Poster: Secure and Scalable Identity Management for the Aviation Industry

Panagiotis Kintis*, Athanasios Kountouras*, Nikolaos Pitropakis*, David Dagon*,
Manos Antonakakis*, Chris Markou †, Pascal Buchner †
*Georgia Institute of Technology,{kintis, kountouras, pitropakis, manos}@gatech.edu, dagon@sudo.sh
†International Air Transport Association, {markouc, buchnerp}@iata.org

***Abstract*—One of the most pressing problems that the aviation industry currently faces is the *integrity validation* of its information as it becomes digitalized. Airlines, maintenance facilities and boarder security entities need to "sign off" the airplane, the equipment and parts that are traded or sold among airlines and other industry stakeholders. The aviation industry's current proposed architecture for secure identity management solutions (internally known as Spec42) contemplated a highly centralized authority (i.e., one master certification authority). However, such an architecture has proven to be extremely hard to implement, especially across an industry with more that 700 airlines, 1,800 maintenance facilities, dozens of countries, and many thousands of personnel. Besides the risk of a single point of failure, diverse regulations and geopolitical conditions make highly centralized solutions unlikely to be successful.**

The aviation industry requires an identity framework that scales, is reliable, and respects the cross-organizational policies and adheres to various international regulations. We are at a unique moment in the history of aviation to ensure that secure digital identity is "built-in by design", and not merely a vendor add-on optional feature. This poster discusses that possibility by introducing a highly decentralized Aviation-Related Digital Identity Validation (ARDIV) framework. This framework enables reliable electronic entity validation using properties of secure DNS protocols.

I. Introduction

As with every other major industry sector, the aviation industry is in the process of adapting digital identities for essential equipment, facilities and personnel. One of the primary goals behind this effort is to "**digitally sign off an airplane**" and to validate the digital signatures of software installed in aviation hardware. Validating digital identities in aviation is essential for asset tracking, auditing, and proving the integrity of systems. The aviation industry has great interest in cost-effective alternatives to traditional, expensive and non-security aware asset management solutions.

The aviation industry is in need of an identity management solution that avoids highly centralized authorities or traditional certification authority (CA) centric models. An ideal system would avoid the broad attack surface found in centralized CAs, and reflect the diversity of international regulations, geopolitical trust and various policies in the aviation industry.

This poster proposes a new Aviation-Related Digital Identity Validation (ARDIV) framework. ARDIV is a simple, scalable and secure solution to the problem of identity validation in the aviation industry, leveraging tools and technologies already proved to scale in the Domain Name System (DNS). While DNS is widely perceived to simply provide a mapping between hosts and addresses, it has the capability to include validation, certificates, and identity management, through various protocol extensions. DNS, and its validating protocol known as DNSSEC [7], [6], [1], [2], lets one audit the integrity and validity of *any* data store. DNSSEC is therefore useful for code validation, inventory management, phone "rolodex" applications, and other scenarios where a strong identity framework is required.

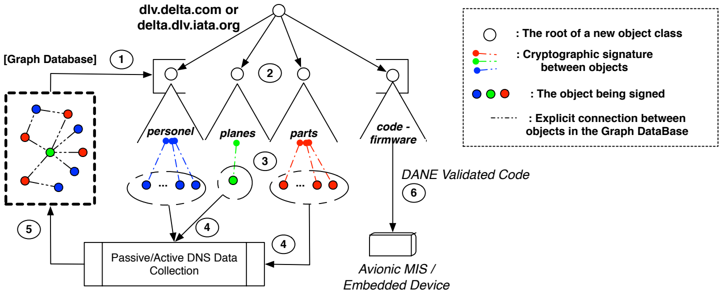
dlv.delta.com or
delta.dlv.iata.org
[Graph Database]
1
2
3
4
4
5
6
personel
planes
parts
code - firmware
...
...
DANE Validated Code
Passive/Active DNS Data Collection
Avionic MIS / Embedded Device
○ : The root of a new object class
: Cryptographic signature between objects
● ● ● : The object being signed
: Explicit connection between objects in the Graph DataBase

Fig. 1. A sample ARDIV-zone.

II. Proposed Solution

Our first consideration is to treat each major entity in the aviation industry (i.e., Airline, Manufacture, Maintenance, etc.) as an `island of trust`. This island of trust could be, for example, a sub-zone under a publicly available domain name (i.e., `dlv.delta.com` or `delta.dlv.iata.org` for Delta). Such a sub-zone would have explicit cryptographic properties. That is, the root zone operator is able to cryptographically sign any object that we want to track as part of the island of trust. These objects could be personnel, parts or even composite systems such as entire planes. Such zones archive and sign relationships between objects, such as those recorded by aviation maintenance task cards, Authorized Release Certifications and other related entities.

Since these objects are cryptographically signed by the parent zone (i.e., `dlv.delta.com` for Delta), all regulations and policies observed by that organization can be expressed in child delegations. Using the DNS-based Authentication of Named Entities (DANE [5], [4]), one can construct any desired combination of equipment, validations, and personnel interactions. Using DNSSEC Lookaside Validation (DLV) [3], [8] one can then test whether that given configuration, expressed as a DNS tree, would be validated by a different airline, organization, or policy regime.

The first component of the ARDIV framework provides integrity checks around tracked objects. In other words, an operator can create relationships between entities, and express them as labels in a DNS tree (a.k.a. DNS zone). The second component of the ARDIV framework provides off-line storage and analysis capabilities. This is done by utilizing established techniques from the DNS data collection and analysis research (i.e., passive and active DNS replication and analysis). The third component of the ARDIV framework provides new capabilities to Cyber Physical Systems (CPS) in aviation that can enable secure code update and recovery. Next we provide some technical details for all these components of the ARDIV framework.

a) Secure Identity Checking: DNS expresses hierarchical relations as well as individual entity attributes in the form of a tree. Typical resources in DNS are host and IP mappings, but they may be *any* arbitrary record, such as keys, inventory items, rolodex information, URLs and other data. These records are logged passively and analyzed.

Figure 1 shows a sample ARDIV assembled zone. We start with a graph database representation of parts (Step 1, Figure 1), planes, and actors in some existing datastore. This assembled hierarchy is then mapped to a DNS zone, to capture current state of an entity. The hierarchical tree would have several logical subzones (Step 2, Figure 1), to capture both the element and its state. For example, a plane (Step 3, Figure 1) may be represented as a high-splay tree, with child zones covering specific parts and maintenance status, along with any associated certificates.

By expressing an aviation asset in a zone format, we capture all the associated certificates and points-of-proof as individual DANE records. We can then test arbitrary assertions about the validity of the tree against various scenarios. Using DNS Look-Aside Validation (DLV), we can test the same tree against any desired policy filter, or regulatory regime.

b) Data Store and Mining: As secure identity checks using DNSSEC are being performed, we can collect (Steps 4, Figure 1) and store (Step 5, Figure 1) the resolution behavior in a graph-based database to enable historic analysis and forecasting. More specifically, we can perform forensic analyses, detect or predict faults or fraudulent behavior, and explore temporal properties using tensor decomposition.

Since ARDIV zones are represented as trees they can trivially be stored and represented as graphs. ARDIV zones are merged when their child labels share something in common, e.g., planes sharing personnel, planes that contain the same parts, or planes passing through the same airport. This relationship is denoted by drawing an edge between related objects. In addition to long-term storage, this also enables natural queries for manual forensic analysis. For example, if a part i fails in plane j, a simple query can identify all other planes that contain part i for potential failures. Further exploration could identify root causes for failure, such as environmental problems afflicting a particular airport.

c) DNSSEC-based Secure Code Updates: An additional important problem in aviation (as in any CPS systems) is the software update and recovery. In older generations of CPS that rely on EEPROM firmware images, one needs physical access to the device to modify the code running on the CPS device, and this presents a challenge to both attackers and those managing the CPS system. On the other hand, newer generation CPS systems usually provide some LAN or serial-based update frameworks; for example some newer CPS hardware permit flexible management of IP parameters via BOOTP or DHCP, and image fetching via TFTP, serial and modem protocols. Such new capability on CPS systems brings both convenience and speed in the update/recovery process, as well as serious security threat of malicious modifications to the software running on the device.

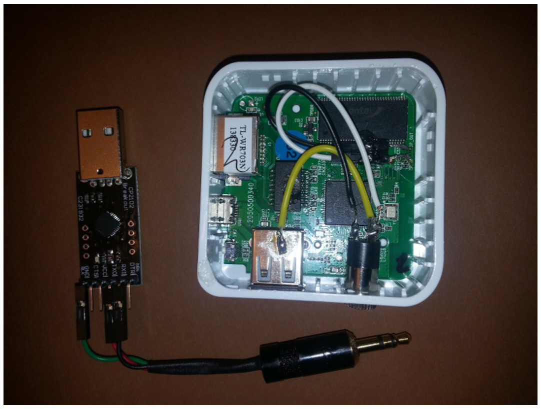

Fig. 2. Modified CPS devices for serial line recovery of uboot development

In order to deliver a new secure CPS update and recovery capability, ARDIV, creates a new code validating resolution process (Step 6, Figure 1). This new process uses a DNSSEC-based code validation logic, and employs modified local boot code to validate signed firmware images. While this is a novel use of the protocol, DNSSEC is a good fit for this problem. Signed DNSSEC records can be up to 64K in size, and just a few records in series can capture an entire firmware image. Further, DNSSEC is highly secure, and with protocols like DANE extend DNSSEC to do more than just IP address resolution. To pilot this recovery capability, we have modified some devices to include recovery serial ports, such as that shown in Figure 2.

III. Conclusion

The aviation industry is at a turning point, and requires secure protocols for electronic record keeping. One of the primary goals behind this effort is to "**digitally sign off an airplane**"and to validate the digital signatures of software installed in aviation hardware. This poster discusses ARDIV, a new Aviation-Related Digital Identity Validation (ARDIV) framework. This framework, allows the secure record keeping of electronic documents among aviation related organization with minimum level of pre-established trust.

References

[1] D. Eastlake 3rd. Dns request and transaction signatures (SIG(0)s). http://tools.ietf.org/html/rfc2931, September 2000.

[2] D. Eastlake 3rd. Secret key establishment for DNS (TKEY RR). http://tools.ietf.org/html/rfc2930, September 2000.

[3] M. Andrews. The dnssec lookaside validation (dlv) dns resource record, rfc 4431. http://www.ietf.org/rfc/rfc4431.txt, 2006.

[4] R. Barnes. Use cases and requirements for dns-based authentication of named entities (dane), rfc 6394. http://tools.ietf.org/html/rfc6394, October 2011.

[5] P. Hoffman and J. Schlyter. The dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa, rfc 6698. http://tools.ietf.org/html/rfc6698, August 2012.

[6] Paul Vixie. Extension mechanisms for dns (edns0), rfc 2671. http://tools.ietf.org/html/rfc2671, August 1999.

[7] Paul Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington. Secret key transaction authentication for DNS (TSIG). http://tools.ietf.org/html/rfc2845, May 2000.

[8] S. Weiler. Dnssec lookaside validation (dlv), rfc 5074. http://tools.ietf.org/html/rfc5074, November 2007.