APPLICATION OF MERKELIZED ABSTRACT SYNTAX TREES TO THE INTERNET OF THINGS LOCATION-BASED CYBERSECURITY SOLUTIONS

Kazimieras Bagdonas, Algimantas Venčkauskas

Computer Department, Kaunas University of Technology, Studentų 50-415, Kaunas, Lithuania

Introduction

We present a novel method for geolocation data integration into a multimodal Internet of Things (IoT) security solution using Merkelized Abstract Syntax Trees (MAST). The proposed method has been developed for the IoT devices operating in the IoT Fog, communicating with the Edge devices. The proposed method allows the exploitation of the IoT Networks Node's (NN) localization solution for data source authentication and data validation.

Localization solutions can be obtained via external systems (e.g. GNSS) or can be derived from IoT localization techniques. The least significant bits of the localization solution are masked to provide the desired geographical Zone of Validity (ZoV). The amount of masked bits defines the size of the ZoV. No other information except the number of masked bits needs to be communicated from the Edge node to the NN.

In cases where improved security is required, additional parameters, such as IDs and location data of neighboring IoT NNs, can be incorporated into the extended MAST structure to enhance security. This information must be present in the Edge nodes in order to validate the signature solution. A proposed novel approach to coordinate verification allows the transmission of hashed values without the need to reveal either the information on the ZoV by the Edge node or the exact coordinates by the NN.

Method

A single-mode identification and authentication method are susceptible to spoofing and thus pose a risk to security and data integrity. The ability to use a multimodal method for object identification and authentication can mitigate these risks. In the case of IoT, where the number of devices is expected to be in orders of billions, manual verification would be practically impossible, thus dramatically reducing the reliability other deployed systems. Further, more specific devices can be expected to perform their functions in specific geographical locations. This data verification can be compromised by the relocation of said devices outside the expected area of operations.

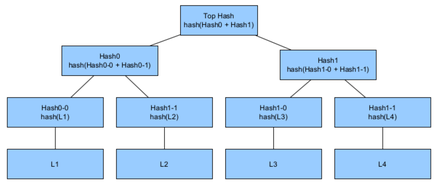

Figure 1: Merkel Tree Structure

In this poster, we present a novel MAST-based multimodal identification and authentication method for IoT devices. It integrates localization-based identification and authentication in a predefined geographical zone with additional parameters.

Geolocation information can be expressed in numerous global and local coordinate standards, such as Latitude and Longitude, Earth-centered, Earth-fixed, UTM, UPS, local tangent plane, etc. For the purpose of this work, we shall consider geolocation information to be expressed in the latitude and longitude as integer numbers, with the highest bits designated for degrees, subsequent value referring to the minute, then, the second, and, lastly arc seconds. A Merkelized Abstract Syntax Tree (MAST) is a combination of Merkel trees, as shown in Figure 1, and Abstract Syntax Trees introduce into the Bitcoin system with the Taproot upgrade.

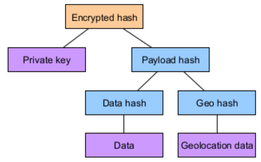

Figure 2: MMIA1: The proposed Merkel Tree structure

The combination of Schnorr signatures and MAST enables MuSig signature aggregation and *m–of–n* signing. This feature is thus proposed to be employed in a Multimodal Cybersecurity Solution integrating the Localization data for IoT nodes and the validity of its transited data verification and authentication. We propose the creation of a geographical Zone of Validity (ZoV). ZoVs are defined by the coordinates of the center of the square. Its dimension is defined by masking the n amount of the least significant bits in its coordinates. The more of the bits are masked, the greater the area is defined. This ZoV definition is managed by the IoT Edge nodes that perform the validation of IoT Network Nodes (NN). Only the number of masked bits is communicated to the NNs at the beginning of the communication session. Thereafter NNs are masking their localization solution coordinates accordingly, before hashing them into a multimodal security solution. We are proposing two MAST structures.

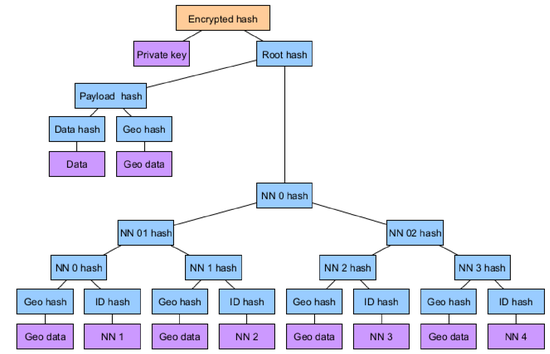

Figure 2: MMIA2: The proposed Merkel Tree structure

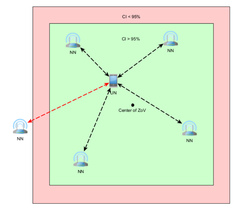

Figure 3: Zone of Validity (ZoV)

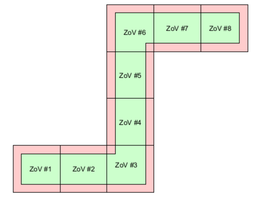

Figure 4: Valid Geographical Area (VGA) representation between bordering confidence intervals

MMIA1 shown in Figure 2 is computationally less demanding as it requires only 4 SHA-256 hashing operations. The MMIA2 expands on the concept and integrates the IDs and geolocation data of the neighboring IoT NNs, that were employed in the gathering of the ranging measurements to obtain the localization solution over the communication channel. The amount of SHA-256 hashing operations in MMIA2 depends on the number of neighboring IoT NNs which form a binary sub-tree in the MMIA MAST structure.

We assume the accuracy of the localization solution to be normally distributed. Within the ZoV the area that falls within the 95% Confidence Interval (CI) constraints is proportional to the dimensions of the ZoV and the σ of the localization solution. *Figure 3* shows the relation between the area of the ZoV that falls within the CI and the σ /size of ZoV when the σ varies between 0m representing the ideal case, and up to 1.4m, with an increment of 0.2m. Numerous ZoV can be defined in the system.

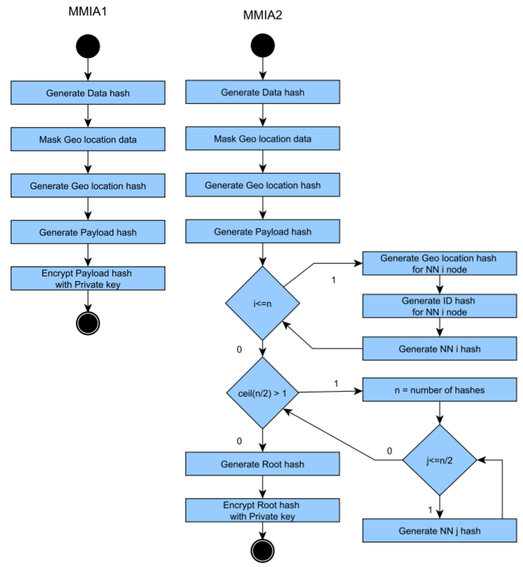

Figure 5: Algorithms for generation of MMIA1 and MMIA2

Results

For any two ZoV that are adjacent, the CI on the border that touch overlap, thus even if the localization solution falls outside the first ZoV, it lands in the second ZoV. By combining numerous ZoV the system can obtain a more precise representation of the VGA (Valid Geographical Area). *Figure 4* illustrates VGA defined by 8 ZoV, where the green zone falls within the 95% CI. The number of ZoVs influences neither the computational burden nor increases the data bandwidth requirements for the UN. For the Edge unit, the computational burden is increased only during the initial computation when the VGA is defined and the MAST tree is computed.

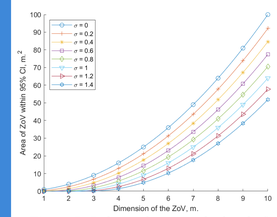

Figure 5: Relation between the level of noise and the size 95% CI area within the ZoV

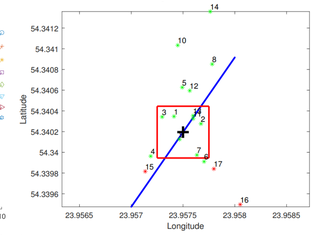

Figure 6: Simulated scenario of a UN traversing the ZoV

The proposed method has been simulated in a MATLAB environment. The ability to identify and authenticate the UN in both MMIA1 and MMIA2 modes has been validated. Figure 5 represents varying levels of noise in the localization solution and its relation to the area of 95% CI. Figure 6 presents the linear path the UN has traversed the ZoV. Table 1 summarizes the compute time experimental results of running the SHA hashing algorithm on an ESP8266 microcontroller with a different number of bits.

Table 1: Duration of the SHA-256 computation ESP8266 uController

SHA-256 Length	16	32	64	128	256	512	1024
Average compute time, us	40.6	41.3	80.6	122.1	204.6	370.4	701.1
Time SDTDEV, us	2.7	2.8	2.0	3.0	3.8	4.5	5.6

Conclusions

The proposed MMIA methods integrate encryption with an asymmetric cryptographic key and UNs localization information. Identification via the combination of a digital signature and the location data synergizes into a more robust security solution. The size of the ZoV can be defined by the number of masked the least significant bits. The masking of the coordinates ensures that the output of the SHA256 hash function is identical within that ZoV. The 95% CI areas are automatically connected for bordering ZoVs thus an irregular shape GaV can be defined without the need to overlap the ZoVs. Neither computational nor data bandwidth burden increases for the UN irrespective of the number of ZoVs, and for the Edge node.