June 26, 2019

Securing IAB SupplyChain objects

Gang Wang

Haskell Garon

Securing IAB SupplyChain objects

ABSTRACT

An online advertising marketplace comprises buyers and sellers, each with their intermediaries. A transaction is documented by a SupplyChain object, which includes a set of entities involved in the transaction. As presently drafted, the Interactive Advertising Bureau (IAB) standard that specifies the SupplyChain object is susceptible to tampering. For example, an entry in the SupplyChain object can be changed to falsely imply the involvement of a reputed player. Conversely, an item in the SupplyChain object can be changed to excise the involvement of other intermediaries. Per the techniques of this disclosure, a market player or intermediary in a transaction digitally signs their entry in the SupplyChain object. The SupplyChain object is thereby authenticated, intermediaries in a transaction are verified as genuine, and parties to a transaction enjoy higher levels of trust.

KEYWORDS

- Online advertising
- Supply-side platform (SSP)
- Demand-side platform (DSP)
- Real-time bidding
- Ad fraud

BACKGROUND

An online advertising marketplace comprises buyers and sellers, each with their intermediaries. In the OpenRTB real-time bidding standard [1] of the Interactive Advertising Bureau (IAB), a transaction is documented by a SupplyChain object, which includes a set of entities involved in the transaction. The SupplyChain object enables buyers to see everyone involved with offering a bid request for sale, from publisher to demand-side platform (DSP). An entry within the SupplyChain object includes an advertising system identifier (ASI) and the seller/reseller account identity of the associated entity.

The SupplyChain object enables transparency in the SupplyChain, thereby reducing ad fraud. However, the SupplyChain object is susceptible to tampering. For example, a malicious supply-side platform (SSP) can change an entry in the SupplyChain object to falsely imply the involvement of a reputed player. By doing so, buyers can get the false notion that the reputed player participated as a seller, thereby falsely making the ad impressions appear trustworthy. Conversely, a malicious SSP can change an entry in the SupplyChain object to excise the involvement of intermediaries legitimately involved in the supply of inventory. The malicious SSP can misrepresent to buyers that it has received a direct request from the publisher, that it is not a reseller, and that the associated inventory is only available from the malicious SSP.

Per the open real-time bidding (OpenRTB) standard, an entry of the SupplyChain object comprises two or more fields, some of which are described in the table below.

Name	**Description**
asi	Advertising System Identifier. The canonical domain name of the SSP, exchange, header, wrapper, etc. that bidders connect to. This may be an operational domain, if different from the parent corporate domain, such that WHOIS and reverse IP lookups can establish clear ownership. This can be set to the value used to identify sellers in an ads.txt file, if one exists.
pid	The identifier associated with the seller or reseller account within the advertising marketplace. This comprises the value used in transactions, e.g., OpenRTB bid requests, in the field specified by the SSP/exchange. Typically, in OpenRTB, this is the publisher ID. For OpenDirect it is typically the organization ID of the publisher.

Table 1: Certain fields of the SupplyChain object, per OpenRTB and other standards

DESCRIPTION

Per techniques of this disclosure, one or more fields are appended to each entry of the SupplyChain object to cryptographically protect the object from tampering or falsification. These additional fields are indicated in Table 2.

Name	Description
next_asi	The current node, which represents an intermediary in the supply chain, sets this field to the next intermediary (node) within the supply chain, e.g., the node to which the current node sends the ad request.
digital_signature	The digital signature of the current node.
previous_asi	The current node, which represents an intermediary in the supply chain, sets this field to the previous intermediary (node) within the supply chain, e.g., the node from which the current node received the ad request.

Table 2: Additional fields of the SupplyChain object, serving to secure the SupplyChain object

The *digital_signature* field enables each entity involved in a transaction to sign its entry in the SupplyChain object, thereby improving the integrity of the SupplyChain object. The *next_asi* and *previous_asi* fields in an entry of the SupplyChain object point respectively to the next and the previous entities of the transaction. Adding the *next_asi* and the *previous_asi* fields transforms the set of entities in the SupplyChain object into a singly or doubly linked list, further improving the integrity of the SupplyChain object. The *digital_signature* is the signature of a node of the linked list, generated by the intermediary represented by the node, and appended to the end of the linked list.

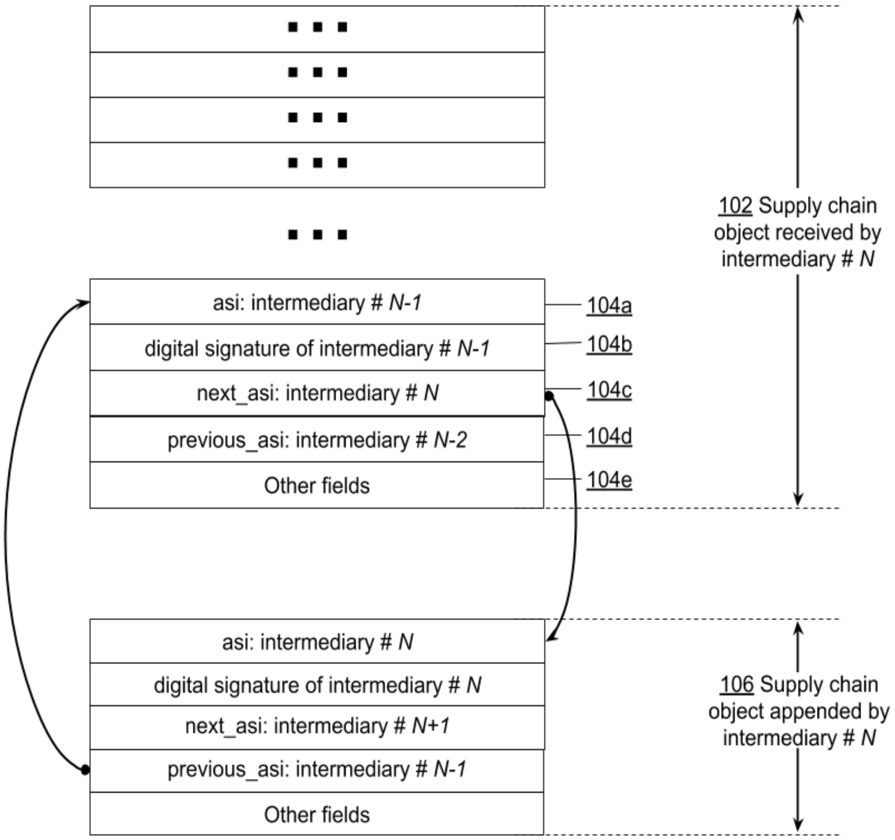
▪ ▪ ▪
▪ ▪ ▪
▪ ▪ ▪
▪ ▪ ▪
▪ ▪ ▪
asi: intermediary # N-1
digital signature of intermediary # N-1
next_asi: intermediary # N
previous_asi: intermediary # N-2
Other fields
104a
104b
104c
104d
104e
102 Supply chain object received by intermediary # N
asi: intermediary # N
digital signature of intermediary # N
next_asi: intermediary # N+1
previous_asi: intermediary # N-1
Other fields
106 Supply chain object appended by intermediary # N

Fig. 1: Formation of SupplyChain object by different intermediaries

Fig. 1 illustrates the coordinated formation of a SupplyChain object by different intermediaries in the SupplyChain. A SupplyChain object (102) is received by an intermediary *N*. Per the techniques, the SupplyChain object includes a linked list, a node of which includes the *asi*-field of the intermediary (104a), the digital signature of the intermediary (104b), a pointer to the next intermediary (104c), a pointer to the previous intermediary (104d), and other fields (104e). The receiving intermediary, identified by its *asi*-field (*N*), creates a node of the SupplyChain object (106) with similar fields, populates the fields appropriately, and appends it to the received SupplyChain object. A proper chain of trust is thus formed by an intermediary creating an entry of the SupplyChain object and appending it to the end of the linked-list of the SupplyChain object.

An intermediary digitally signs its appended SupplyChain object as follows. All fields of the to-be-appended SupplyChain object are populated. In particular, the digital signature field is set to the value of the digital signature field of the previous node in the supply chain. If such a node doesn't exist, then the digital signature field is set to null. The digital signature of the to-be-appended SupplyChain object is calculated using the private key of the intermediary. The digital signature field of the to-be-appended SupplyChain object is updated with the just-calculated digital signature.

Verifying the chain of trust: overall integrity of the SupplyChain object

A recipient of a SupplyChain object can verify the overall integrity of the SupplyChain object as follows. Starting with the first node in the SupplyChain object, the recipient walks down the chain, comparing the *next_asi* field of a node with the *asi*-field of the next node. If the two fields don't match, the supply chain has a gap; it is incomplete. Similarly, starting with the last node in the SupplyChain object, the recipient walks up the chain, comparing the *previous_asi* field of a node with the *asi*-field of the previous node. If the two fields don't match, the supply chain has a gap.

Verifying the chain of trust: integrity of each node

To verify the integrity of a node in the supply chain, e.g., whether a node has been modified during transmission, the recipient downloads the public key of the canonical domain included in the *asi*-field of the node. Such a public key can be obtained from a well-known URL in the domain, e.g., of the form intermediary_N.com/.well_known/public_key.txt. The recipient verifies the digital signature using the example pseudo-code illustrated in Fig. 2.

```
for each node in the SupplyChain object:
      set copy_of_node = node
      if previous_node exists:
         set copy_of_node.digital_signature = previous_node.digital_signature
      else
         clear field copy_of_node.digital_signature
      verify digital signature of copy_of_node using the public key
      downloaded from node.asi and node.digital_signature
```

Fig. 2: Pseudo-code to verify a node of the supply chain

Attesting the beginning of the chain

A malicious SSP may supplant a received supply chain with a new, false SupplyChain object and claim itself to be the beginning of the supply chain. To guard against this possibility, a publicly verifiable attestation specifies the beginning of the chain as follows. When an ad request is generated, e.g., by an app or browser, the operating system of the device generates an ad request attestation token, one of the parameters of the token being the canonical domain name of the entity to which the request is being sent. The *asi*-field of the first node of the SupplyChain object is set to that canonical domain name. To verify the beginning of the chain, intermediaries compare the *asi*-field of the first node of the received SupplyChain object with that of the ad request attestation token.

Reducing the size of the SupplyChain object during transmission

For well-formed SupplyChain objects, the value of the *asi*-field of one node is the same as the value of the *next_asi* field of the previous node, and the *previous_asi* field of the next node. The size of SupplyChain object can be reduced for the purposes of bandwidth optimization without sacrificing tamper-resistance, as follows. The *next_asi* value of the previous node can be omitted during transmission if it is equal to the value of the *asi*-field of the current node. Similarly, the *previous_asi* field of the current node can be omitted if it is the same as the *asi*-

field of the previous node. During verification, if the *next_asi* field of a node that is not the last node in a supply chain is missing, the *next_asi* value of the node is assumed to be the same as the value of the *asi*-field of the next node in the supply chain. Similarly, if the *previous_asi* field of a node that is not the first node in a supply chain is missing, the *previous_asi* value of the node is assumed to be the same as the *asi*-field of the previous node in the supply chain.

Client-side header bidding or mediation

Most communications between adjacent entities in the advertising marketplace are of server-to-server type, e.g., RTB calls over OpenRTB or other standards. However, some communication can be between server and client, e.g., browser. If an intermediary transmits a snippet comprising a SupplyChain object to a client browser, it may not receive feedback on how the snippet behaves when rendered in the browser. An intermediary in communication with a client can append a new node to the SupplyChain object and set the *next_asi* field of the appended node to client. In such a remnant line item, or similar, scenario, the snippet calls one server, e.g., the (*N+1*)st intermediary, with the SupplyChain object received by the *N*th intermediary as parameter. The (*N+1*)st intermediary appends a new node using previously described techniques. An example of the fully constructed SupplyChain object is illustrated in Fig. 3.

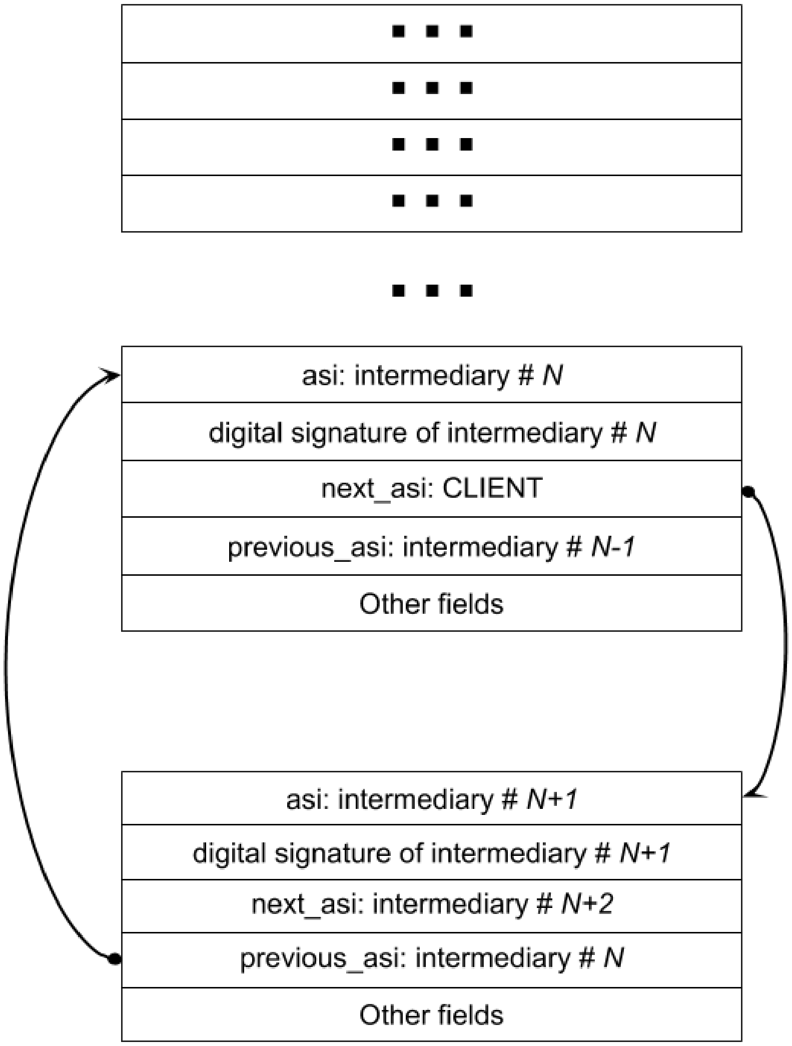
■ ■ ■
■ ■ ■
■ ■ ■
■ ■ ■
■ ■ ■
asi: intermediary # *N*
digital signature of intermediary # *N*
next_asi: CLIENT
previous_asi: intermediary # *N-1*
Other fields
asi: intermediary # *N+1*
digital signature of intermediary # *N+1*
next_asi: intermediary # *N+2*
previous_asi: intermediary # *N*
Other fields

Fig. 3: Example SupplyChain object under client-server communications

CONCLUSION

Per techniques of this disclosure, a market player in an online advertising marketplace governed, e.g., by IAB’s open real-time bidding standard, digitally signs its entry in the SupplyChain object that documents a transaction. The SupplyChain object is thereby authenticated, intermediaries in a transaction are verified as genuine, and parties to a transaction enjoy higher levels of trust.

REFERENCES

1. Interactive Advertising Bureau, “Real time bidding (RTB) project OpenRTB API specification version 2.5” https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf accessed Jun. 21, 2019
2. OpenRTB SupplyChain object https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/supplychainobject.md accessed Jun. 21, 2019.