Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities

Phuong Cao (PI), Jim Basney, Ravishankar Iyer, Anita Nikolich

https://pmcao.github.io/projects/nsf-2319190

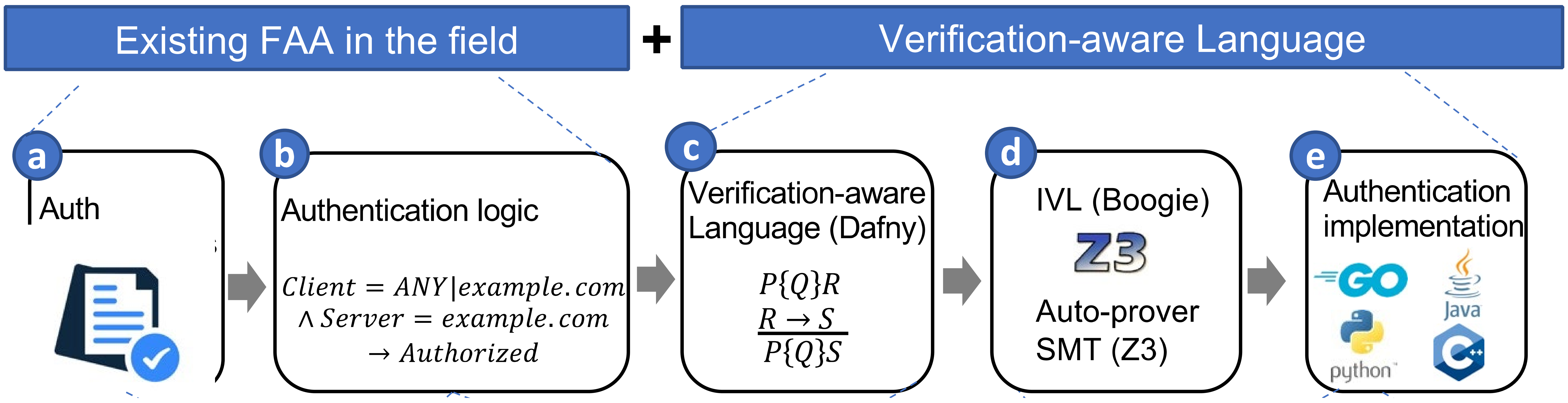
ILLINOIS NCSA | National Center for Supercomputing Applications

CSL

ILLINOIS iSchool

FABRIC

TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE



Existing FAA in the field + Verification-aware Language

a Auth

b Authentication logic

$Client = ANY|example.com$
$\wedge\ Server = example.com$
$\rightarrow Authorized$

c Verification-aware Language (Dafny)

$$\frac{P\{Q\}R \quad R \rightarrow S}{P\{Q\}S}$$

d IVL (Boogie)

Z3

Auto-prover SMT (Z3)

e Authentication implementation

FAA: Federated Authentication and Authorization

Challenges:

- Informal natural language specifications
- Complicated federated authentication logic
- Wide developer experience spectrum w.r.t security knowledge
- Operational, albeit unclear memory safety model in existing implementations
- Significant effort in validating downstream implementations upon specs revision

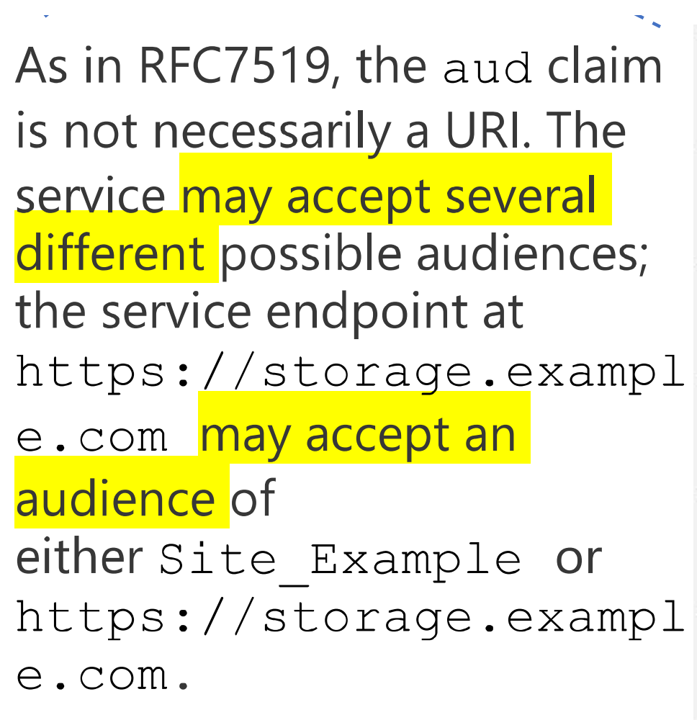
Scientific Impact

- Identified novel threat, failures, and uncertainty of security alerts affecting federated authentication infrastructure [IEEE QCE'24, IEEE DependSys'20, USENIX Security'24]
- Formalized a subset of critical authentication functions, using Dafny, in token-based authentication based on SciTokens and FABRIC Testbed Credential Manager [Github]
- Automated program synthesis of such implementation in Python, Java, and Rust [Github]
- Security testbed for reproducing authentication-related attacks [Secure-HPC Workshop @ Supercomputing'24]

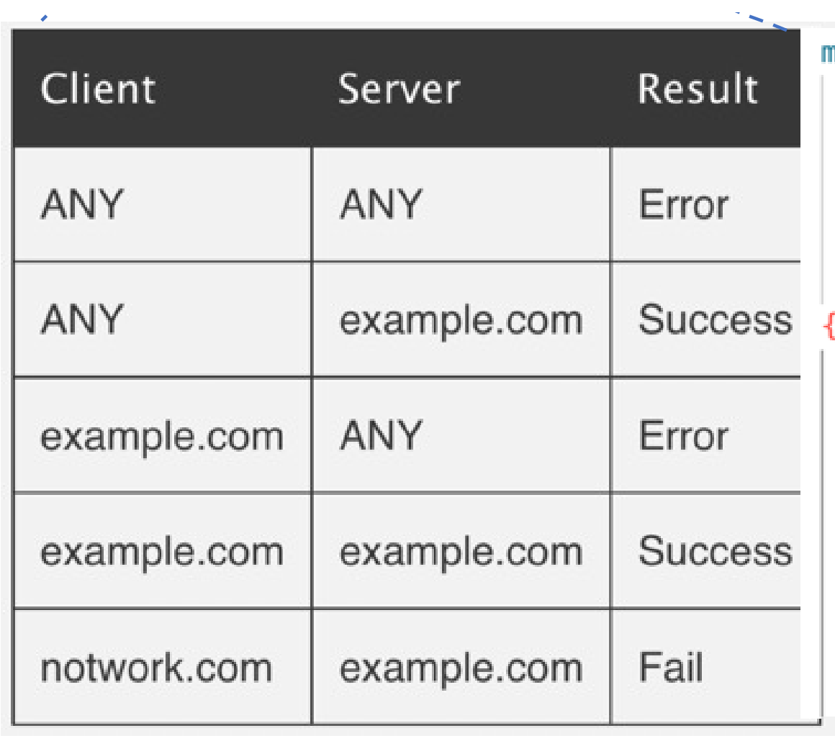
Technical Approach Demonstration

Input:

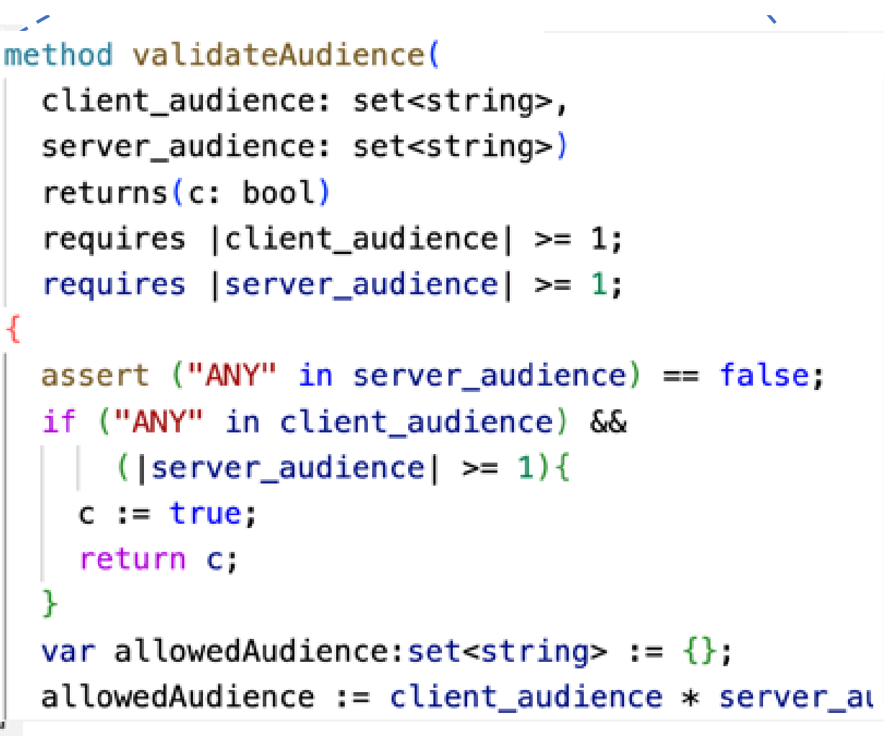
- *SciTokens specs*
- *Source repositories*
  - *SciTokens Python*
  - *FABRIC credential manager*
- *Knowledge of experts in SciTokens and FABRIC*



As in RFC7519, the `aud` claim is not necessarily a URI. The service may accept several different possible audiences; the service endpoint at `https://storage.example.com` may accept an audience of either `Site_Example` or `https://storage.example.com`.

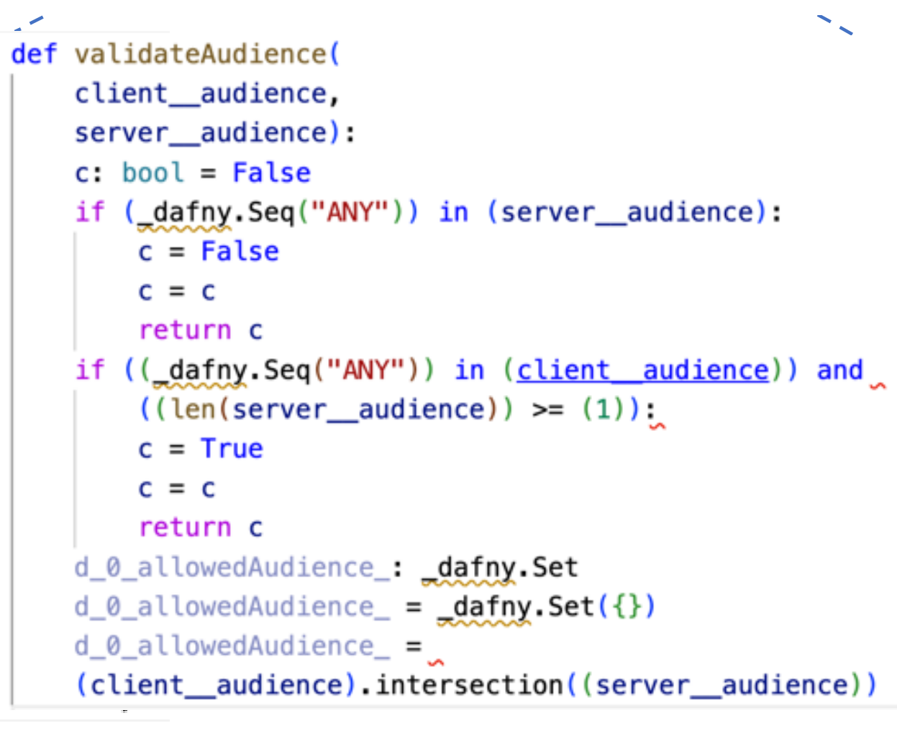


Client	Server	Result
ANY	ANY	Error
ANY	example.com	Success
example.com	ANY	Error
example.com	example.com	Success
notwork.com	example.com	Fail



```
method validateAudience(
  client_audience: set<string>,
  server_audience: set<string>)
  returns(c: bool)
  requires |client_audience| >= 1;
  requires |server_audience| >= 1;
{

  assert ("ANY" in server_audience) == false;
  if ("ANY" in client_audience) &&
     (|server_audience| >= 1){
    c := true;
    return c;
  }
  var allowedAudience:set<string> := {};
  allowedAudience := client_audience * server_au
```



```
def validateAudience(
    client__audience,
    server__audience):
    c: bool = False
    if (_dafny.Seq("ANY")) in (server__audience):
        c = False
        c = c
        return c
    if ((_dafny.Seq("ANY")) in (client__audience)) and
        ((len(server__audience)) >= (1)):
        c = True
        c = c
        return c
    d_0_allowedAudience_: _dafny.Set
    d_0_allowedAudience_ = _dafny.Set({})
    d_0_allowedAudience_ =
    (client__audience).intersection((server__audience))
```

Output

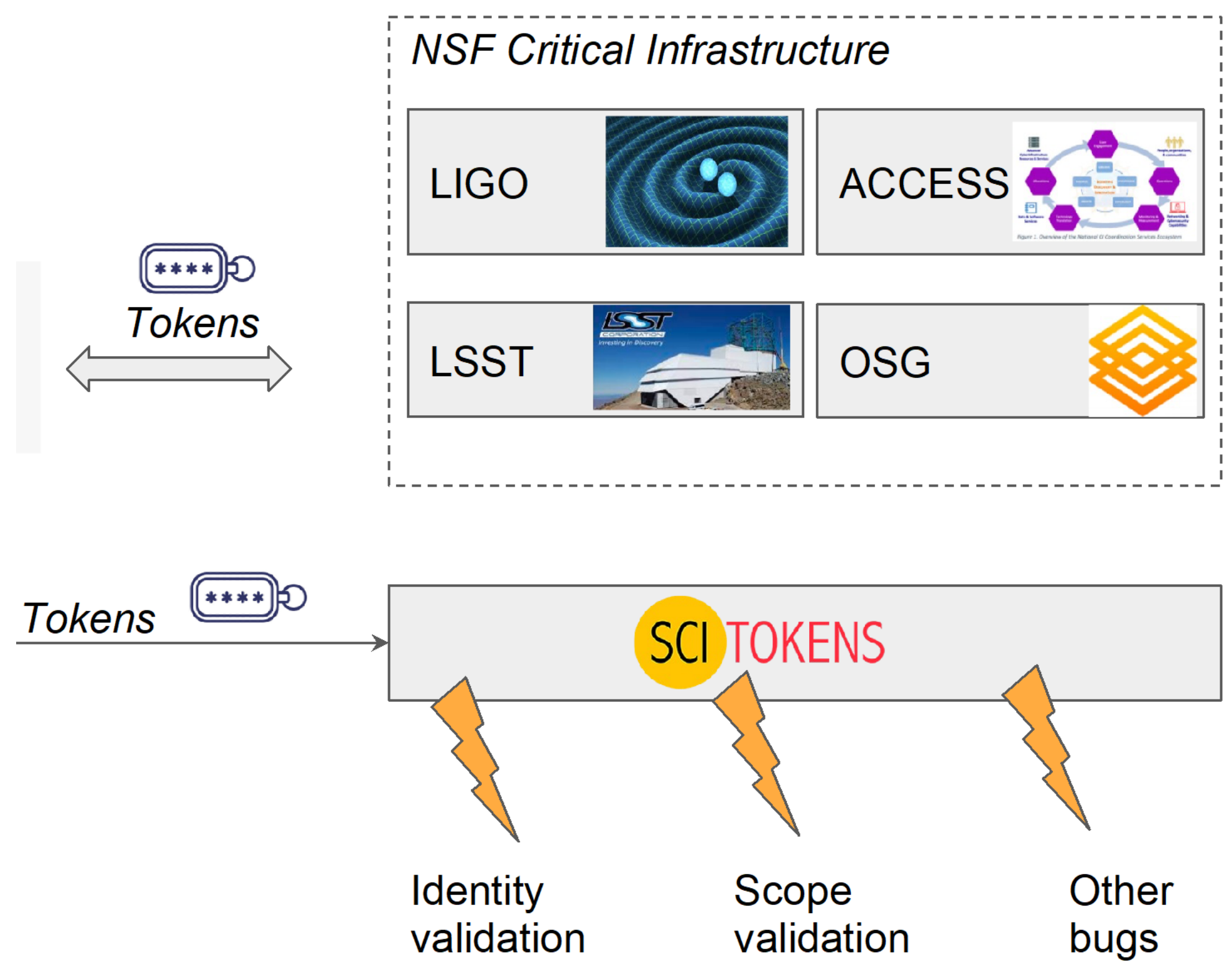
- *Verified correct implementation of scoping, caching functionalities in SciTokens Python*
- *Synthesized implementations in Python, Rust, and Java*

Feedback to Federated Authentication & Authorization (FAA) development team

Report UNSAT (bugs)

Correct implementation

Impact on NSF Cyberinfrastructure



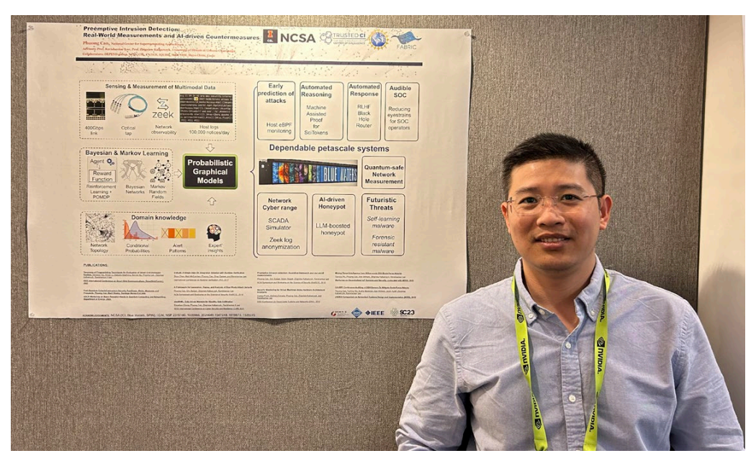
[NSF Research Infrastructure Workshop '24]

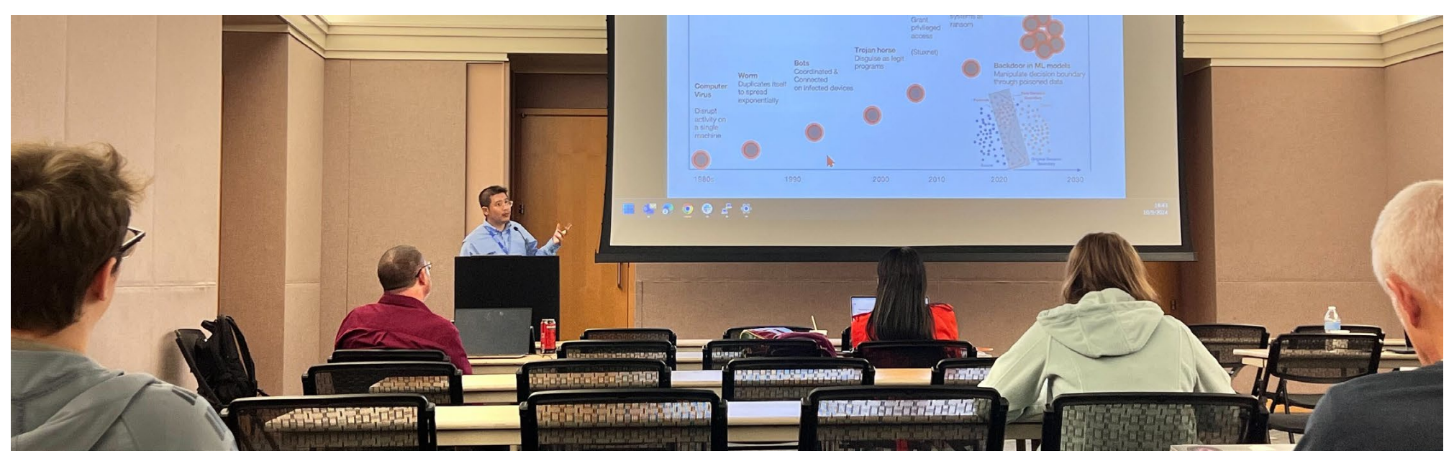
Impact on Security Operators

- Quantitative survey of security staff attending Supercomputing, NSF Cybersecurity Summit, and IEEE QCE
- Seminar on federated authentication and authorization in TrustedCI Webminar
- Hands-on tutorial on security log analyses with National Center for Supercomputing Applications (NCSA) Incident Response Team, and attendees located at Berkeley Lab and CMU

Broadening Participation in K-12

- Explained Federated Authentication for K-12 students through interactive game at Carrie Busey Elementary Scientific Night





References

Complete bibliography are available on project page: https://pmcao.github.io/projects/nsf-2319190

The NSF Formal Methods in the Field PI Meeting (2024 FMitF PI Meeting)
November 12-13, 2024 | The University of Iowa | Iowa City, Iowa