Countering the Cyber Threat through Trusted and Secure Cross-Domain Collaboration

Surevine's experience with inter-agency information sharing in UK Central Government has influenced design choices in the infrastructure and collaboration models used for Cyber-defence in the UK spanning the public and private sectors. In particular, reusing techniques designed for cross-domain, multi-level information handling models allows fine control over which information is shared, and enables solid security.

This paper discusses:

- Authorization using fine-grained access control and ABAC.
- User-driven authorization based on security labeling and RBAC.
- Semantic enrichment of metadata.
- A publisher-based strong authentication model.
- Anonymity as a collaboration enabler.

Surevine's position is that this combination leads to increased collaboration by giving partner organizations increased confidence to maximize cyber-threat intelligence sharing.

Introduction

About Surevine

Surevine is the provider of software and consultancy services to Her Majesty's Government (HMG) within the UK, and are a key supplier to CERT-UK. In particular, Surevine provide the CiSP platform for CERT-UK, allowing partners across Government and Industry to collaborate by sharing threat data and discussing mitigations.

Due to this work, Surevine have been selected as part of the UK Prime Minister's delegation to the USA promoting international cyber-threat sharing, and have been invited to attend the forthcoming RSA Conference.

Authorization Technologies

RBAC and SIO – Explicit Labelling

A key technology used within military and government agencies for the past 20 years has been security labelling based on the Rule Based Access Control (RBAC) model described in [SDN.801c]. This provides for a set of absolute levels of sensitivity, called *Classifications*, and a set of vertical *Categories*, typically driven by a *Security Policy Information File* (SPIF) that defines the classifications and categories and the relationships between them.

End-users typically deal in *Protective Markings*; a human-readable phrase which can be constructed from the machine-readable label using the rules in the SPIF. Labels can be checked against Clearances to provide access control decisions.

A complete *Information Handling Model* (IHM) expressed as an SDN.801c SPIF has relatively high complexity for end-users, however it can express complex and rigorous handling rules, and by selecting particular labels, end users can control the access level.

Surevine has found that a simple "traffic-light" policy has been extremely effective at allowing untrained users to convey the sensitivity of the data, where "Green" information is freely shared, "Amber" is restricted, and "Red" is solely between the industrial partner and HMG. It seems likely a more complex policy might also work; military and government agencies routinely use more complex IHMs, though in most cases users receive some training.

ABAC - Automated Fine-grained Access Control

For fine-grained access control, it is often useful to use the incident metadata to define how it is shared. This is conceptually equivalent to the Attribute Based Access Control model defined by [NIST SP 800-162].

Information from the Resource (the threat data), the Subject (the entity the data is to be shared with), and the Environment (the source of the data) is evaluated to produce an access control decision. Included in the resource attributes is the explicit label provided by the publisher, and one of the subject attributes is the subject's clearance – this enables an ABAC system to easily incorporate concepts from a RBAC system.

The key standards for ABAC are the XACML family of syntaxes from OASIS which define the policy declaratively in XML; however we have found in practise that the technically-skilled policy administrators typically working with sharing technical data such as cyber-threat intelligence are more comfortable with defining a data-driven policy imperatively using JavaScript. This has the advantage of familiarity, though these are unstandardized.

Semantic Enrichment

It is important to note that authorization policy is easier to express when dealing with semantically combined units of data. An email thread has a different significance to any individual email within it; an IM message out of context is different to the conversation as a whole. Similarly, individual incidents can be associated with larger-scale attacks, and the desirability to share data in the incident will change when this happens.

The metadata of the attack therefore feeds into the access control decision, and in the model outlined above becomes additional attributes for the ABAC policy. Attacks, of course, may well span incidents reported by multiple organizations unaware of the bigger picture; it seems likely that a typical policy will be to allow more sharing between organizations targeted by the same single attack.

Anonymity as a Collaboration Enabler

Surevine has witnessed an unwillingness of most organizations to share information that highlights a prior weakness in cyber defence. A typical tendency, most obviously visible in press releases and other public information, is to downplay attacks. This, in turn, leads to a reduction in incident intelligence sharing, even within closed systems.

Surevine believes the correct mitigation for this is to sanitize data at the point of sharing, removing identifiable data as required. In Surevine's implementation, this is driven in part by the "traffic light" system which we characterize as a simple RBAC system, as above.

This enables confidence that intelligence can be shared without publicizing its provenence, and embarrassing the source organization.

Publisher-based Strong Authentication

There are two bases for authentication currently deployed within the cyber-defence information sharing community. AbuseHelper uses the authentication model of XMPP, where peer servers authenticate strongly (via PKIX/TLS); we assume that data peering would be carefully mediated such that essentially this equates to trusting the Publisher.

TAXII on the other hand favours message object signing in a transport independent manner, such that the trust is not of the Publisher but of the Originator.

Due to the requirements of anonymity as stated in the previous section, the data is often sanitized between partners, and therefore is required to be signed and resigned each time it is shared. Moreover a signature clearly identifies the Originator.

Therefore Surevine strongly favours authenticating the Publisher, typically by authenticating the TLS transport layer via PKIX. This implies a mesh-style federation, such as used by XMPP. Note that TAXII's signing is not mandatory, so the two models are not incompatible.

Conclusions

Surevine's experience with sharing many kinds of information between security-concious agencies has led to the use of a number of technologies and techniques. In each case, these are designed to facilitate, enable, and promote collaboration, through increasing Originator confidence in the security of their data and identity.

Bibliography

[SDN.801c] "SDN.801: Access Control Concept And Mechanisms, Revision C", National Security Agency.

[NIST SP 800-162] "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", Vincent Hu et al, National Institute of Standards and Technology.