DATA SECURITY

Diego Lopez

Telefónica I+D, S.A.U, C/ Emilio Vargas 6, 28043 Madrid, Spain
Email: diego@tid.es

1 STATE OF THE ART

There is a range of reasons for securing data and systems, from those already common nowadays (IPR, licenses, privacy, confidentiality, etc.) to others likely to appear in the future (distributed trust, reputation building, social collaboration, etc.). The systems need to manage the data according to these restrictions while maintaining other requirements for data infrastructures (e.g., scalability, interoperability, provenance), and also the systems themselves need to be secured against potential external attacks.

Obviously, "data security" covers a lot of different aspects of data infrastructures that may be both technical and organizational: procedures, policies, physical access, etc. Indeed, data security must be implemented for all components of a data infrastructure as a single loose link would potentially break the secure chain. Moreover, even though the definition of what data security encompasses may vary with the requirements of a specific community, a generic data infrastructure needs to account for all security aspects of the communities combined.

For the purpose of this report, let us divide security issues into the following three groups.

1. Business continuity: Measures taken in order to guarantee the operation of the system, such as protection against loss of data, disaster recovery, standard operating procedures of data centres including physical access control, policies governing access, etc.
2. Incident handling: Measures taken to prevent and remedy security losses, including the analysis of events to consolidate knowledge into improved security procedures
3. AAA (Authentication, Authorization, and Accounting): Measures taken in order to establish the rights of (any kind of) users to access the system, to apply those rights, and to appropriately register that access

The first group can be considered as covered by common IT best practices and few, if any, issues are related to specific aspects of data infrastructures. Therefore, we will not discuss it in this report and will just recommend the adherence to those best practices as they evolve along the lines of technology evolution (ISO/IEC 27031, 2011).

Security incident handling in Internet-based systems has a well-structured knowledge and practice corpus (RFC 2196 - Site Security Handbook) including recent considerations about highly distributed computing and data infrastructures (through experience gained in handling security incidents within computing grids). It is reasonable to expect that technologies and policies will evolve accordingly in this area though certain particular aspects connected to data management deserve particular attention. Those particular aspects of incident handling will be considered at the correspondent sections in the rest of the report.

Authentication is the process that allows entities (*users*, that will be humans in general though other agents can be requested to do so as well) to establish their *identity*, in the form of the *attributes* associated with them that are relevant for a certain purpose. *Authorisation* establishes the rights of such a user to perform a certain operation on a certain *resource* at a given time, according to the received identity attributes and the appropriate *policies* defined for resource access. *Accounting* collects data about both acceptable and rejected access requests to resources, recording the credentials provided by the requestor, the resource requested, and the outcome of the request. These data can be

further processed for many purposes though the most relevant in terms of security is the ability of tracing activity in order to identify breaches, attack patterns, and compromised entities.

From the above definitions it becomes clear that, in a highly distributed and collaborative environment that crosses multiple administrative domains and national boundaries, authentication must be performed as close to the users as possible while authorisation should be decided as close to the resources as possible, and accounting must be performed in a coordinated way in order to make any sense out of records.

2 TEN-YEAR VISION

Security cannot any longer be a matter of keeping “the inside” out of reach of “the outside”. The borders between these two become completely blurred in an open, highly heterogeneous, distributed environment and much more when it comes to data subject to complex usage and aggregation patterns. Security must become pervasive and be dynamically associated with data themselves and their metadata so the entities in the different ecosystems can apply the policies they consider relevant.

These security metadata should contain access requirements for datasets, accounting records to evaluate their provenance and integrity, and reputation records that will allow the entities to decide on the trust and usability of each dataset. Derived datasets built for whatever purpose (interdisciplinary access, privacy preservation, correlation, etc.) will generate their security metadata from the origin dataset(s) so as to provide a coherent availability of security information across different ecosystems and access patterns.

Security metadata accuracy requires well-established services for identifying not only entities but also datasets themselves, and therefore a system guaranteeing global, well-structured, verifiable permanent identifiers should be in place.

Entities should be able to prove their identities by different mechanisms at identity providers (IdPs), according to security and usability criteria. Identity attribute values will be established by means of attribute authorities (AAs), under control of different organisations and communities. The identity will be transferred to applications by means of identity relying parties (IRPs) that will accept data of recognized IdPs and AAs. This requires an established trust framework between the interacting parties. Whereas this can be considered the current status of identity federations, we envisage evolution along these main lines: the dynamic establishment of federation associations, the aggregation (and possibly translation) of identity data from different sources, and the possibility of expressing the levels of assurance for identification mechanisms and attributes. Furthermore, communities should be empowered to manage their AAs as they see fit, as long as they comply with the rules expressed for the relevant level of assurance.

RPs and applications should be able to rely on policy decision points (PDPs), where rules can be stored and managed by the data infrastructure operators and dataset owners. Rules should consider not only access control but also requirements related to accounting mechanisms, security metadata updating, and reputation establishment. It should be possible to manipulate rules according to human-friendly mechanisms and specifically to express them in a way close to natural language.

Accounting logs should be kept at least to the level of PDP rule matching though much finer detail should be possible when necessary. Since accounting logs are themselves datasets, the security mechanisms previously described also apply to them. Accounting records should use a rich format that is able to support semantic information and therefore suitable for complex querying and reasoning, supporting the wide range of potential applications for such information, from supporting security incident handling and resolution to providing evidence for resource planning or auditing procedures.

As mentioned above, security metadata and accounting logs should be used to enhance security incident handling and simplify the procedures for responding to security breaches, a key requisite as the protected infrastructure becomes more distributed and heterogeneous.

We have mentioned reputation several times above. We envisage the availability of mechanisms through which entities will be able to express the value they give to a certain dataset so other entities will be able to make decisions based on these statements and the confidence they put in the reporting entity. This will result in a "web of trust" that combines formal (such as peer paper reviews or project reports), informal (such as social tags or user ratings), and infrastructural (such as availability indexes or security incident reports) statements. Reputation is, in essence, a special type of accounting record, and it will have similar characteristics though it is important to note that derived datasets should be able to inherit their component dataset's reputation.

All this requires the support of a trust framework that experience has shown cannot be derived hierarchically from a single global root (this has been the perpetuum mobile of digital security for many years), and therefore the necessary support of mechanisms for maintaining a set of roots of trust and for selecting where to apply them according to a heterarchical model in the scientific data ecosystems. The diversity of the infrastructure should make these mechanisms be based on different trust-enabling technologies (Perlman, 1999) and able to associate different policies with different subsets of the roots and applicable technologies. Being the core of any of the services discussed in this document, the correct definition and implementation of these mechanisms constitute the key aspect for the availability of a global data security infrastructure.

3 CURRENT CHALLENGES

The main challenges to the realisation of the vision depicted above are essentially related to the evolution of the AAA infrastructures themselves (e-IRG Blue Paper, 2010) though it is important to take into account as well the consolidation of security metadata models and the exploration of new patterns for integrating the two former (AAA evolution and security metadata) with the rest of the data infrastructure.

When it comes to authentication and authorisation, the most obvious challenge is the requirement to align the current so-called academic identity federations, essentially grouped around REFEDS (http://www.refeds.org/), to user-centric identity technologies (Jøsang & Pope, 2005) and the adoption of the powerful usability paradigms that these technologies are providing, harmonizing them with the diverse access-control requirements implied by the nature of data. The concept of a "home organisation" able to provide all identity attributes pertaining to a certain individual is becoming more and more questioned even by current usage patterns. User identification and attribute aggregation from several sources, and possibly from different trust domains, must be supported as the normal way for identity building, backed by appropriate mechanisms to support the expression of relative values to the sources of those identity data (levels of assurance). This requirement introduces interesting challenges in the way in which research networks have established their user identities. Going further, identity infrastructures must address how non-human entities (e.g., servers and agents) can be identified and data about them updated, collected, and processed, and how their attributes can be linked back to a human acting as eventually responsible for their behaviour.

The challenges mentioned above become even stronger in the case of the management of virtual teams, a key tool for supporting the collaborative (and even social in most cases) nature of the virtual research environments that data infrastructures will enable and rely upon. Current systems are highly centralised and oriented towards closed community environments, supporting reduced user populations where links are tight and user status is generally a rather stable condition that changes according to well-established patterns. In the future, these systems must provide support for the much more open and distributed environment required by interdisciplinary science, the different levels of data aggregation, and open linking, just to cite a few of the challenges described in the GRDI current roadmap. Furthermore, virtual team management systems must be able to incorporate social aspects that will eventually make them the foundation for reputation systems.

So far, we have concentrated on authentication challenges. Because the processes to identify users, to collect data about them from trusted sources, and to transfer these data to relying parties are the best understood and widely deployed, it is relatively easy to identify more detailed challenges ahead. When it comes to authorisation, the first and most important challenge is to make it reach a status similar to authentication infrastructures. The current model for access control relies on few-to-many relationships: many final users consuming a few resources that apply their well-controlled local authorisation policies. Data infrastructures require the support of many-to-many relationships, where users and communities act indistinctly as resource producers and consumers. Ways must be found to easily express and enforce authorisation rules; therefore, a pervasive authorisation infrastructure that is simple and easy to access and manage is required.

While accounting in homogeneous (such as OS, application, specific infrastructures) environments is commonplace, that is not the case for highly distributed, heterogeneous infrastructures like the ones envisaged for global research data. Some initial efforts have been made, and particular mechanisms have been deployed in Grid infrastructures and elsewhere such as the GRID Accounting and Usage Study (JISC, 2007). However, this remains as an area that requires extensive development in the coming years.

The integration of security metadata in the general metadata schemas must be accomplished well beyond the status of a declaration of access policies or rights. Security metadata, in all their aspects, have to become an integral part of data modelling and management as well as a foundation for data services and virtual research environments. Ontologies must take into account security aspects, allowing the assessment of security policy interoperability and supporting security among the mediation services.

To conclude, let us remark the extraordinary relevance of security services into any workflow taking place on data infrastructures and, as a consequence, the need that those services can be used as transparently as possible. Security services must be considered as one of the foundation services for data infrastructures and therefore offer developers and users the possibility of implicitly applying them unless more fine-grained explicit control is required.

4 RESEARCH DIRECTIONS PROPOSED

The current situation in what relates to identity technologies within the research network environment is of a slow convergence between Grid identities, based on X.509 certificates (Foster, 2003), and NREN-operated identity infrastructures, based on RADIUS (eduroam, the secure, world-wide roaming access service developed for the international research and education community: http://www.eduroam.org/) and SAML (http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf). Several proposals have already been demonstrated (and some actually deployed) to achieve this convergence, though they are yet to provide a full integration path and do not address problems such as agent identification or the integration of different authorities. On the authorisation side, there exist proposals for rule engines that mostly use XACML (http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html) to express policies and decision queries, but none of them has reached great acceptance, and they are far from the goal we mentioned above of being accessible to data providers willing to take advantage of them in a reasonably simple way.

The Moonshot project (http://www.project-moonshot.org/) constitutes a rather interesting approach in accelerating identity infrastructure convergence. The proposal is intended to leverage already existing infrastructures, thus flattening the adoption curve, and proposes the use of a general open interface (the GSS-API (RFC 5554 - Generic Security Service Application Program Interface)) for the exchange of identity data to applications, allowing them to consume these data with very limited changes (if any). A parallel approach is the one taken by the KITTEN working group (http://datatracker.ietf.org/wg/kitten/charter/), which seeks to improve and extend GSS-API and explore new SASL (RFC 2222 - Simple Authentication and Security Layer (SASL)) mechanisms. It is worth noting that these integration paths seem suitable for managing non-human agent identities as well. Another path worth exploring in this direction is the integration with governmental identity infrastructures, mostly rooted on PKIs that

leverage the availability of smart-card-based Digital National IDs. These infrastructures can provide roots of trust for many of (if not all) the identity assessment procedures applicable as well as constitute the choice when legally binding mechanisms are required, due to the nature of the data and/or the processing applied to them.

To achieve the goal of simplifying access to authorisation mechanisms and, in general, security services while offering rich internal mechanisms for identity data aggregation and authorisation decisions, the highly heterogeneous nature of the infrastructure we are considering calls for service-oriented solutions, either by means of the STS concept coined inside WS-Trust (http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html) or the OAuth (http://oauth.net/) protocol under discussion in the IETF. Identifying the most suitable protocols and profiles in each case, balancing expressiveness, efficiency, and simplicity of use while keeping the obvious interoperability goals will be a key task in the provision of service-oriented security solutions to the data infrastructure elements. Virtual team management systems and the emerging social protocols, such as FOAF (http://www.foaf-project.org/) and OpenSocial (http://www.opensocial.org/), appear as natural means for both providing support to enable the expression of collaboration-related attributes and expressing reputation. Another interesting direction for research is the applicability of user-centric (or user-mediated) models, either for identity exchange, such as OpenID (http://openid.net/) and OpenID Connect (http://openidconnect.com/) or for privacy and privilege management, such as UMA (User Managed Access – Kantara Initiative: http://kantarainitiative.org/confluence/display/uma/Home).

In order to facilitate the management of security rules, significant effort must be allocated to mechanisms able to map trust frameworks and access control models as close to human natural language as possible. In this respect, linguistic approaches to manipulate this information, based on computational intelligence techniques (like neural networks or fuzzy logic), seem the most promising direction.

Service-oriented architectures provide support for transparent accounting at a common baseline, that of the specific service invocations and results. In this respect, the use of semantically rich formats, the definition of accounting ontologies, and the application of distributed architecture and techniques for privacy preservation are areas of future research that should lead to an accounting infrastructure able to satisfy the goals described in the previous section.

Finally, significant effort is required in at least four distinct ways relating to schemas for security metadata. First of all, we have the identification of the structure of such metadata, their elements, attributes, and values (the schema itself, strictly speaking). Second, the expression of these schemas when security information is sent under different protocols “through the wire” must be decided. Third, the ability to deal with the multi-domain nature of these metadata is an essential feature. And, of course, security metadata have to be seamlessly integrated with general metadata formats.

5 RECOMMENDATIONS

- Stimulate the process of the continued integration of different identity technologies in the research and academic community through active collaboration with initiatives such as REFEDS and the IGTF, and contacts with strategy forums such as e-IRG and ESFRI.
- Coordinate with research groups and pilot projects dedicated to federated identity models applicable beyond Web access, providing requirements, use cases, and validation mechanisms at their earliest possible stage.
- Collaborate in the development of standard methods for the new frontiers in data service integration with security infrastructures, especially in what relates to user-mediated authentication and authorisation, distributed accounting, and security metadata.
- Promote awareness among research projects and e-infrastructure operators, exhorting them to consider their data security requirements from the beginning, in accordance with the standards and best practices adopted by the community.

6 REFERENCES

e-IRG Blue Paper (2010) pp 19-20.

Foster, I. (2003) The Grid: A New Infrastructure for 21st Century Science. In Berman, F., Fox, G., & Hey, T. (Eds.) *Grid Computing: Making the Global Infrastructure a Reality*, John Wiley & Sons.

ISO/IEC 27031 (2011) Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity.

JISC (2007) Grid Accounting and Usage Study. Retrieved from the World Wide Web, July 1, 2013: http://www.jisc.ac.uk/whatwedo/programmes/einfrastructure/accountingandusage.aspx

Jøsang, A. & Pope, S. (2005) User Centric Identity Management. AusCERT Conference.

Perlman, R. (1999) An overview of PKI trust models. *IEEE Network 6*, pp 38-43.

(Article history: Available online 30 July 2013)