Actor-Oriented Trust*

Ioanna Dionysiou[1]†, Deborah Frincke[2], David E. Bakken[1], and Carl Hauser[1]

Technical Report EECS-GS-006

[1] School of Electrical Engineering and Computer Science
Washington State University
Pullman, WA, USA
{idionysi, bakken, hauser}@eecs.wsu.edu

[2] CyberSecurity Group
Pacific Northwest National Laboratory
Richland, WA, USA
deborah.frincke@pnl.gov

January 26, 2005

Abstract

In a collaborative environment, a number of entities interact with each other to execute a task. In this situation, trust is examined not as a single relationship between a trustor and a trustee but as a chain of relationships related to some information. This paper presents actor-oriented trust modeling, a methodology for modeling trust characteristics when entities collaborate to achieve information delivery from source to destination, such as in peer to peer networks. Actor-oriented trust allows expression of a wide range of trust requirements imposed by different entities during the lifetime of an information flow within a system. A preliminary examination of actor-oriented trust in peer-to-peer, publish-subscribe and status dissemination systems shows the trust relationships in an ideal trust setting.

*The work was funded in part by the National Science Foundation under Grant CCR-0326006US Department of Commerce, and by the National Institute of Standards and Technology Grant #60NANB1D0016 (Critical Infrastructure Protection Program), in a subcontract to Schweitzer Engineering Labs Inc.

†Contact Author

1 Introduction

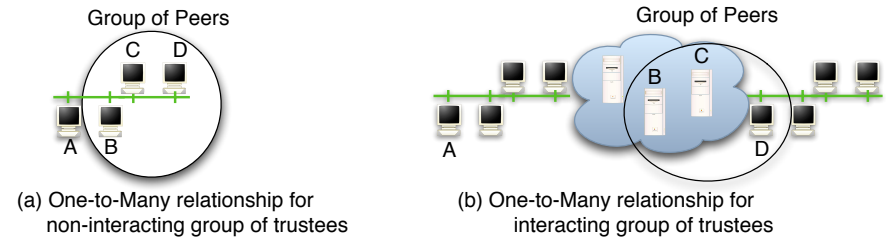
Trust is a multifaceted concept, encompassing even more than message integrity, source authentication and reliance on other entities. While trust evaluation is an integral part of decision-making in collaborative models, there is no single way to determine the right level of trust, or which aspects to include. Decisions about how to weigh each facet lie with the evaluator and can differ substantially from situation to situation. Researchers have defined trust concepts for many perspectives, with the result that trust definitions overlap or even contradict each other[12]. This makes it difficult to combine and compare the trust facets expressed in these models in many systems, especially those involving multiple participants. In contrast, we present the actor oriented trust model, which provides a framework for organizing general trust relationships between multiple participants in a broad range of systems. Actor-oriented trust supports reasoning about a chain of relationships related to some information as opposed to just a single relationship.

In a typical trust setting, there is a *trustor* and a *trustee*. A trustor is the entity that places its trust in another entity to act as expected, within a particular *context*. This second entity is the trustee. A trust relationship is one-to-many when a group of trustees are trusted similarly within the same context [7]. Current trust models are *pairwise* and support trust towards a non-interacting group of trustees. In Figure 1(a) A trusts B, C, and D to consume[1] data d in a one-to-many relationship. Recognition of one group member as untrustworthy would not affect the trust placed in the remainder of the group, provided that the untrustworthy member is expelled.

A pairwise approach cannot encompass the complexity of trust in collaborations that go beyond two. Consider the WAN in Figure 1(b). A trusts D, that resides on a different LAN, to consume its data. Intermediate entities B and C forward this data to D, so some form of trust also exists between entity A and the forwarding servers. Malicious intermediary servers would affect the trustworthiness of data received by D. Untrustworthy servers cannot simply be expelled from the trust group but must be replaced by trustworthy ones. Here, a trustor places its trust in interacting trustees that collaboratively execute a task rather than one alone. Actor-oriented can represent such *composite* views of trust based upon systematic assessment of data trustworthiness when data is handled by a chain

[1]Consume in this context means appropriately utilize

of different trustees. Both models are illustrated in Figure 1.



(a) One-to-Many relationship for non-interacting group of trustees

(b) One-to-Many relationship for interacting group of trustees

Figure 1: Pairwise and Composite Trust Models

2 Actor Oriented Trust: A Composite Trust Model

The composite trust model we are introducing is called *actor-oriented* to highlight the importance of trust bonds among *actors*. Actor-oriented trust operates on three key principles:

1. ***Principle of Information Lifecycle Decomposition:*** The information lifecycle is decomposed into stages, allowing independent examination of trust at each stage. We define *information lifecycle* as the interval during which information is created and consumed.

2. ***Principle of Trust Expectations:*** An actor forms expectations as a way to express concretely its interpretation of trust.

3. ***Principle of Information Trustworthiness Within its Lifecycle*** Information trustworthiness during a particular lifecycle stage is related to the trustworthiness of the actor that handles the information during that stage. Information trustworthiness is related to the trustworthiness of all entities that handle it, not just that of the creator of the data.

Trust in this model is an abstraction of individual beliefs and requirements that an actor has for specific situations and interactions. Behavioral, security and QoS requirements are included in a trustor's *expectations*. Expectations pertain to a specific trustor, in a given context, and this permits setting expectations based on individual perspective - who is assessing a given scenario.

Definition 2.1. *An expectation includes all behavioral (competence and motivation), security and QoS requirements derived from a trustor's goals, standards, principles and morals.*

Actor-oriented trust incorporates expectations in its definition and this empowers a trustor to customize trust for trustees at the different stages of the information lifecycle.

Definition 2.2. *Actor-oriented trust is the composition of subjective and dynamic beliefs placed by an actor (trustor) in other actors (trustees) to act as expected during the information lifecycle.*

There are two specialized forms of actor-oriented trust: *Information Provider Trust* (IPT) and *Information Consumer Trust* (ICT). IPT refers to the subjective and dynamic belief placed by an information consumer actor (trustor) on a information provider actor (trustee) to provide information as expected. Similarly, ICT refers to the subjective and dynamic belief placed by an information provider actor (trustor) on an information consumer actor (trustee) to consume information as expected.

As indicated earlier, there are many definitions of trust in the literature [5, 9, 7, 2, 11, 1, 12]. Grandison et al. [7] list five types of trust that are primarily tied to the resources and environment. This differs from our model in that trust is customized to either specific actions a trustee is allowed to do (resource access, service access, delegation) or specific actors (trustee certification, infrastructure). The trust view of Rahman et al. [1] focuses on the subject-object relationship. However the model in [1] considers explicitly a trustor's general trusting attitude as a trust type whereas actor-oriented trust encapsulates this attitude in its trust definition in the form of expectations.

It should be possible to represent each of these models using the actor-oriented approach. For instance, consider trustee certification, one of the trust types in [7], that refers to the certification of the trustworthiness of a trustee by a third party (certificate authority). In the actor-oriented model, the information consumer actor will be the entity that receives the certificate and the information provider actor will be the certificate authority. The certificate receiver establishes an IPT between itself and the certificate authority regarding the certificate contents.

2.1 Principle of Information Lifecycle Decomposition

Figure 2(a) shows the trust relationship between an information producer actor and an information consumer actor. Each is simultaneously a trustor and a trustee, but with different trust requirements. In distributed systems such as publish-subscribe information is delivered by intermediaries and their trustworthiness also must be assessed.

Information lifecycle was defined earlier as the interval during which information is created and consumed. By decomposition, we can break this three stages: generation, dissemination, and consumption.The actor responsible for the information at each stage is the information producer (generation stage), information dissemination medium (dissemination stage) and finally information consumer (consumption stage). After decomposition, trust can be examined and evaluated at this finer granularity for each stage in the information lifecycle.

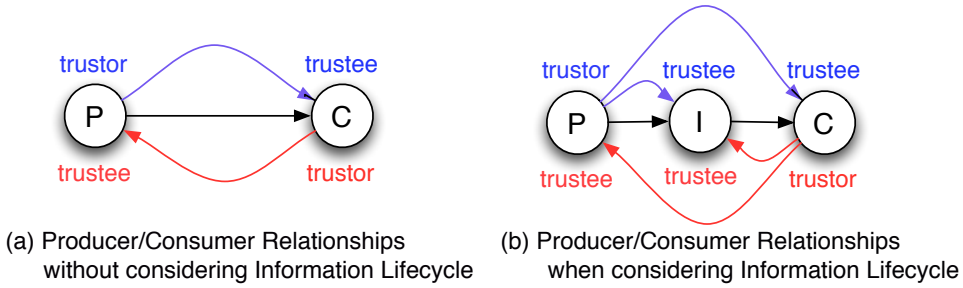


Figure 2: Trust Relationships without and with Information Lifecycle

Figure 2(b) illustrates the extended trust framework between an information producer and information consumer that takes into account the intermediary actor. Both the producer and consumer have a dual role (trustor and trustee) whereas the intermediary only acts as the trustee.

2.2 Principle of Trust Expectations

In an information system, an actor accepts one of these two:

- An information producer risks leakage or misuse of its information
- An information consumer risks receiving inaccurate or malicious information for use

The risk accepted when collaborating is based on assessments of both the entity at the end of the interaction and all intermediate entities. By Definition 2.1, expectation is a blend of behavioral, security and quality of service (QoS) requirements (Figure 3). Assessment of these requirements is an indicator of how much trust is to be placed on an information flow during its lifetime.

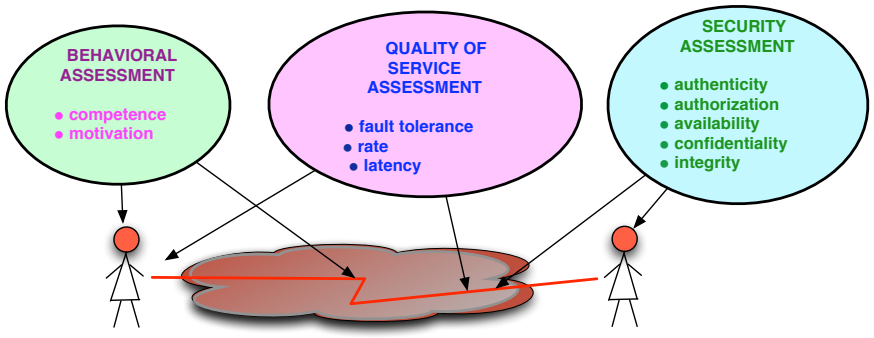


Figure 3: Trust Expectations: Behavior, Security and QoS Requirements

2.3 Principle of Information Trustworthiness Within its Lifecycle

The third principle is that information trustworthiness during a particular lifecycle stage is linked to the trustworthiness of the actor that handles the information during that stage. This principle is manifest in three different existing applications:

- Multilevel Security (MLS) systems use multilevel integrity and confidentiality policies to control information flow [13]. By definition, a subject need not question whether there has been a change in the authenticity or integrity of any document obtained via a trusted path.
- The PGP web of trust uses this principle in the relationship between an intruducer, a user, and a new contact. A user quantifies the degree of confidence placed in the introducers capability to authenticate new contacts. Consequently, the user decides the validity of the credential - mapping between a public key and its claimed owner - by examining the degree of confidence of the credential signer.
- In online auction sites such as eBay [ref], a buyer usually chooses a seller for the desired item from a pool of

potential sellers. Such an item can be a DVD player. The process of selecting a reliable DVD player largely hinges on the seller's reputation profile. A buyer is more likely to buy from a seller with a high reputation score than a seller whose profile contains negative feedback about unreliable DVD players. The buyer predicts reliability of the DVD player based on the reputation of the seller.

3 Using Actor-Oriented Trust

In this section we illustrate actor-oriented trust by applying it to peer-to-peer (P2P), publish-subscribe, and status dissemination (SD) systems. The basic actor-oriented trust relationships are shown in Table 1:

Table 1: Actor-oriented Trust Relationships in Generic Information Sharing System

RELATION	TRUST PLACED BY (Trustor)	TRUST PLACED ON (Trustee)
ICT(producer,consumer)	Producer of Information	Consumer of Information
ICT(producer,dissemination medium)	Producer of Information	Dissemination Medium
ICT(consumer,producer)	Consumer of Information	Producer of Information
ICT(consumer,dissemination medium)	Consumer of Information	Dissemination Medium

The four trust relationships are mapped to lifecycle stages. Consider each stage of the lifecycle in turn:

- In the generation stage, the information provider is the actor that assumes the role of the trust evaluator. It evaluates two ICT relationships, one for the information consumer and one for the information dissemination service.
- In the consumption stage, the information consumer assesses the trustworthiness of the information provider and the information dissemination medium by formulating the appropriate IPT relationships.
- In the dissemination stage, the dissemination medium has no expectations from either the provider or the consumer of the information.

We now show that this generic trust model can be applied to peer-to-peer, publish-subscribe and status dissemination, respectively.

3.1 Actor-Oriented Trust In Peer-to-Peer (P2P) Information Systems

Peer-to-peer file sharing systems allow users to collaborate in a dynamic manner and share information in large-scale distributed systems [10]. Information retrieval in P2P consists of two tasks: information discovery and information downloading. Information discovery includes forwarding query messages to locate peers that have the desired information and returning a list of those peers to the user who initiate the query. Information downloading is achieved with a direct connection with some peer that has the requested information.

There are four major actors in a P2P system: the downloading peer, the information dissemination medium, the uploading peer and the information discovery peer [2]. There are two information flow lifecycles: the query request from the downloading peer to the information discovery service and the information stream from the uploading peer to the downloading peer. Based on these two information flow lifecycles, the requirements for P2P require the following:

1. A downloading peer must be able to determine
    1.1. which uploading peers provide authentic files whose contents match their descriptions
    1.2. which peers are trustworthy during the information discovery search
    1.3. the trustworthiness of the connection that facilitates file downloading
    1.4. the trustworthiness of the connection that provides the information discovery list of target peers
2. An uploading peer must be able to determine
    2.1. which downloading peers will not further upload without permission
    2.2. the trustworthiness of the connection that facilitates file downloading.

Each information flow lifecycle is considered separately in the actor-oriented trust model. Therefore, two sets of the four trust relationships of the generic information sharing system are required, one set per lifecycle.

[2] We narrow the scope of the information discovery service to a single peer that locates target uploading peers

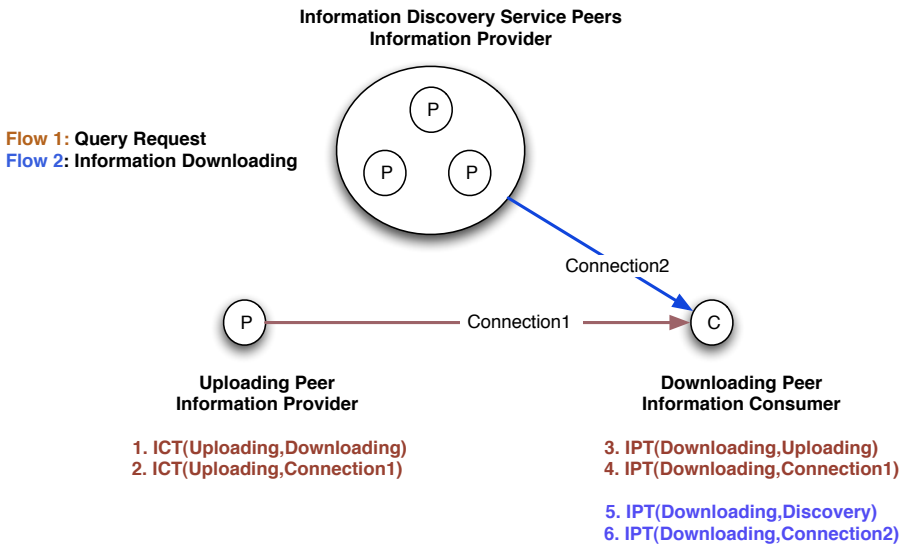


Figure 4: Actor-oriented Trust in Peer-to-Peer

The query request flow (Flow1 in Figure 4) is initiated by the downloading peer and targets a discovery information service peer that provides a list of uploading peers. In the actor-oriented trust paradigm, the requester peer is the consumer of the information and the discovery peer is its provider. Following the generic model of the trust relationships, the consumer establishes two IPT relationships: one for the provider and another one for the connection (Relationships 5,6 in Figure 4). Trust requirements 1.2 and 1.4 are satisfied by these two relationships. In a P2P environment, the information discovery service does not have any specific expectations[3] from the downloading peer and does not set the ICT relationships as dictated by the model.

The second information flow is the downloading of the requested file (Flow 2 in Figure 4) from the uploading peer to the downloading peer. The uploading peer is the provider actor whereas the consumer actor is the downloading peer. The generic model is applied for this flow without any customizations. The provider formulates two ICT relationships to build trust for the downloading peer and the facilitating connection (Relationships 1,2 in Figure 4). These two ICT relationships satisfy trust requirements 2.1 and 2.2. The equivalent IPT relationships (Relationships 3,4 in Figure 4) are constructed at the consumer site, covering trust requirements 1.1 and 1.3.

[3]The only trust issue would be to trust the requester peer that it does not abuse the service by launching denial of service attack

The question that emerges is whether or not these trust relationships are feasible to establish and evaluate. At this point, we must consider the fundamental principle of anonymity that governs pure P2P systems. P2P systems did not make any provisions for trust evaluations. This is by no means a design fault, because P2P was built as an open shared file paradigm. However, malicious peers' behavior has destructive effects on the operation of the system. In order to defend and protect themselves, peers rely on reputation systems to obtain opinions about other peers. These schemes range from simple recommendation systems to more dynamically updated reputation systems that operate on some form of centralized reputation database. Assuming that a recommendation system exists for all actors, we believe that IPT and ICT relationships involving provider and consumer actors are conceivable. Actor-oriented trust framework must consider more factors, such as motivation, that cannot be answered by recommendation networks. Nevertheless, it is a starting point.

The focus on peer trustworthiness neglects the connection properties and how they affect the trustworthiness of the transferred data. A compromised connection is vulnerable to numerous attacks. The actor-oriented approach explicitly considers the security (as part of the more general concept of trust) of the network. Due to the fact that a point-to-point connection (including transport layer TCP/UDP connections) is a degenerate form of an information dissemination medium, its trust properties are easy to verify by examining the security features of the direct connection. SSL, TLS, IPSec provide security services that guarantee authentication, integrity and confidentiality. VPNs are also possible candidates for connecting extranet peers in a secure manner.

Finally, we consider the matter of synthesizing trust relationships. For example, trust relationships 3 and 4 of Figure 4 assess at consecutive lifecycle stages the trustworthiness of the information during its generation (at the uploading peer) and its dissemination (by the connection). In order to minimize the risk of downloading malicious information, the consumer must decide the appropriate course of action when the uploading peer is untrustworthy and the connection is trustworthy, and vice versa. The contribution of the actor-oriented approach is that it provides a model to enable the synthesis of the various relationships at each stage to reflect the overall trustworthiness of the information.

3.2 Actor-oriented Trust in Publish-Subscribe Information Systems

Publish-subscribe is an asynchronous form of messaging that allows decoupling in time, space and flow[4]. A subscriber registers its interest with an event service and a publisher advertises its publication to the same event service. A network of event servers facilitates the distribution of event messages between publishers and subscribers. The dissemination of events is accomplished through matching algorithms that control the way event messages are delivered to the subscribers.

There are a few papers, such as the work by Wang et. al [14], dealing with security issues for a type of publish-subscribe system (content-based system) but without any special attention to trust issues. The major concern is that security mechanisms eliminate, in most cases, the spatial decoupling feature of the publish-subscribe system. Trust is also challenging in this system because of the intermediary network of store-and-forward servers between publishers and subscribers.

The main actors in a publish-subscribe system are the publishers, subscribers and the event servers. The event servers facilitate information dissemination as well as matching between publications and subscriptions. There are three information flow lifecycles: message forwarding from publisher to subscriber, publication advertisement from publisher to event servers, and subscription request from subscriber to the event servers. The trust requirements for publish-subscribe are:

1. A publisher must be able to:
    1.1. infer which subscribes are likely to leak information
    1.2. rely on the event servers regarding message forwarding
    1.3 rely on the event servers for proper handling of its publication notification
2. A subscriber must be able to:
    2.1. infer which publishers publish trustworthy data
    2.2. rely on the event servers regarding message delivery

2.3. rely on the event servers for proper handling of its subscription request

3. An event server must be able to rely on the other trustworthy servers that receives messages from or forwards messages to them

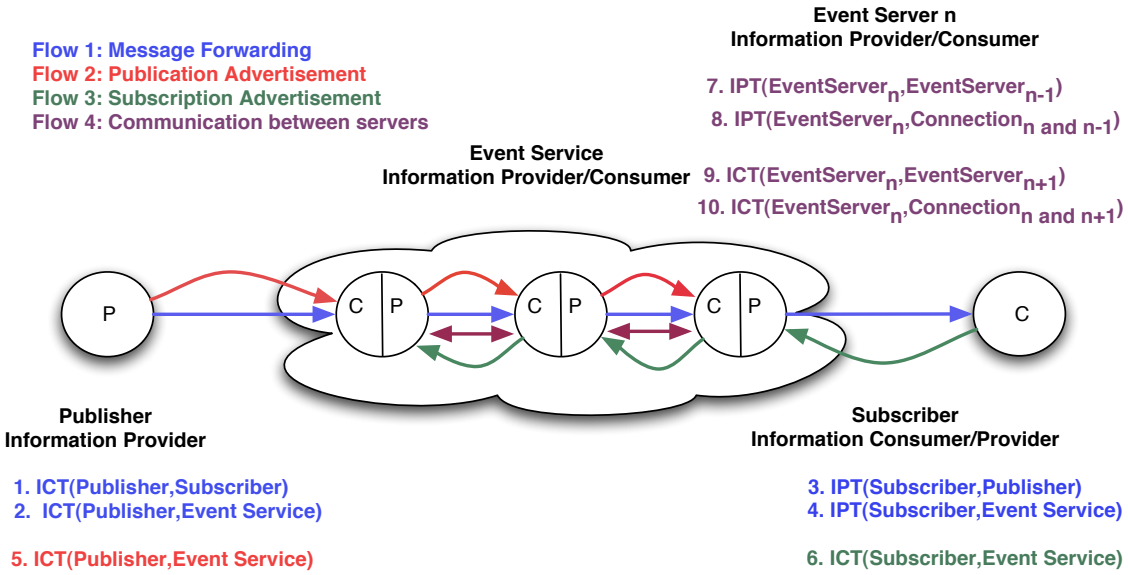


Figure 5: Actor-oriented Trust in Publish-Subscribe

Figure 5 illustrates the trust relationships that satisfy the requirements mentioned above. As in P2P, each flow is examined independently in the actor-oriented model. Starting from the first flow of message forwarding, the trust relationships of the generic model are applied as they are. The provider is the publisher, the consumer is the subscriber and the event servers are the information dissemination medium. Hence, relationships 1, 2, 3, and 4 of Figure 5 map to the trust requirements 1.1, 1.2, 2.1, and 2.2. The next flow is between the publisher and the event servers. The publisher expects that the event servers will operate correctly with respect the proper forwarding and placement of its publication advertisement. We assume that the event servers have no expectations or demands from the publisher. Due to this simplification, there is only one trust relationship for this flow, which is the ICT between the publisher and the event servers (relationship 5 of Figure 5). Trust requirement 1.3 is satisfied by this relationship. The third flow, the subscription notification request, is similar to the previous one and the same reasoning applies for this case too. The ICT between the subscriber and the event service (relationship 6 of figure 5) maps to trust

requirement 2.3.

The difference between the dissemination services of P2P and publish-subscribe is that the former is a point-to-point connection whereas the latter is a chain comprised of interconnected servers. Each event server acts as both a provider and consumer of information by forwarding to and receiving messages from its adjacent servers. Hence, the four trust relationships of the generic model apply for each pair of interconnected servers. Relationships 7 through 10 of Figure 5 illustrate the trust establishment for server n, which is positioned as the middle server in the path chain $< n-1, n, n+1 >$. Both a provider and a consumer actor must synthesize the individual trust relationships for the servers involved in forwarding/matching operations so as to derive the trustworthiness of the information dissemination medium as a whole.

3.3 Actor-Oriented Trust in Status Dissemination Systems

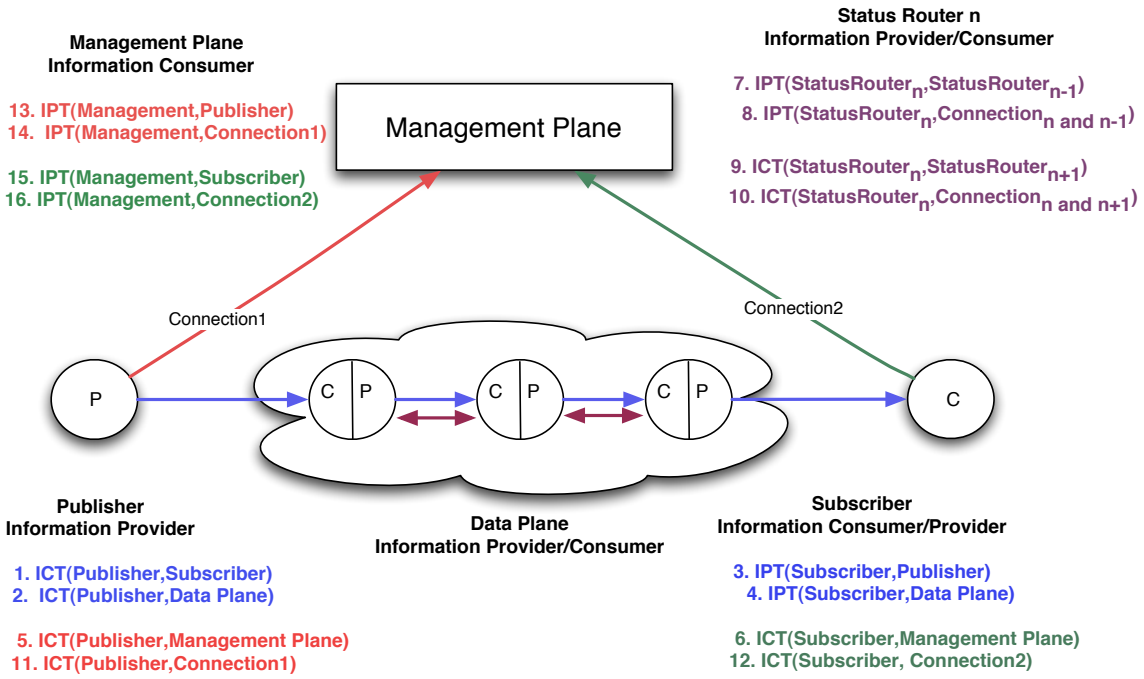


Figure 6: Actor-oriented Trust in Status Dissemination

Status Dissemination (SD) is a specialization of the publish-subscribe paradigm that is designed to take advantage

of the semantics of status variables, which are periodic sequences of time-stamped values [8, 6, 3]. The SD paradigm separates data flow from its management: a data plane that delivers events and a management plane that controls resource allocation in the data plane. QoS guarantees are met by pre-allocating subscription paths. Restricting the general publish-subscribe to SD allows for a simplified and more manageable trust infrastructure. In SD, the management plane can systematically instrument its explicit topology to collect resource information from the data plane.

SD, as a specialization of publish-subscribe, supports the four actors: publisher, subscriber, management plane, and data plane. The trust requirements presented in Section 3.2 are applicable to SD with the management plane and the data plane undertaking the task of the event servers. Figure 6 illustrates the trust relationships in status dissemination. The data plane replaces event servers in Relationships 1, 2, 3, and 4 of Figure 6. The management plane introduces new trust relationships because it processes the publication and subscription notifications. To be more specific, relationships 5, 11, 13, and 14 are the four relationships of the generic trust model between the publisher and the management plane for the publication notification. The assumption is that the management plane might want to protect the data plane from resource starvation by restricting access to it. Similarly, relationships 6, 12, 15, and 16 capture trust between the subscriber and the management plane regarding the subscription request.

4 Conclusions

Actor-oriented trust is a new paradigm that examines information trustworthiness in a piece-wise manner by composing the trustworthiness of the actors that handle the information from its creation to its consumption. The actor-oriented framework is applicable to a wide range of architectures including peer-to-peer, publish-subscribe, and status dissemination.

References

[1] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *Proceedings of the 33th Hawaii International Conference on System Sciences (HICSS)*, pages 1769–1777, Maui, Hawaii, January 2000.

[2] Alfarez Abdul-Rahman and Stephen Hailes. A distributed trust model. In *Proceedings of the ACM New Security Paradigms Workshop*, pages 48–60, September 1997.

[3] Ioanna Dionysiou, Kjell Harald Gjermundrod, and David E. Bakken. Fault tolerance issues in publish-subscribe status dissemination middleware for the electric power grid. In *Supplement of the 2002 International Conference on Dependable Systems and Networks (DSN-2002)*, Washington, DC, June 2002.

[4] Patrick Eugster, Pascal Felber, Rachid Guerraoui, and Anne-Marie Mermarec. The many faces of publish/subscribe. *ACM Computing Surveys (CSUR)*, 35(2):114–131, July 2003.

[5] Diego Gambetta. Can we trust trust? In *Trust: Making and Breaking Cooperative Relations*, chapter 13, pages 213–237. Electronic edition, Department of Sociology, University of Oxford, 2000.

[6] K. Harald Gjermundrod, Ioanna Dionysiou, Carl Hauser, David Bakken, and Anjan Bose. Flexible and robust status dissemination middleware for the electric power grid. Technical Report TR-EECS-GS-003, Washington State University, September 2003.

[7] Tyrene Grandison and Morris Sloman. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials*, Fourth Quarter, 2000.

[8] Carl Hauser, David E. Bakken, and Anjan Bose. Failure to communicate: Next generation requirements, technologies, and architecture for the electric power grid. *IEEE Power and Energy Magazine*, March/April, to appear 2005.

[9] Daniel W. Manchala. E-commerce trust metrics and models. *IEEE Internet Computing*, 4(2):36–44, March 2000.

[10] Dejan S. Milojicic, Vana Kalogeraki, Rajan Lukose, Kiran Nagaraja, Jim Pruyne, Bruno Richard, Sami Rollins, and Zhichen Xu. Peer-to-peer computing. Technical Report HPL-2002-57, HP Laboratories Palo Alto, March 2002.

[11] Robert Solomon and Fernando Flores. *Building Trust in Business, Politics, Relationships and Life*. Oxford University Press, 2001.

[12] University of Southampton and QinetiQ. *Trust Issues in Pervasive Environments*, September 2003.

[13] U.S. Department of Defense. *Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD*, December 1985.

[14] Chenxi Wang, Antonio Carzaniga, David Evans, and Alexander Wolf. Security issues and requirements for internet-scale publish-subscribe systems. In *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS-35)*, Big Island, Hawaii, January 2002.