# Managing Trust with Tokens and Capabilities

**Miron Livny**
UW-Madison Vilas Research Professor
John P. Morgridge Professor of Computer Science
PATh Principal Investigator

CHTC Center For High Throughput Computing

HTCondor Software Suite

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

AI Overview

Trust, in its most basic form, is the belief that someone or something is reliable, good, honest, and effective. It involves a willingness to be vulnerable to another party, trusting that they will act in ways that benefit you. This concept can apply to individuals, groups, or even institutions.

Here's a more detailed breakdown:

1. Trust as a Belief: Trust is fundamentally a belief in the positive attributes of another person or thing. This belief can be based on past experiences, reputation, or simply a general inclination to see the best in others.

# Is Trust a mutual relationship?

AI Overview

Yes, trust relationships are generally considered mutual, meaning both parties involved should feel a sense of confidence and reliance in each other. This mutual trust is built through consistent actions, open communication, and a willingness to be vulnerable and honest.

I am a Cat
My
Passport #
is 17

Autherization Entity

Identifier Entity

Client

Server

My name is Roo

My name is Soo

Server receives a request “send file Foo back to the requesting client”

How does the server trust the request?

1. Request presents an “Identifier”
2. Request presents an “Identifier Token”
3. Request presents a “Access Token”
4. Request presents a “Secrete”

I am a Cat
My
Passport #
is 17

Autherization Entity

Identifier Entity

Client

Copy of Foo

Give Me Foo

Server

My name is Roo

My name is Soo

CHTC Center For High Throughput Computing

HTCondor Software Suite

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

# For #1 server needs:

1. A proof from a trusted identifier entity that whoever (software) issued the request is associated with the provided Identifier
2. An Access Control List (ACL) from a trusted authorization entity
3. Understand the schema of the ACL

# For #1 Client needs:

1. Get an Identifier and a Secret (password) from the trusted identifier entity
2. Register Identifier with trusted authorization entity

## For #2 server needs:

1. To trust the Identifier and the Identifier entity that issued the identifier token.
2. An Access Control List (ACL) from a trusted authorization entity
3. Understand the schema of the ACL

## For #2 Client needs:

1. Register Identifier and obtain Identifier Token from trusted Identifier entity
2. Register Identifier with authorization entity

# For #3 server needs:

1. Trust that the token was issued by an authorization entity identified by the token
2. Trust the authorization entity that issued the token
3. Understand the schema of the token

# For #3 Client needs:

1. Obtain a token from the trusted authorization entity with the desired access permissions

# For #4 server needs:

1. To obtain from a trusted authorization entity a list of secrets and associated permissions
2. Understand the schema of the list

# For #4 Client needs:

1. To obtain a Secrete from trusted authorization entity

- When a Researcher places a job that reads Foo at the Access Point (AP) it entrusts the flie copy with the AP – namely the AP has full control over the copy of Foo and can hand it over to any client
- The AP is the client (via the EP) that requests the copy of Foo  from the server
- The server entrusts Foo with the AP – namely, must trust the AP as an authorization entity for Foo who can hand Foo over to any client

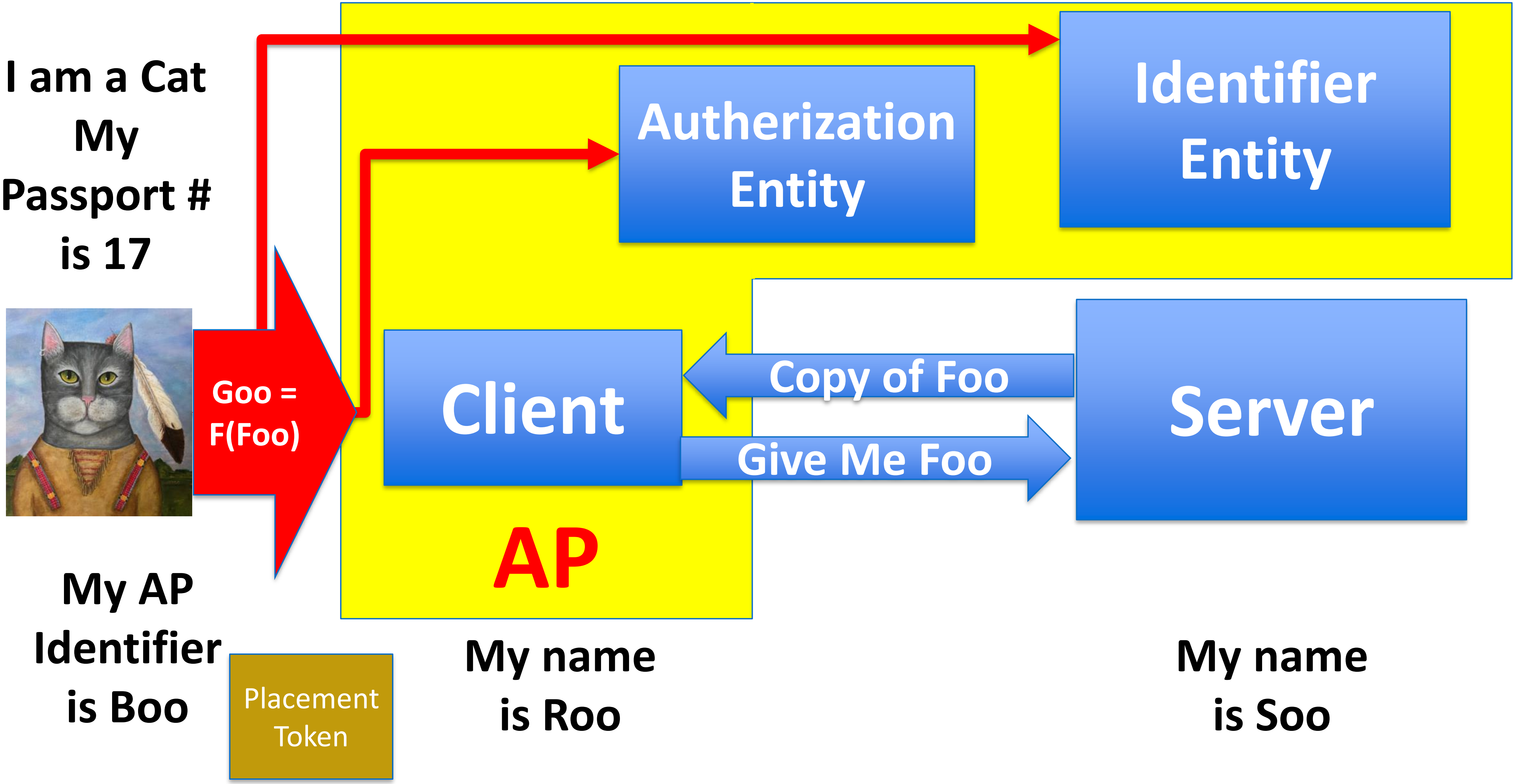
How does a researcher establish trust with the AP?

How does the AP associate a Job with a Researcher?

How does the Server establish trust with the AP?

# Prototyping Placement Tokens

- **To place a JobList at an AP the researcher needs to register with the AP**
  - If authorized, researcher is assigned an AP identifier.
  - AP registration does not mean an OS account on the server hosting the AP
- **To place a JobList at an AP the researcher needs a PlacementTokent for the AP**
  - If authorized, researcher is given an PlacementToken (capability, cookie)




CHTC Center For High Throughput Computing

HTCondor Software Suite

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

- **We are working on a prototype for the Placement Dameon (DP)**
  - Prototype includes a Web Server
  - Uses (external) campus Identifier Entity for “Passport # identifiers”
  - Uses an Access Control List provided by a Research Computing Facilitator
  - SchedD supports AP Identifiers for placement control and “Owner” identifiers