C-BAS: Certificate-based AAA for SDN Experimental Facilities

Umar Toseef
Adel Zaalouk, Tom Rothe, Matthew Broadbent, Kostas Pentikousis

EWSDN 2014, Budapest, Hungary
September 3, 2014
Outline

- Motivation
- Problem statement
- Certificate based authentication
- ClearingHouse services
- C-BAS in SDN experimental facilities
- Conclusions
Motivation

- Secure and easy to use

- Large scale networks
  - Diverse device types
  - Different technologies

- Federation of SDN networks
  - Heterogeneous Experimental facilities federated through NSI-enabled networks
  - World-scale testbed for Future Internet research
  - Attractive business use-cases
Problems with current solutions

- Tight-coupling of AAA mechanisms
- Little reusability considerations
- Lack of a standard access interface
- Kerberos
- LDAP
Authentication using certificate

A. Provide private key
B. Create evidence
C. Send certificate & evidence over secured connection
D. Validate certificate and verify evidence
E. Authentication succeeded/failed

CA

Relying server
Authorization using credentials

Credentials

- Provide an owner with privileges on a target object
- Represent a set of assertions for authorization
- Digitally signed by issuer

C-BAS credential types

1. SFA (Slice Facility Architecture) credentials
2. ABAC (Attribute-Based Access Control) credentials
Privilege delegations

Delegation

Delegation

Speaks-for

Speaks-for

Speaks-as

Speaks-as
ClearingHouse services

- **Member Authority**
  - Manages and asserts attributes about particular members
  - Maintains a set of members, SSH & SSL keys and certificates
  - Keeps mapping of members to user-agent tools

- **Slice Authority**
  - Creates new slices, updating existing slice, maintains list of slices
  - Generates and offers slice credentials
ClearingHouse services

- **Service registry**
  - Maintains a list of registered services like MA, SA etc.

- **Project service**
  - Maintains list of projects
  - Asserts the existence of projects and the roles of members

- **Logging service**
  - Stores transaction details for accountability
ClearingHouse services

Member roles

- Lead
- Admin
- Member
- Auditor

Context: Slice / Project
C-BAS in SDN experimental facility

AM: Aggregate Manager
GAPI: GENI AM API
FAPI: Federation API
VPN: Virtual Private Network
LDAP: Lightweight Directory Access Protocol
Summary

- Currently deployed AAA solutions are not up to the requirements
- C-BAS is a certificate-based AAA architecture
  - Well-structured privileges system
  - Reusable in design
  - Flexible for extensions
  - Open to future evolutions
- C-BAS is viable and experimentally tested
- Legacy AAA mechanisms get seamless migration to C-BAS
THANK YOU FOR YOUR ATTENTION

Acknowledgement
This work was conducted within the framework of the FP7 projects ALIEN and FELIX, which are partially funded by the Commission of the European Union.

Umar Toseef
EUREF Campus Haus 13, Torgauer Straße 12-15
10829 Berlin
+49 30 3670 235 115
Umar.toseef@eict.de