A Research Project of InterSOC Cooperation b/w Keio and Hitachi

11/20/2017@Mita Campus, Keio Univ.

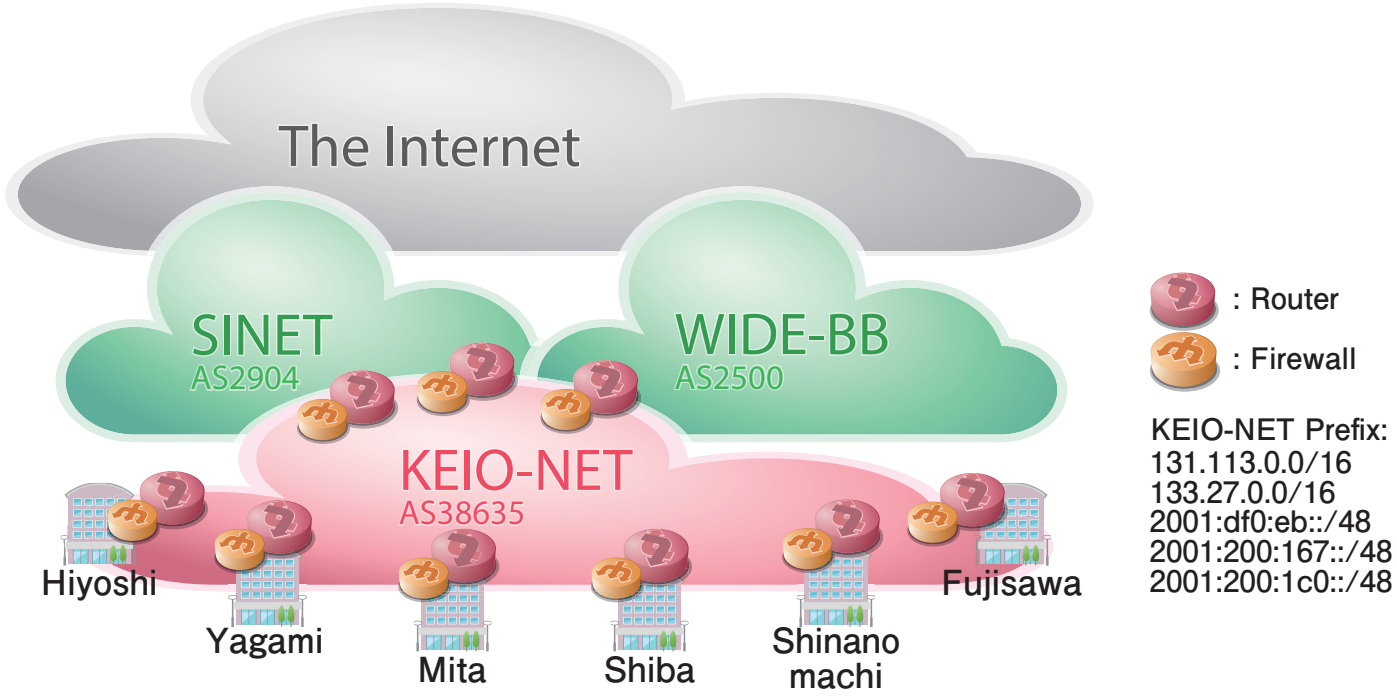
Graduate School of Science and Technology, Keio Univ.
Headquarters of Information Technology Center, Keio Univ.

Takao KONDO

latte@itc.keio.ac.jp

Security Operation in Keio Univ.

- KEIO-NET has 3 PoPs for upstream networks
  - For WIDE-BB: 1 PoP
  - For SINET: 2 PoPs
- Installed next generation firewalls at upstream networks boundary and campus boundary
  - Conducts application protocol analysis
  - Separates security zones by each campus (zero trust approach)



Features of University Networks

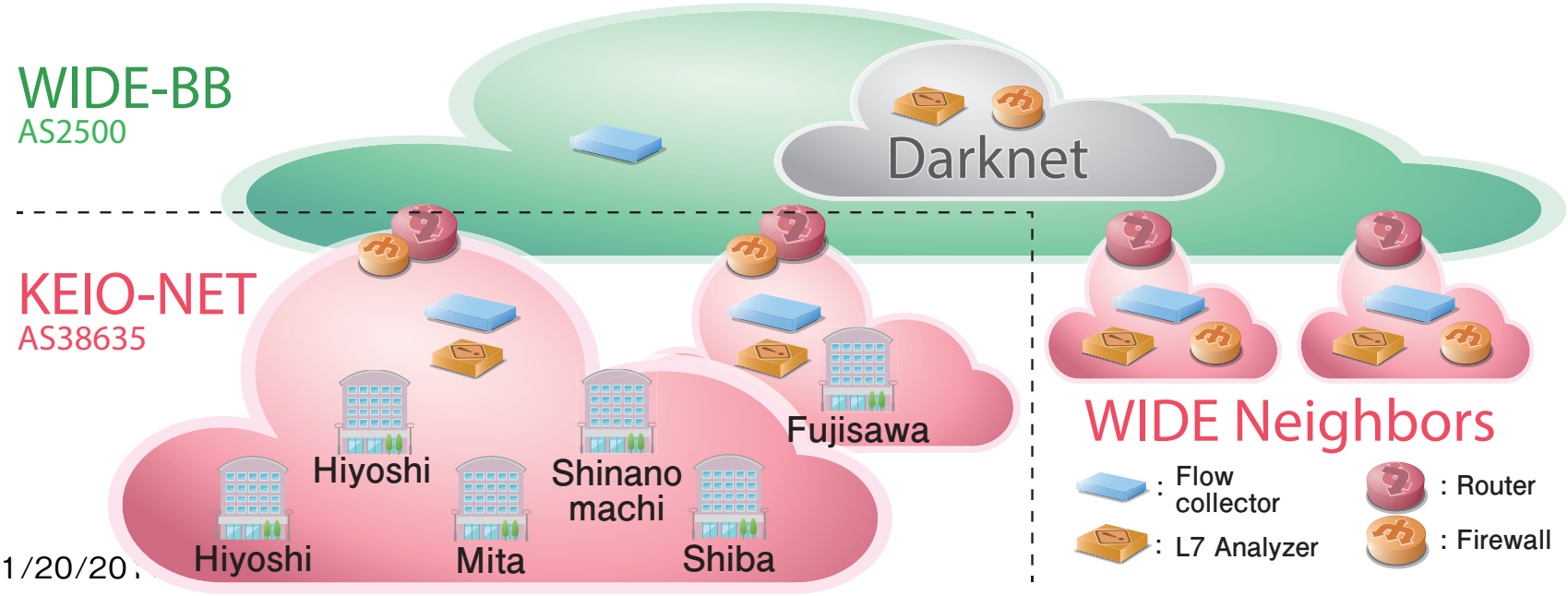
- Research and Education (RandE) networks
  - Assigned to each faculty and department
  - Basically, operated by the assigned faculty and department (due to regard for research and education activities)
  - Information Technology Center (ITC) monitors RandE network traffic by FWs

- Administration (Adst) networks
  - Assigned to administration offices
  - Basically, operated by ITC
  - ITC installed full-stacks security software (TLS proxy, Mail security, vulnerability scanner etc.) into the Adst networks

Necessary to suppress too much security scan in RandE networks

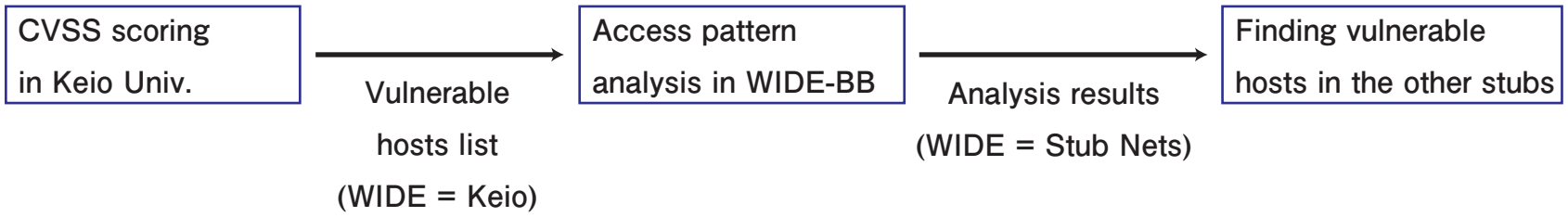
Keio SOC / WIDE SOC

- WIDE-BB: nationwide RandE backbone network
  - Operational and experimental network
  - Commodity traffic and Darknet traffic can be captured
- KEIO-NET: Service network in Keio Univ.
  - Flow info (5 tuples) analysis, L7 analysis by FWs



Use-cases of InterSOC Cooperation

- Vulnerable hosts list (stub => upstream)
  - E.g., Hosts which have bad CVSS score



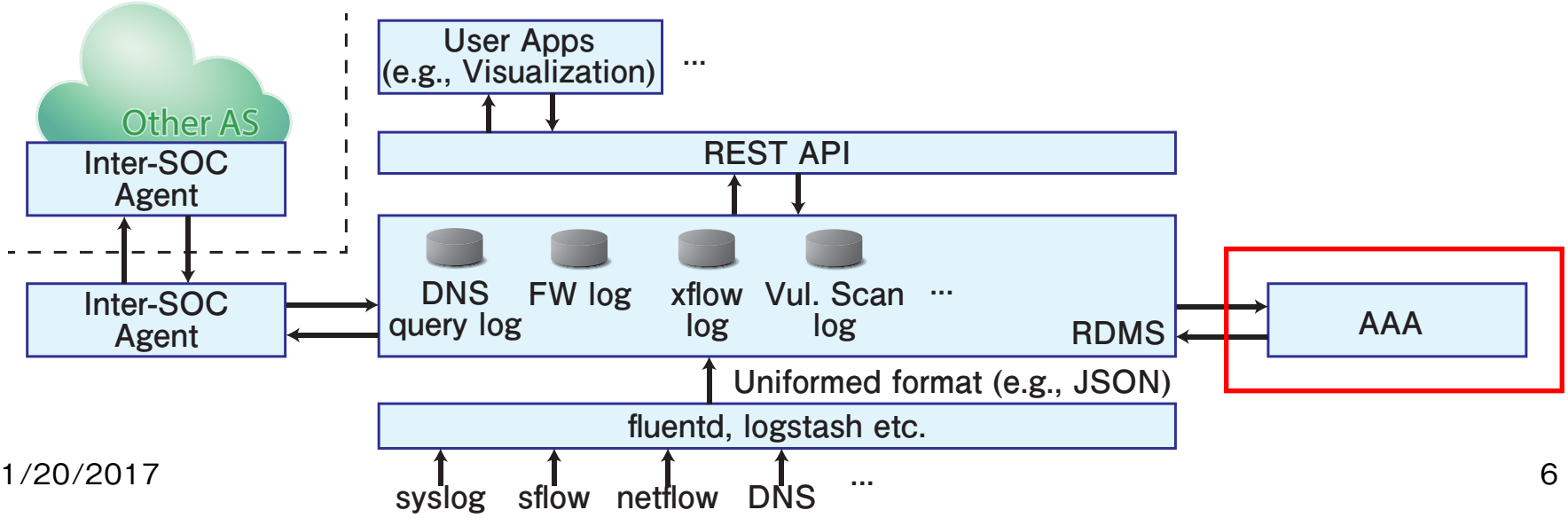
- Darknet analysis result (upstream => stub)
  - Early threat warning:
    (e.g., the num of dst port 445 accesses shapely raised about two weeks before the world first affected report of WannaCry.

Necessary to conduct access control for cooperation

InterSOC Modules Overview

- AAA agent conducts access control of gathered info.
  - In User Apps, InterSOC cooporation
- Uniformed format in DB input/output
  - For flexible changing of gathering info.
  - E.g., Fluentd, logstash etc.

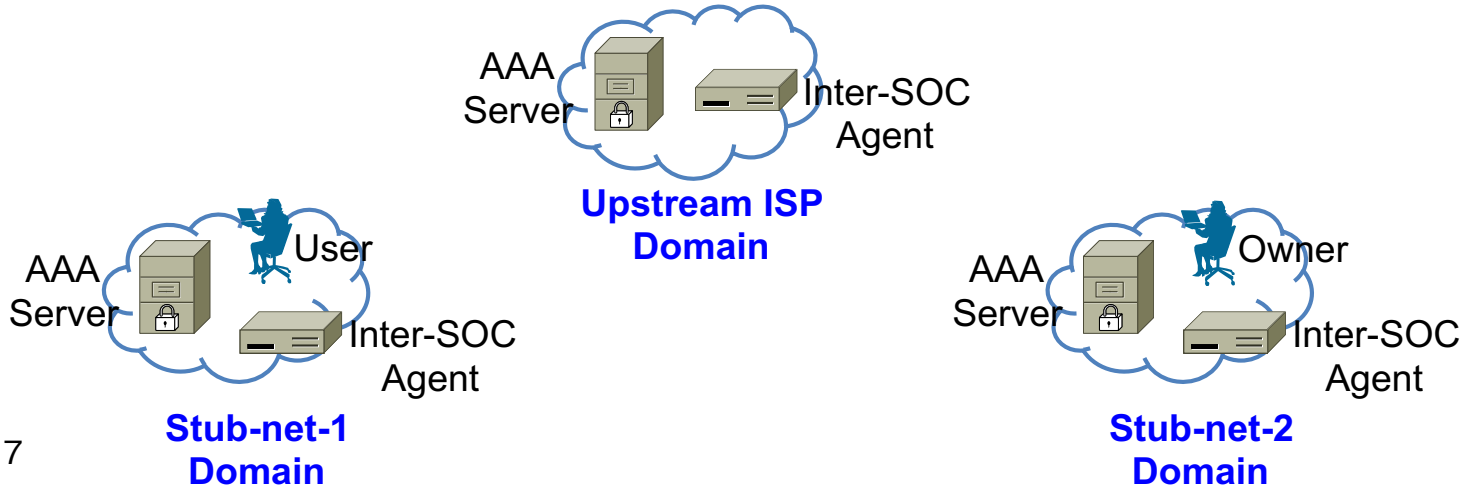
- SOCs are communicated via InterSOC Agents
  - For hide the actual DB from external entities
- User Apps retrieve gathered info via REST API



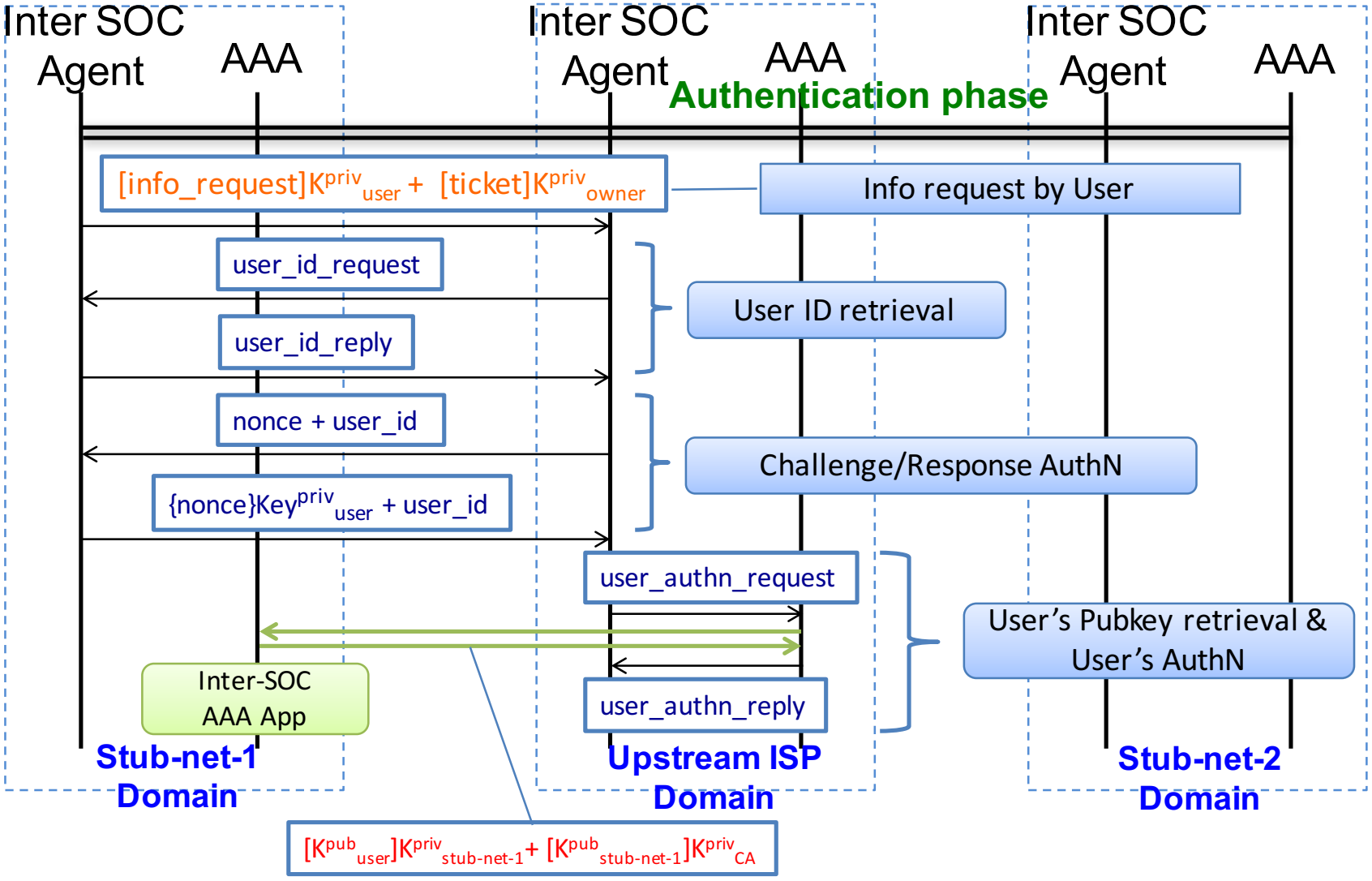
Assumed Environment

- Public Key Infrastructure (PKI) is available
- AAA Server in each domain stores:
  - its domain's public key signed by CA
  - its members' public keys signed by domain AAA server
- Inter-domain routing of AAA signaling
  - Requirements: policies b/w domains, scalability

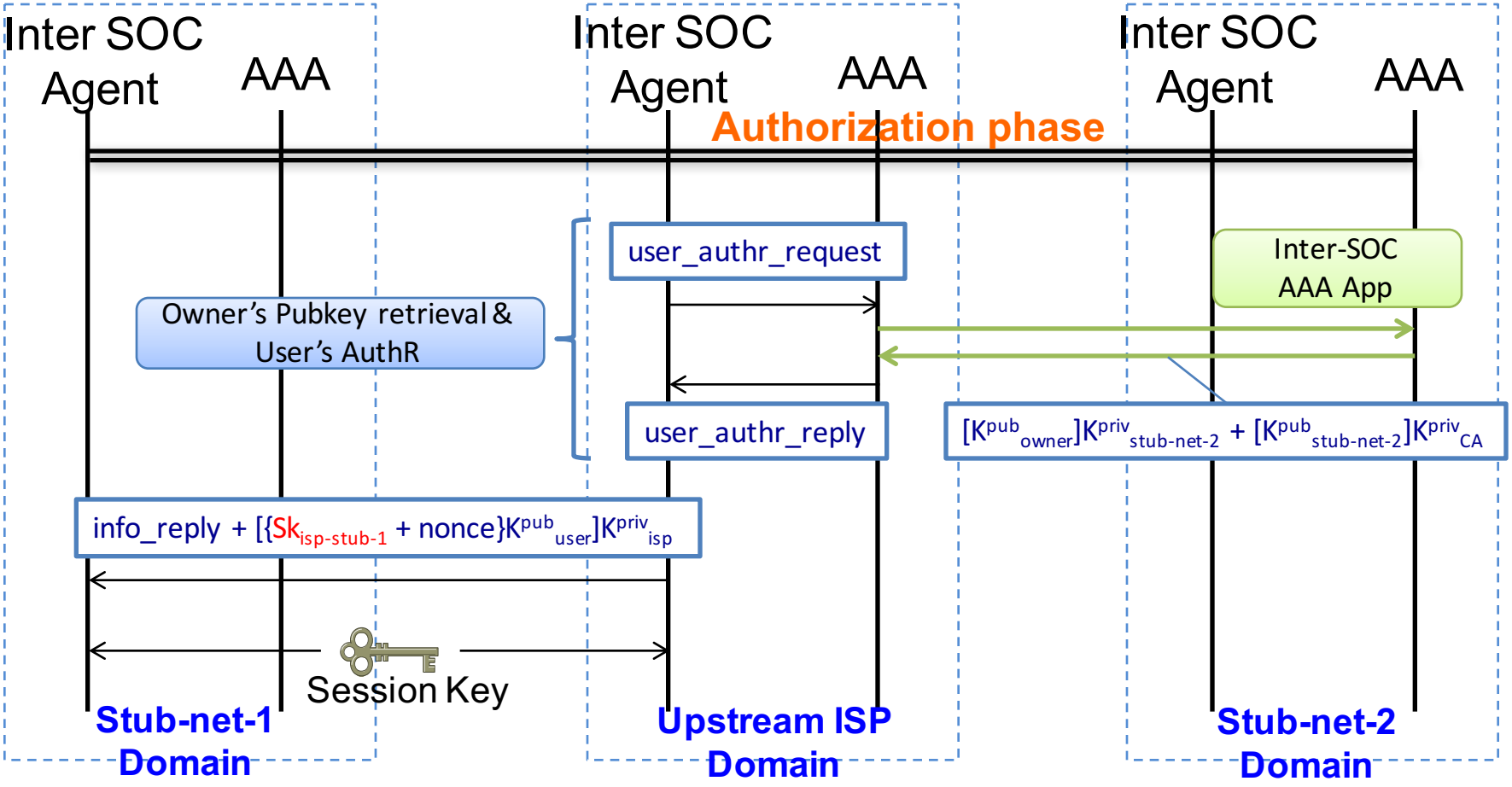
- Ticket-based Access Control System
  - Access Control List (ACL) is distributed as Ticket to each User
  - Ticket contains: Subject, Action, Resource, Valid time
  - Ticket is signed by Owner and pre-distributed to User



User Authentication Procedures



User Authorization Procedures



Related Work

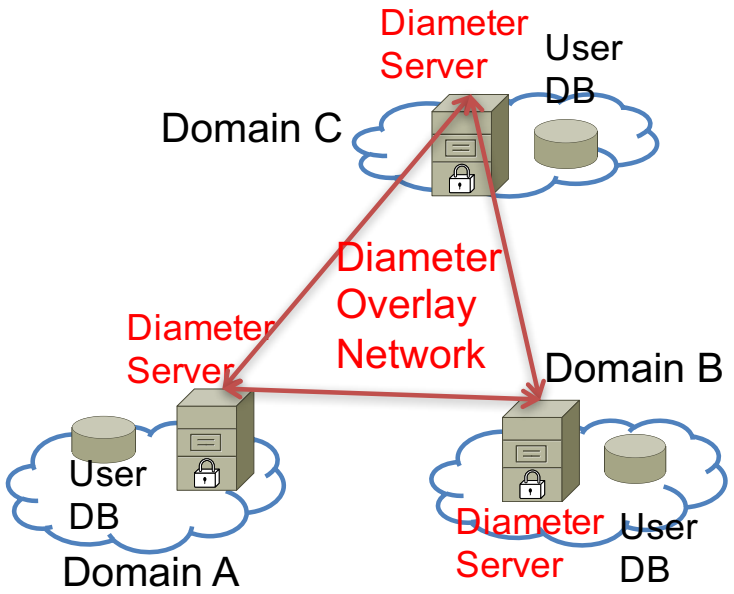
- Access control per content
  - Authenticated / authorized users can (i) know existence of content, (ii) retrieve content
- Access control based on multi-domain routing
  - AAA signaling mechanism on multi-domain overlay
- Scalability
  - The num of content files and domains

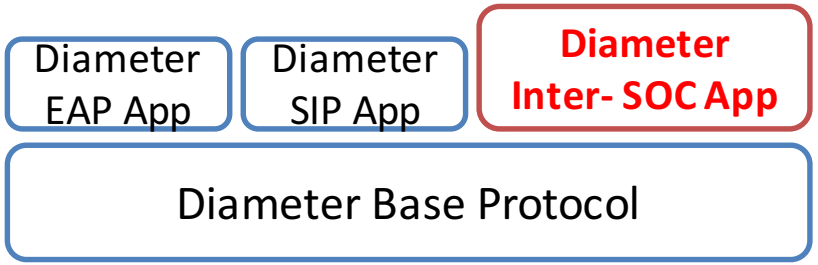
	Kerberos [1]	Shibboleth[2]	RADIUS[3]	Diameter Inter-SOC App
Per-content	yes	yes	yes	yes
Multi-domain routing	yes	yes	no	yes
Scalability	No[4]	no	no	yes

[1] C. Neuman et.al., "Kerberos: An Authentication Service for Computer Networks", In Proc. of IEEE Communications Magazine, 1994, pp. 33 – 38
[2] W. Jie et.al., "A Guanxi Shibboleth based Security Infrastructure", In Proc. of IEEE EDOC WKSHPS'08, 2008, pp. 151 – 158
[3] C. Rigney et.al., " Remote Authentication Dial In User Service (RADIUS)", RFC2138, IETF, 2000
[4] S. Sakane et.al., " Problem Statement on the Cross-Realm Operation of Kerberos." RFC5868, IETF, 2010

AAA Protocol "Diameter"

- Diameter base protocol
  - Exchange AAA related information safely
  - For signaling in Multi-domain Environment
- Diameter application
  - Extension of Diameter base protocol extension
  - Defines diameter message format for carrying app. specific data
  - e.g., Diameter EAP App. (AuthN and AuthZ for network access)





Diameter Inter-SOC Application

- Diameter message: Command + AVPs
  - Command code: specifies action when Diameter message is received
  - AVP (Attribute Value Pair): stores data delivered by command
- New command of Diameter InterSOC App.
  - Public key Request/Answer Command for AuthN & AuthZ

- New AVP of Diameter InterSOC App
  - Carry AuthN & AuthZ information
  - Public key Request Command
    - Origin-Host AVP, Origin-Realm AVP, Destination-Realm AVP, User-name AVP, Session ID AVP,
  - Public key Answer Command
    - Origin-Host AVP, Origin-Realm AVP, Session ID AVP, Public-key AVP

Conclusion

- Security operation in Keio Univ.
  - Installed next generation firewalls at upstream networks boundary and campus boundary
  - Necessary to suppress too match payload scan in RandE networks

- InterSOC cooperation system
  - AAA agent conducts access control of gathered info.
  - Uniformed format in DB input/output
  - SOCs are communicated via InterSOC Agents
  - User Apps retrieve gathered info via REST API