www.trakpointsolutions.com
12526 High Bluff Drive Suite 300 San Diego, CA 92130

TRAKPOINT SOLUTIONS TECHNICAL BRIEF - SECURITY

TrakPoint's two-way architecture employs the strongest and most secure processes available and is very similar to that used in 4G and 5G systems - known as the 3rd Generation Partnership Project 3GPP standard (3GPP). 3GPP is a global group of 7 core telecom giants across the world (also known as Organization Partners). The scope of 3GPP is to put down globally recognized specifications and standards for 3G,4G and 5G network deployments. The AKA protocol and procedures support powerful entity authentication, message integrity, and message confidentiality, among other security properties. The AKA protocol is a challenge-and-response authentication protocol based on a symmetric key shared between a tag and a secured cloud database. After the mutual authentication between a tag and the cloud authentication server process, cryptographic keying materials are derived to protect subsequent communication between a tag and the network, including both signaling messages and the plane data. More detail here: https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/10.03.00_60/ts_133401v100300p.pdf

The AKA method was developed to ensure the highest privacy, and security of communications and there have been no publicly known breaches of this approach except those based on getting physical or other access to highly controlled and singular secure databases in order to acquire secret keys (which has been, for example, been rumored to have been done by the US/UK security agencies in 2010 in order to get access to certain European cellular communications through a breach at root of trust security provider Gemalto (strongly denied by them of course): https://www.gemalto.com/press/pages/gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-sim-card-encryption-keys.aspx

Our architecture uses these known and proven best practices and puts the platform into the league of military grade approaches. We are not "cooking up our own security" approach.

For example, the architecture guards against major flaws of previous technologies including:

1. Attacks such as network spoofing by faked infrastructure –For example, a faked detection point can advertise spoofed network codes with a stronger signal strength to lure tags equipment away from its legitimate network elements causing the tag to register and engage with the faked network.
2. Lack of confidentiality in certain signaling messages, resulting in privacy violation–For example paging information, which if not encrypted, can be used to detect the presence of a particular tag.

------ A bit more detail on the AKA method as applied to TrakPoint's platform:

The AKA is triggered after the SECURE DATA BASE SERVERTAG completes the MAC LAYER procedure with detection point and sends an Attach message to the MME. The MME sends an Authentication request, including TAG identity (i.e., IMSI) and the serving network identifier, to the SECURE DATA BASE SERVER located in the home network. The SECURE DATA BASE SERVER performs cryptographic operations based on the shared secret key, Ki (shared with the TAG), to derive one or more authentication vectors (AVs), which are sent back to the MME in an

Authentication Response message. An AV consists of an authentication (AUTH) token and an expected authentication response (XAUTH) token, among other data.

After receiving an Authentication Response message from the SECURE DATA BASE SERVER, the cloud sends an Authentication request to the TAG, including the AUTH token. The TAG validates the AUTH token by comparing it to a generated token based on Ki. If the validation succeeds, the TAG considers the network to be legitimate and sends an Authentication Response message back to the cloud, including a response (RES) token, which is also generated based on Ki.

The cloud compares the RES token with an expected response (XRES) token. If they are equal, the cloud performs key derivation and sends a Security Mode Command message to the TAG, which then derives the corresponding keys for protecting subsequent CONTROL signaling messages. The cloud will also send the detection point a key from which the keys for protecting the MAC LAYER channel are derived. After the TAG also derives the corresponding keys, subsequent communication between the TAG and the detection point is then protected.

TrakPoint Solutions, Inc. located in San Diego, CA is a technology company offering a hardware-supported, cloud-based, B2B SaaS service to indoor facilities for electric tracking of critical assets. TrakPoint eliminates the need to rely on the customer's WIFI or network infrastructure by utilizing an independent IoT network with cellular backhaul. This advanced technology is the only solution designed to provide economic, reliable indoor asset tracking with guaranteed accuracy and performance. For more information on TrakPoint Solutions or InsideTrak, please go to www.trakpointsolutions.com or call 1-888-650-TRAK.