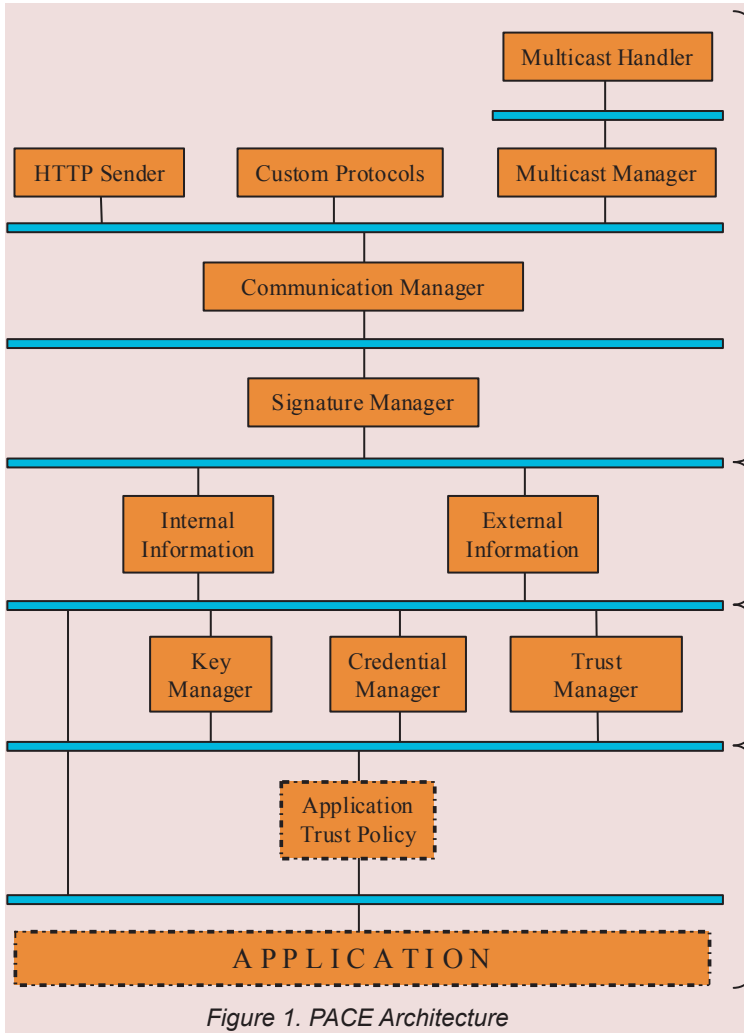


Introduction

We present a new architectural style PACE that facilitates trust management in decentralized applications where peers coordinate with each other. PACE enables a peer to develop meaningful trust relationships with other peers by providing trust-centric guidance regarding the internal composition of a peer. PACE uses message-based asynchronous communication and is a specialization of the C2 architectural style.

Key Benefits

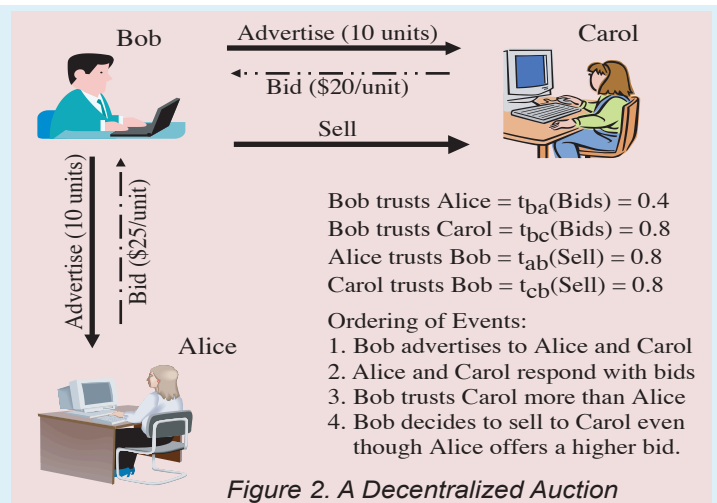
- Provides guidance for integrating trust, communication, and data models within a decentralized peer.
- Induces beneficial properties that help address common threats of decentralization.
- A modular generic architecture that can be modified for use for a wide range of decentralized applications.
- A framework to support application development in the PACE architectural style.
- Plug-in trust, communication, and data components that can be reused across applications.



- Handles the interaction of a peer with other peers
 - Signature Manager signs messages and verifies identities
 - Communication Manager creates protocol handlers at run time
 - Protocol Handlers convert protocol-specific messages into events and vice-versa
- Separates information into internal and external
 - Internal information refers to a peer's personal beliefs
 - External information refers to the communicated beliefs of other peers
- Encapsulates trust management policies of the peer
 - Trust Manager incorporates trust models/algorithms
 - Credential Manager maintains the identities of other peers
 - Key Manager generates unique public-private key pairs used for message authentication
- Includes components that satisfy specific application needs
 - Application Trust Policy allows the use of trust dimension that depend upon the need of the application
 - Application-specific components determine local behavior and may include user interfaces

Example 1: Decentralized Auction

- No centralized controlling authority
- Sellers advertise availability of goods and provide a URL where bids may be placed
- Buyers contact seller directly
- Advertisements are multicast; bids are sent point-to-point
- All peers use the same trust model and policy to facilitate semantic comparison of trust values
- Reverse auctions are also supported where buyers place advertisements and seller contact buyers



Example 2: COP

The Common Operational Picture is a near real-time picture of a battle scenario shared by multiple independent coalition partners, in this case USA, France, and England. Using PACE allows:

- entities to be added dynamically with less complexity
- a peer to assess confidence in the incoming data by determining trust in other coalition partners

USA Command and Control UI

Set Trust Val | Publish Trust Val | Peer Manager

Info Source | Recommendations | Share Info

Select a Recommendation to respond

USA_RRQ00

Requestor ID:

Target ID:

Category:

Request PK:

Expire:

Recommendation

Requestor ID: USA | Target PK:

Recommendation Set | Recommendation Path

England	Middle East... 2	10/10/2004	France
---------	------------------	------------	--------

Show RRQ | Show Recom | Show Info | Send RRQ | Send Recom

Figure 3. USA Command and Control

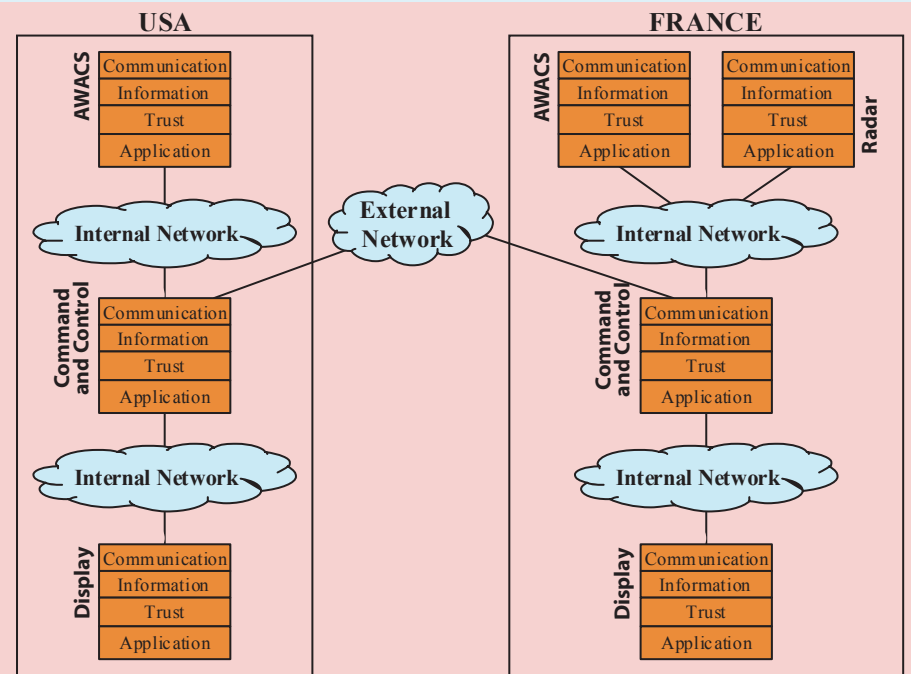


Figure 4. COP Architecture in PACE

- USA trusts France as a recommender and so requests France for information about England
- USA receives recommendation about England from France
- The USA Command & Control uses this information to evaluate data received from England

Threats	Policies	Key Components	Comments
Impersonation	Signatures	Key Manager, Signature Manager	Without the correct private key, the signature will not validate as coming from the corresponding public key
Fraudulent Actions	Trust Values, Broadcasts	Application Layer, Trust Manager, Communication Layer	In response, malicious users may be assigned a low trust value which can be broadcast to others to warn
Misrepresenting Trust	Trust Values	Application Layer, Trust Manager, Communication Layer	Users are able to consider the evaluations of others; messages may be published to warn others of malicious activity
Collusion	Signatures, Transitivity	Signature Manager, Trust Manager	A malicious collective can be defeated using explicit trust communication, digital signatures, and isolation of malicious peers
Denial of Service	Isolation	Communication Layer	By isolating protocols to the Communication Layer, malicious attacks can be blocked; firewalls can be actively controlled
Addition of Unknowns	Untrusted Events Still Seen	Signature Manager	Do not assign trust values to unsigned or incorrectly signed messages; allow users to still view and respond to such events
Deciding Whom to Trust	Domain-Specific Policies	Application Trust Policy	Each application may have certain behavior indicative of goodness or maliciousness that can be detected by an algorithm
Out-of-Band Knowledge	Overrides	Application Layer	Almost infeasible to have trust model capture all relevant inputs, therefore the user may need to adjust manually

Contact Information

Girish Suryanarayana, Justin Erenkrantz, Scott Hendrickson
 Professor Richard N. Taylor
 Institute for Software Research
 University of California
 Irvine, California 92697-3425

{sgirish, jerenkra, shendric, taylor}@ics.uci.edu
 949-824-{4047, 2776, 3100, 6429}
 949-824-4056 (fax)

This material is based upon work supported by the National Science Foundation under Grant No. 0205724. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.