ACHILLES: Access **C**ontrol and aut**H**entica**I**on de**L**egation for interoperab**LE** IoT application**S**

Athens University of Economics and Business – Research Center (AUEB)

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

About us

Mobile Multimedia Laboratory
Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business

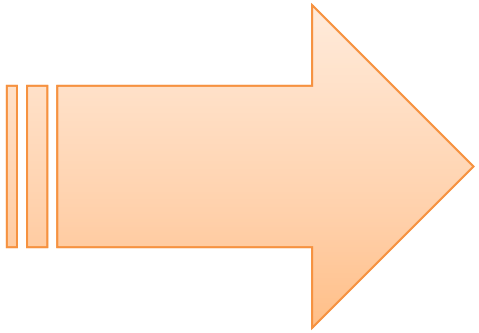
About us

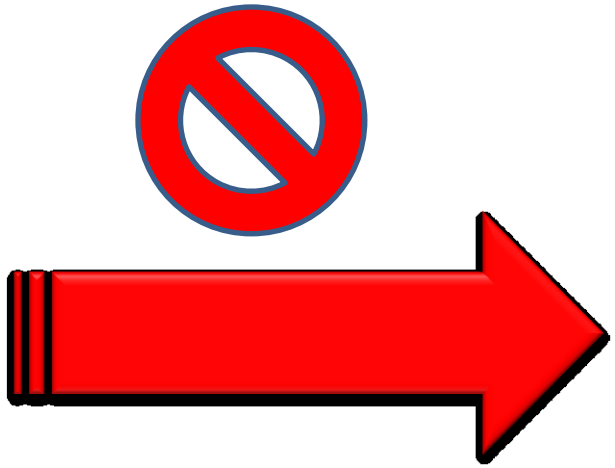
Prof. George C. Polyzos

Dr. Nikos Fotiou

ACHILLES use case

SMART PORT





Additional constrains

- Devices (usually) have limited computational power
  - No support for PKE, D-H
- Devices can be easily tampered with
  - Not the best location to store “important” secrets
- Devices are not always connected to the Internet
  - Key management becomes harder

How this problem is typically solved?

Container 1 wants to access
- Your role

OK Cancel

How this problem is typically solved?

If role == ”port employee” then

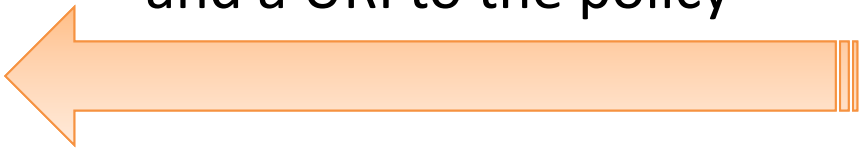
….

Authentication and authorization for interoperable IoT architectures

OUR SOLUTION

“Hi, I want to register container X with you, only your employees can access it”

“Of course, here is a secret key and a URI to the policy”

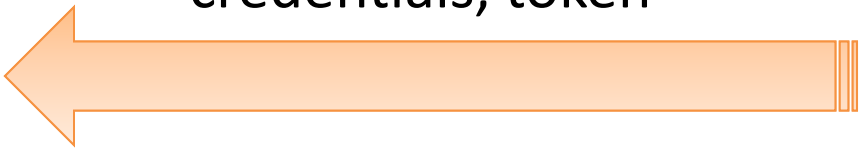


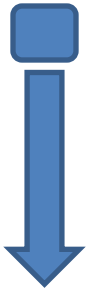
“secret key, URI to policy”

Hello

“URI to policy, token”

"I want to access container X, credentials, token"





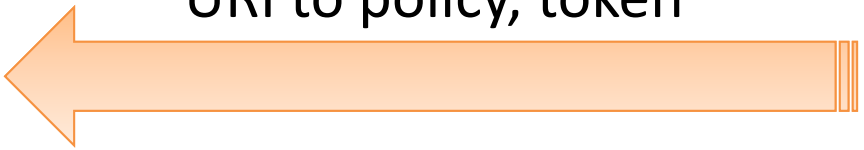
Token

HMAC

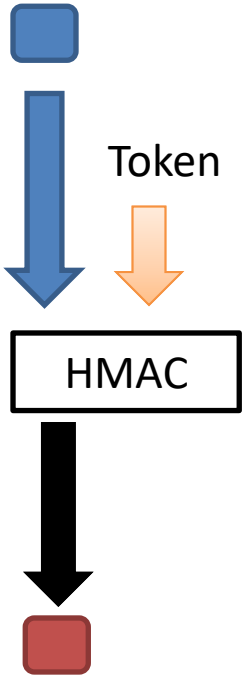
Hello

“URI to policy, token”

“URI to policy, token”



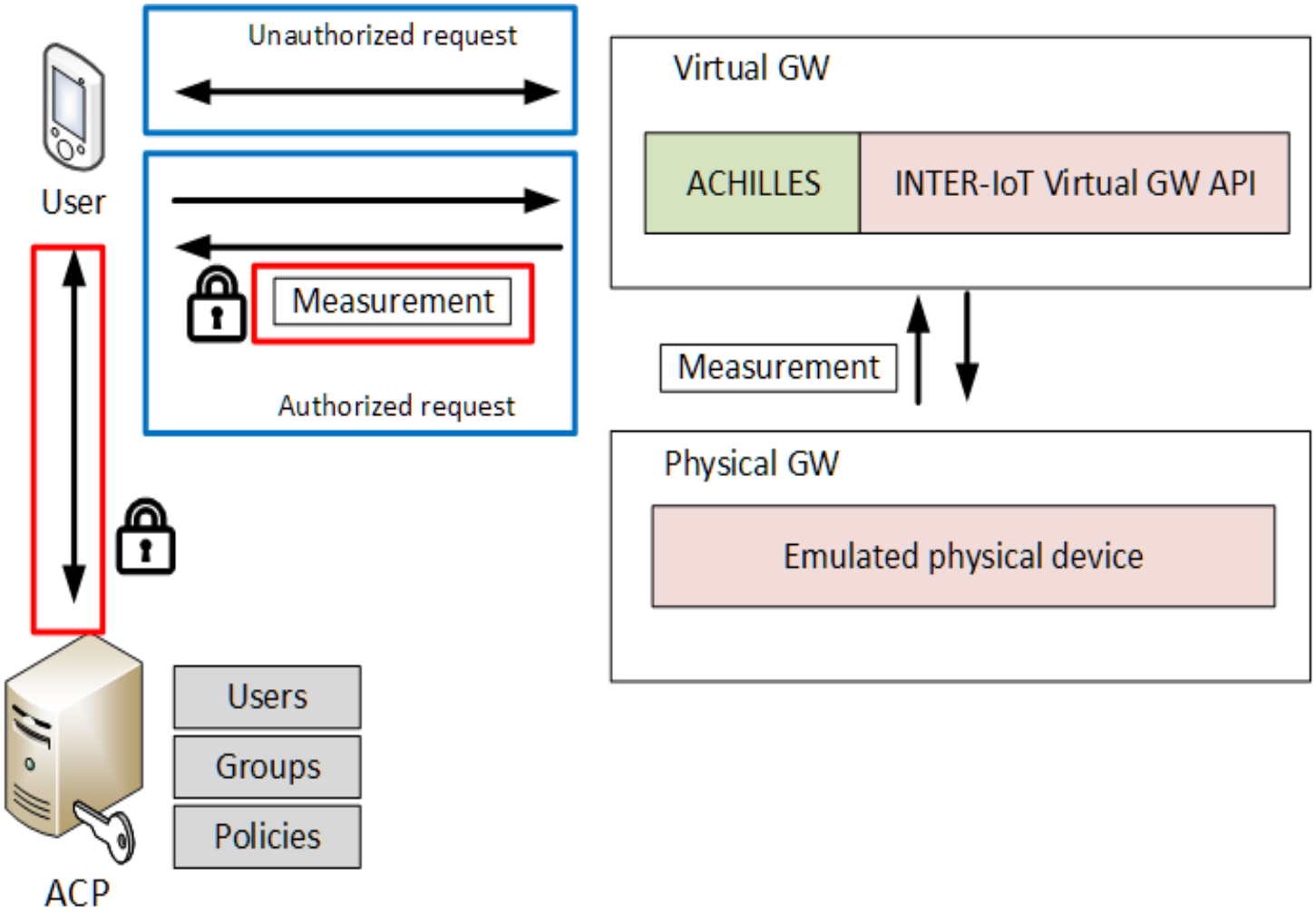
“Token”


Token
HMAC

Advantages

- Things have no access to user-sensitive information
- Things to do not have to understand business logic, access control policies
- User management systems do not have to be aware that a user interacts with a Thing
  - Not IoT specific solution
- Security management does not involve communication with the Things
- New business opportunities
- Damage control in case a secret key is compromised

INTEGRATION WITH THE INTER-IOT GATEWAY


Unauthorized request
User
Measurement
Authorized request
Virtual GW
ACHILLES
INTER-IoT Virtual GW API
Measurement
Physical GW
Emulated physical device
Users
Groups
Policies
ACP

DISSEMINATION ACTIVITIES

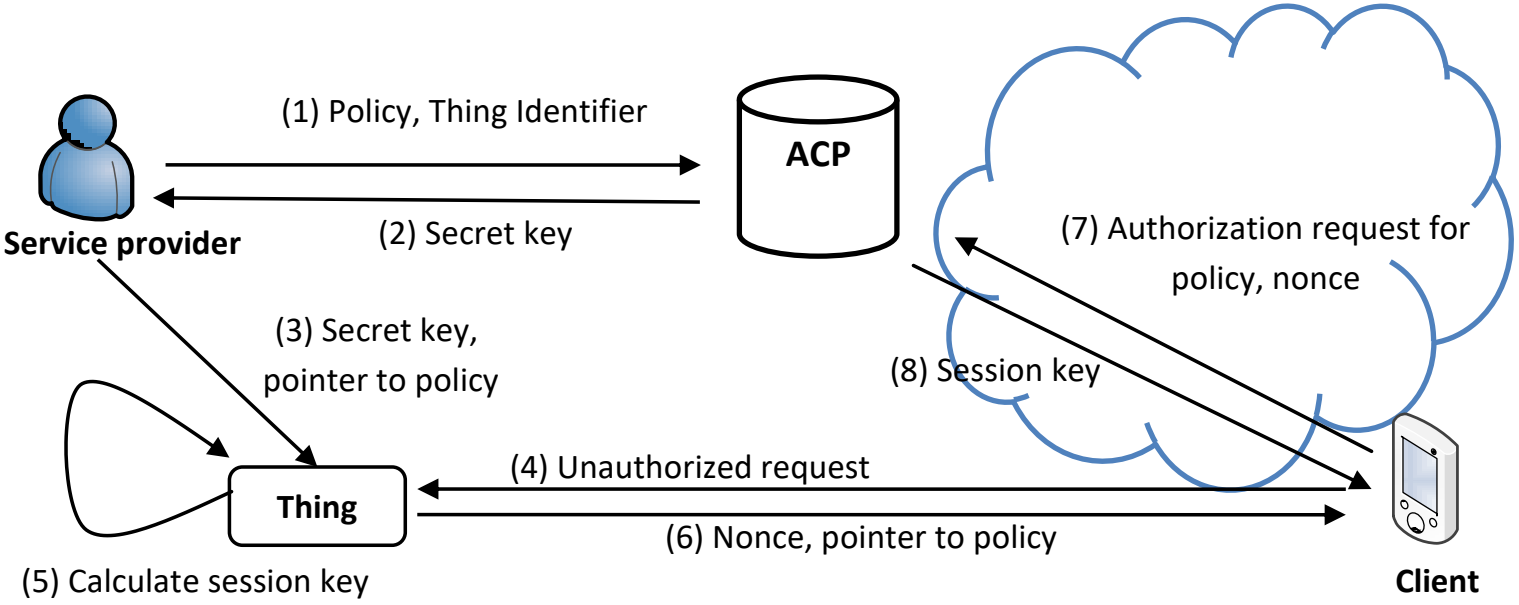
Publications

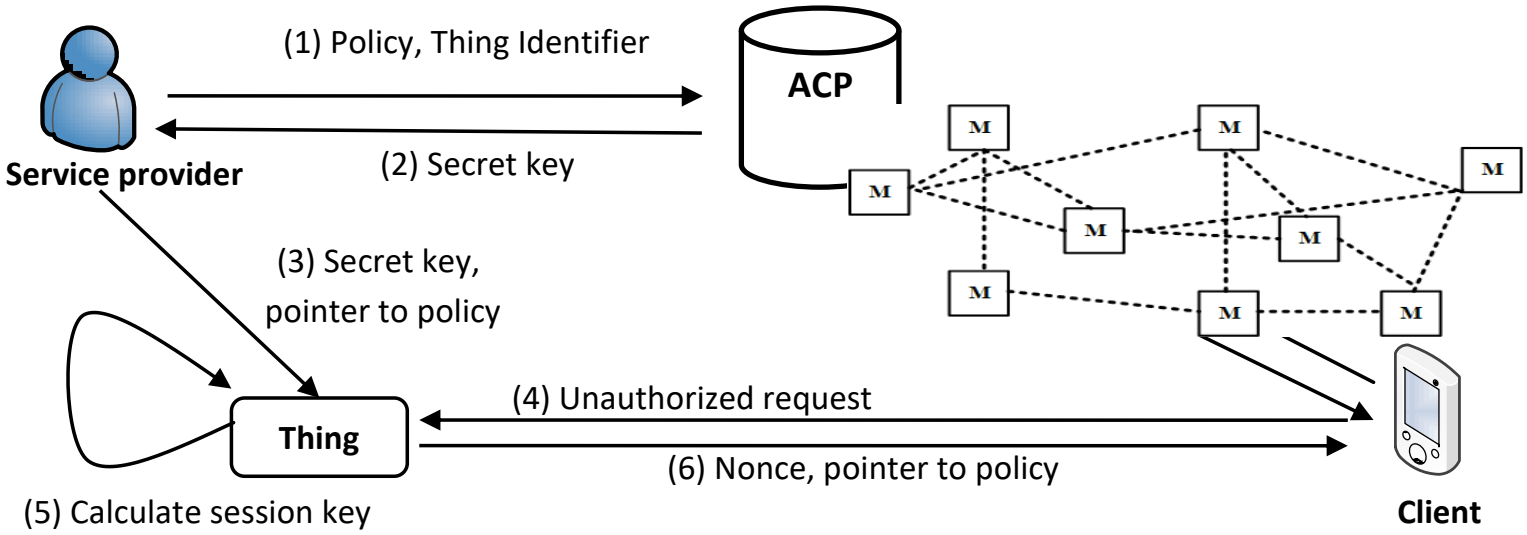
- N. Fotiou and G.C Polyzos, “Authentication and authorization for interoperable IoT architectures,” in Proc. 1st International Workshop on Emerging Technologies for Authorization and Authentication (Co-Located with ESORICS 2018)
- S. Lepeniotis, “Access control policy definition using XACML,” MSc. Thesis
- D. Mermigas, “Access control providers and their use in access control systems” Dipl. thesis

Presentations

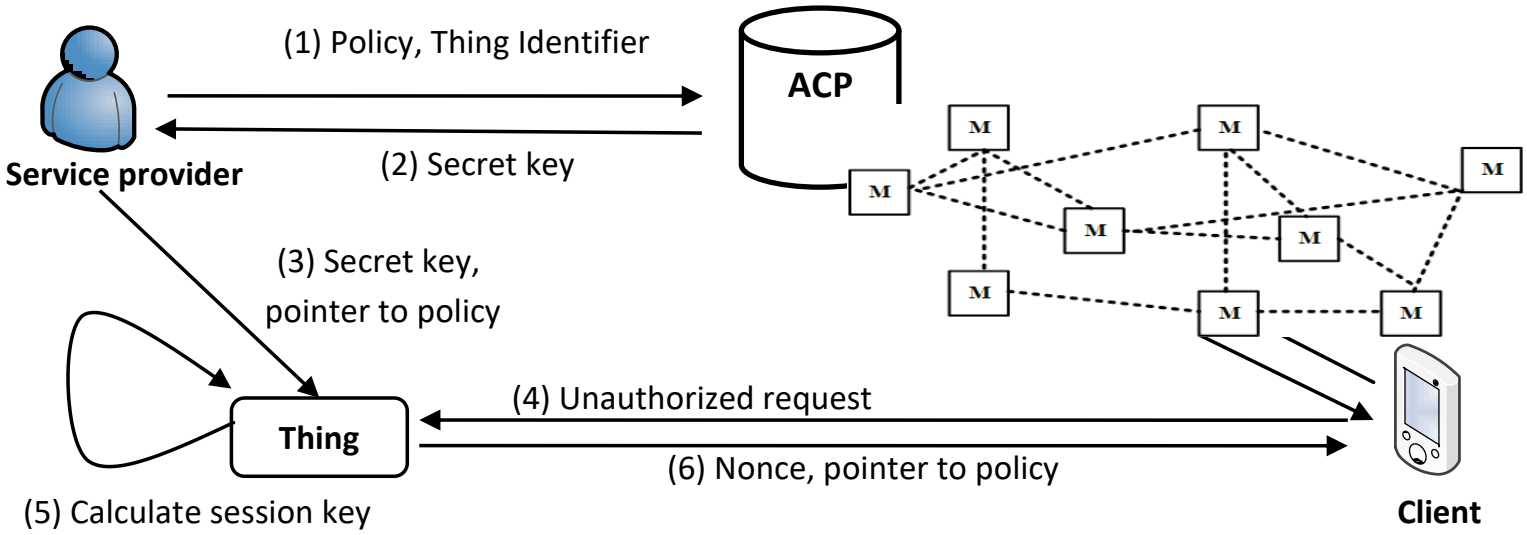
- Introductory presentation during AUEB's new building inauguration
- Presentation at the Athens Center for Entrepreneurship and Innovation

FOLLOW UP


(1) Policy, Thing Identifier
ACP
(2) Secret key
Service provider
(7) Authorization request for policy, nonce
(3) Secret key, pointer to policy
(8) Session key
(4) Unauthorized request
Thing
(6) Nonce, pointer to policy
(5) Calculate session key
Client


(1) Policy, Thing Identifier
ACP
Service provider
(2) Secret key
M
(3) Secret key,
pointer to policy
(4) Unauthorized request
Thing
(6) Nonce, pointer to policy
(5) Calculate session key
Client

SOFIE https://www.sofie-iot.eu



Thank you

https://mm.aueb.gr/achilles

fotiou@aueb.gr

polyzos@aueb.gr