GENI Authorization
GEC 13

Tom Mitchell
March 13, 2012
www.geni.net

Sponsored by the National Science Foundation

Considering ABAC

- Evaluation
- Costs and Benefits
- Remaining Work
- Conclusion

Evaluating ABAC: Creating Attributes

Make Alice an ABAC Principal:

```
creddy --generate --cn alice
```

Results:

```
alice_ID.pem
alice_private.pem
```

Make Bob an ABAC Principal:

```
creddy --generate --cn bob
```

Results:

```
bob_ID.pem
bob_private.pem
```

Bob declares that Alice is a friend:

In ABAC notation: Bob.friend ← Alice

```
creddy -attribute
       --issuer bob_ID.pem
       --key bob_private.pem
       --role friend
       --subject-cert alice_ID.pem
       --out bob_friend__alice.der
```

Evaluating ABAC: Running the prover

In English:

Is Alice a friend of Bob?

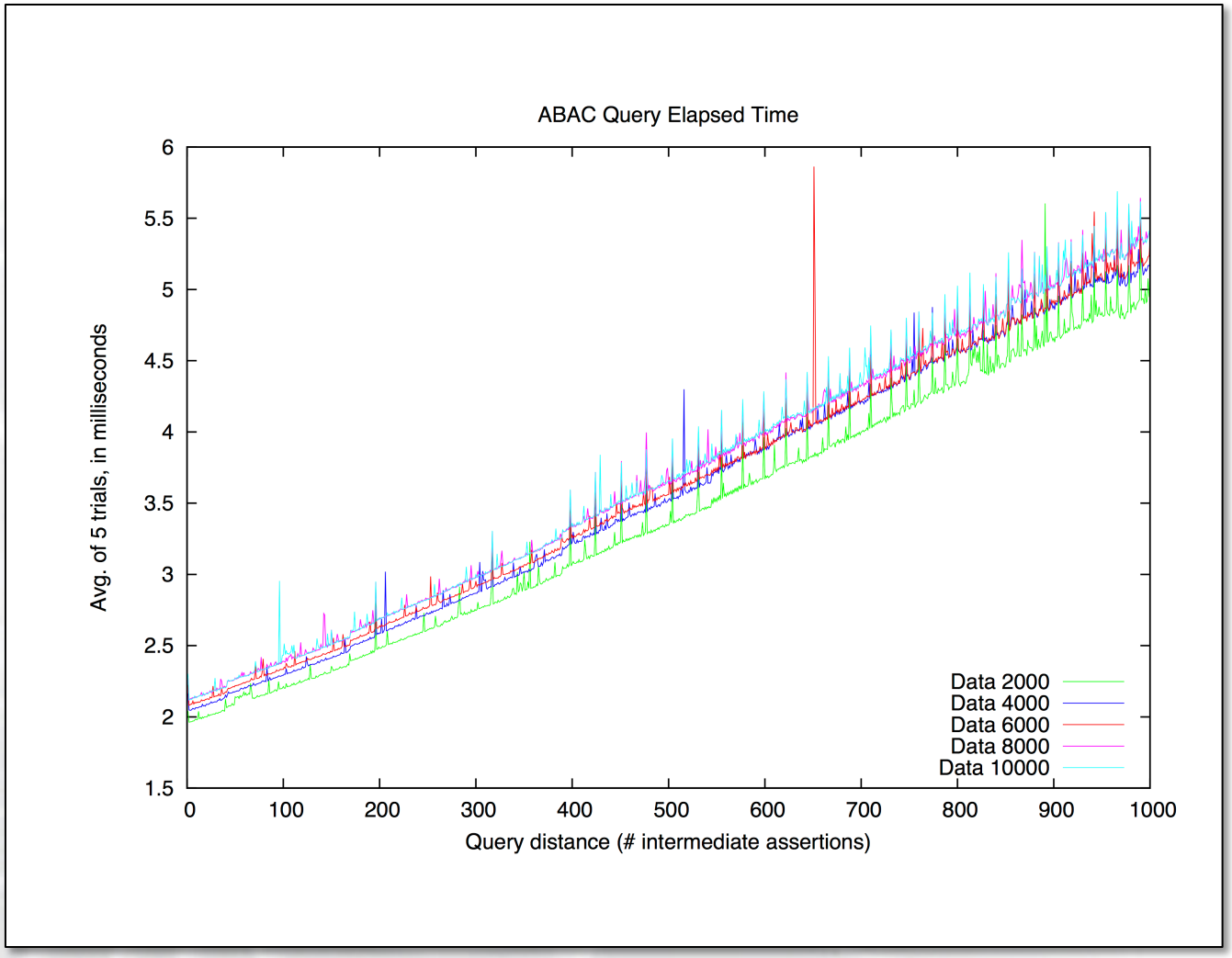
In ABAC:

Bob.friend $\stackrel{?}{\Leftarrow}$ Alice

In Python:

```
ctx = ABAC.Context()
ctx.load_directory('.')
principal_alice = Creddy.ID('alice_ID.pem')
principal_bob = Creddy.ID('bob_ID.pem')
role = str(principal_bob.key_id()) + ".friend"
ctx.query(role, principal_alice)
```

Evaluating ABAC: Prover Performance



ABAC: The Positives

- Allows policies of arbitrary complexity
  - Simple policies: Single attributes – “roles”
  - Moderate policies: A handful of attributes and/or assertions
    - “Is a member of project X”, “has write privileges on Slice Y”
  - Complex policies: Tens or hundreds of attributes and/or assertions
- Declarative and portable policies
- Logical proofs
- Partial chains

ABAC: The Negatives

- libabac is a work in progress
  - Under active development
  - Few users
  - Minimally field-tested
- RT1 & RT2 released March 6, 2012
  - Alpha code
  - Insufficient time to evaluate
- libabac does not improve interoperability
  - Little support for X.509 attribute certs
- Tools and infrastructure are in their infancy

Risks of Adopting ABAC

- Few examples to follow
  - How do we benefit from the experience of others?
- RT0 requires work-arounds:
  - RT1-lite
    - Replaces parameters with notational convention
    - Underscore represents separator between role and paramter
  - Template policies
    - Instantiated on the fly to create project-specific or slice-specific rules
  - RT1 & RT2 could help – is it ready?
- Some work remains…

Risks of Not Adopting ABAC

- Current GENI credentials are home-grown
  - Are they up to the task?
    - New AuthZ areas: Projects, I&M, Operations, Opt-In
  - How much effort is required to stretch the format?
- Forensics
  - How do we know what policies are in place?
    - Code inspection? Table-driven AuthZ library?
  - How do we know why someone was granted access?
    - Logging and manual inspection?

The End.