its simplest, tree walking is a binary search in which the reader "walks" from the trunk through the branches and twigs of a binary tree to the leaves. On each leaf is a unique tag number. Binary search is akin to roll calling or polling except that the queries relate to single or multi-bit fields. In polling, the Reader says: *"Answer only if you are the tag on the item number xxxxxxxx"*.

The MITAutoID Center, now superseded by EPC Global([www.epcglobalinc.org/](http://www.epcglobalinc.org/)), has proposed that the item number xxxxxxxx on tags be a string of binary bits, 64 or 96 bits in length and called the Electronic Product Code (EPC™). Binary tree search has been used in some "closed" RFID tag systems for at least the last ten years. The fact that the bugging device never transmits during tag reading means that the presence of one or more "Silent Tree Walkers" would be

almost impossible to detect. To nullify Silent Tree Walking attacks and as an alternative to the "Kill" option Juels proposes the use of a "Blocker Tag".

The Blocker Tag is an adapted or emulated passive tag that responds ambiguously to reader queries. Every response from single or multiple tags to these Reader queries is a "yes" and then a "no". Consequently, in a binary tree search the reader thinks that every "leaf" on the tree is populated with a tag number. As a result the search time for reading ID numbers from tags present tends to be very long and the inventory data obtained is valueless.

Juels points out that the Blocker Tag can, in the wrong hands, be used for malicious "denial of service" attacks on RFID tag systems. "Blocking" attacks would soon be detected. However, locating and removing portable or switchable Blocker tags could be difficult.

### **Eliminating the basic problem at source.**

We have experience over the last decade of developing low cost RFID tags, tag chips and readers for open systems use. Our key designs and those of other RFID suppliers have been embodied in Final Committee Draft ISO-IEC 18000 "Radio Frequency Identification (RFID) for Item Management" - Part 6: Parameters for Air Interface Communications at 860-930 MHz.

ISO/IEC 18000-6 compliant RFID tag designs including Supertag use a totally different method of managing contention between grouped tags and singulating them. This alternative method frustrates the use of "Tree Walkers" as eavesdroppers. It goes under various names. We call it "Time Slot" transponder identification. The Juels paper calls it the "ALOHA" protocol. Another descriptor is "Random Hold-off and Retry" arbitration.

Time slot singulation and reading of multiple tags is embodied in the Draft ISO/IEC 18000-6 Standard for UHF tag systems. It has the characteristic of separating tags for reading or writing in randomly distributed time intervals rather than in code space. A "Tree Walker" cannot deduce Item ID's from just listening to an ISO/IEC 18000-6 reader's transmissions, because when reading, the Reader does not transmit any part of the tag's identity while singulating and reading multiple tags in its vicinity.

From the Data Privacy point of view one can say that these singulation methods enable the tags to be "Anonymous but distinguishable".

### **Threats to Privacy – real or perceived?**

As far back as 1995, we suggested the use of Digital Signatures to allay the concerns about future misuse of tag stored data once RFID tag systems had been widely deployed in Retail and like applications. There were then and still are economic factors to be overcome and the Laws of Physics barriers to be circumvented. Bob Williams recently cited several of these barriers in "Product ID Magazine of PIRA" and concluded that Retail item tagging is still far from economic.

However, the lower price of today's disposable "Radio Labels" means that no such barriers exist to deployment of long read range RFID tag systems in other applications such as on bulk packs, cartons and reusable containers in the Retail Supply chain. Indeed RFID tags are currently being used to track and trace consignments in the Retail Supply Chain.

In our view, Users and their Suppliers need to build in security whenever an open system is being planned. The threats of today and tomorrow are from thieves wanting to access corporate data in order to help them steal goods in bulk before they ever reach the Retailer. Attention should therefore be given to

possible threats from eavesdropping for criminal gain. It is not our intention to educate the criminal fraternity in how to profit by disrupting the legitimate operation of RFID tag systems. However, it is obvious that the best designs should not rely on "security by obscurity". The correct choice of countermeasures to eavesdropping on tag reading should be given priority when designing a new RFID tagging system.

It might be supposed that encryption will easily stop all types of theft of goods. This is not the case. Once the would-be thief knows which type of goods are in particular tagged containers he can associate the consignment with whatever (fixed) ID code is carried in the container tags, then tracking and tracing becomes as easy for him as for the owners. Cloning an EPC™ numbered tag on a container helps the thief avoid early detention after he has obtained the goods he required by; for example high-jacking. Substitution of an empty box carrying the correct tag ID number will delay the discovery of the "diversion" of a consignment of valuable items.

### **Other Benefits of Time Slot Singulation**

There are other benefits to be gained from time slot singulation as used in ISO/IEC 18000-6, which are not available to users of Tree Walking protocols to effect singulation (Anti-contention). For example, the reduced activity by the Reader's transmitter means that more time is available to collect identities and data from tags.

When there is relative motion between a reader and a group of tags, late arriving tags still get read. The Tree splitting search methods assume the tree shape stays the same during the census of tags present in the reader's field. To allow for errors induced by late arriving tags some proprietary "Closed" RFID tag systems that use binary tree searching, actually poll through the list of tags

present after deducing the likely population resulting in unnecessarily extended transaction times.

Numerous RFID tag manufacturers across the world support the time slot approach. For UHF frequencies of operation they have contributed their patent rights to the draft Standard ISO-IEC 18000-6 Radio Frequency Identification (RFID) for Item Management - Part 6: Parameters for Air Interface Communications at 860-930 MHz.

### **Conclusions**

Firstly, Juels, Rivest and Szydlo's paper marks an important milestone in the evolution of RFID tag systems towards their use in ubiquitous computing.

Secondly, the case for using RFID tag systems compliant to ISO 18000-6 with the EPC™ numbering system should be considered if eavesdropping attacks are thought to be a likely threat. This applies now for the tagging of goods in transit to Retailers and similar non-retail applications.

Finally, we do not consider that there is any cure-all to the potential threats to RFID tag system security from criminals, terrorists and E-Vandals. More collaborative Research is needed such as that funded by the UK Home Office "Chipping of Goods" initiative.

### **Disclaimer**

The views expressed in the above note are the Authors own and not those of BTG plc or RFIP Solutions Ltd.