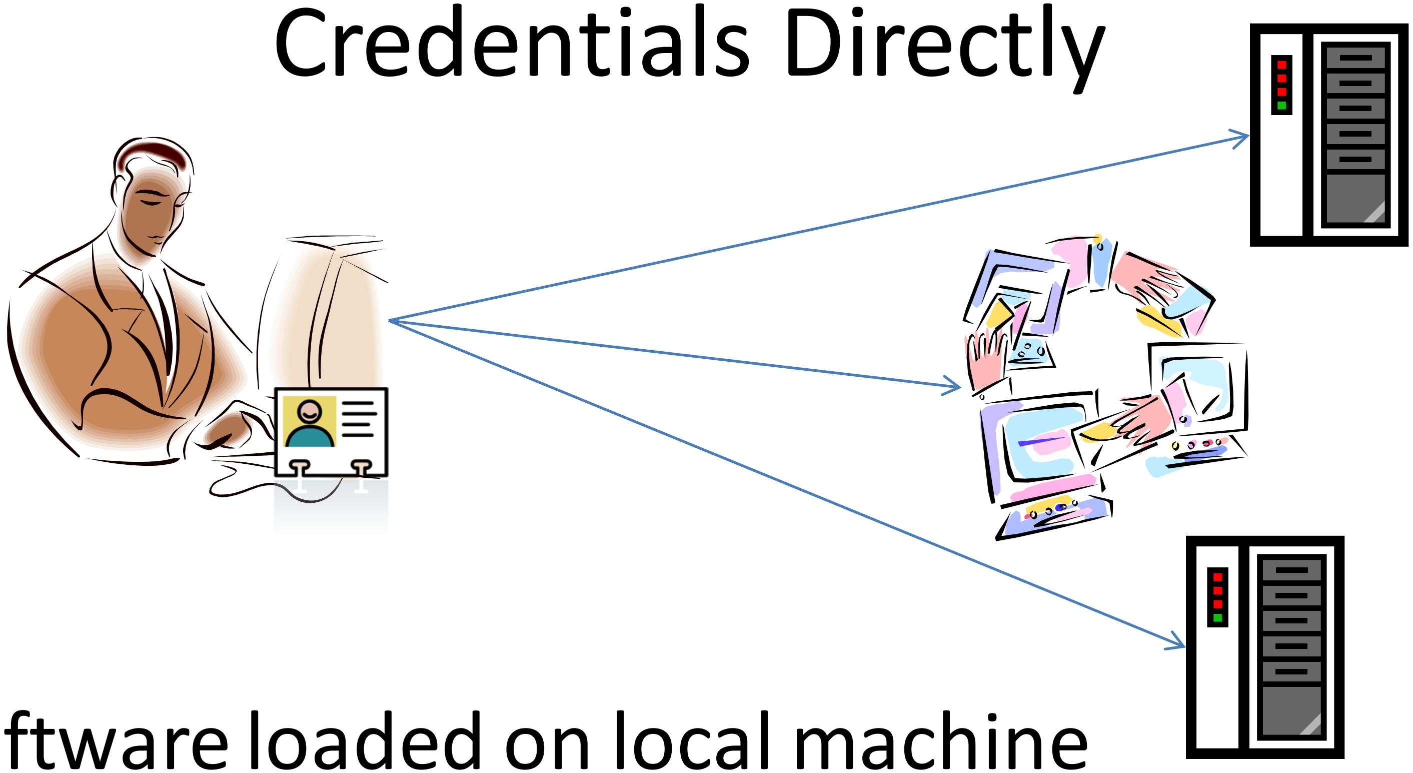
Speaks-for Delegation and ABAC

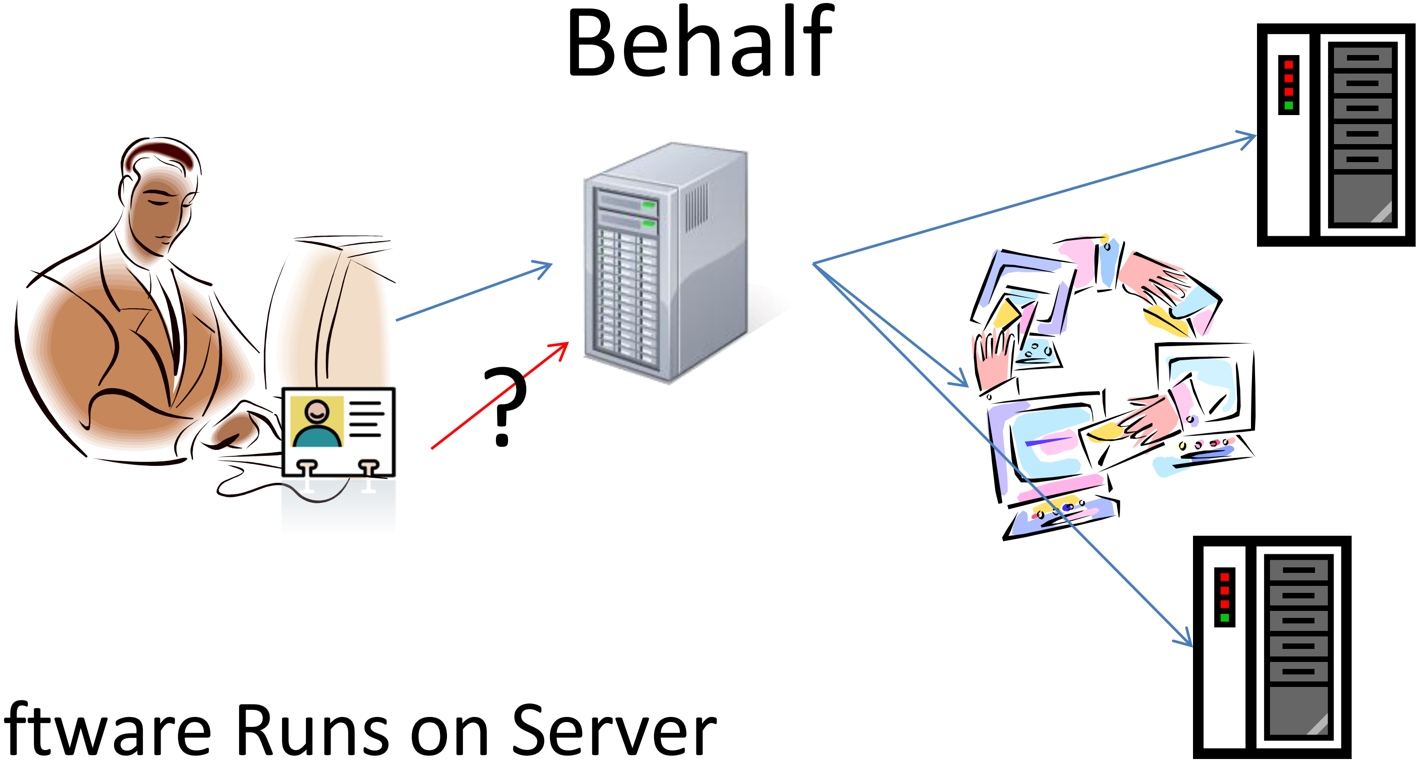
Ted Faber & Steve Schwab
USC/ISI

Local Tools Use Researchers Credentials Directly



- Software loaded on local machine
  - Researcher maintains software
- Researcher credentials secure on local storage

Hosted Tools Act on Researchers Behalf



- Software Runs on Server
  - Researcher accesses through browser
  - Minimal maintenance overhead
- How Is The Tool Authorized???

Speaks-for

- Giving a hosted tool the researcher's ID is dangerous…
- Speaks-for delegation
  - Researcher explicitly states tool may act for them
  - Statement is embodied in credential
  - Tool requests service saying "speaking for X"
- Can we do this in ABAC?

ABAC??

http://abac.deterlab.net

- An attribute-based authorization system that combines attributes using a simple reasoning system to provide authorization that
  - Expresses delegation and other authorization models efficiently and scalably
  - Allows access requesters and granters to control how much information they reveal
  - Provides auditing information that includes both the decision and reasoning
  - Supports multiple authentication frameworks as entry points into the attribute space

Speaks-for semantics in ABAC

- Write policy to support speaks-for
    - Slice authorities grant rights to Researcher and speaks-for folks
        - Interpret existing GENI credentials as ABAC statements
    - Researchers can issue speaks-for
    - Details: http://groups.geni.net/geni/wiki/TIEDCredentials

Speaks-for Credentials

- Libabac reads 2 kinds of signed XML:
  - GENI privilege credentials (slice credentials…)
  - Pure ABAC credentials (ABAC assertions)
- Speaks-for as privilege credential
  - Existing base of code generation
  - Minimal or no API changes
- Speaks-for as Pure ABAC
  - Flexible in the long term (scoping)
  - Libabac produces these credentials

ABAC Improvements

- Library improvements
  - more robust
  - better documented
  - Imports/exports XML formats
    - Including existing GENI credentials
- Policy specification (previous page)
- Prototype speaks-for implementation
  - Marshall did the implementation

Next Steps

- Standardize Speaks-for format
  - GENI privilege?
  - GENI ABAC (current prototype)?
- Credential generation in browser
  - ProtoGENI prototype
- Move to production…