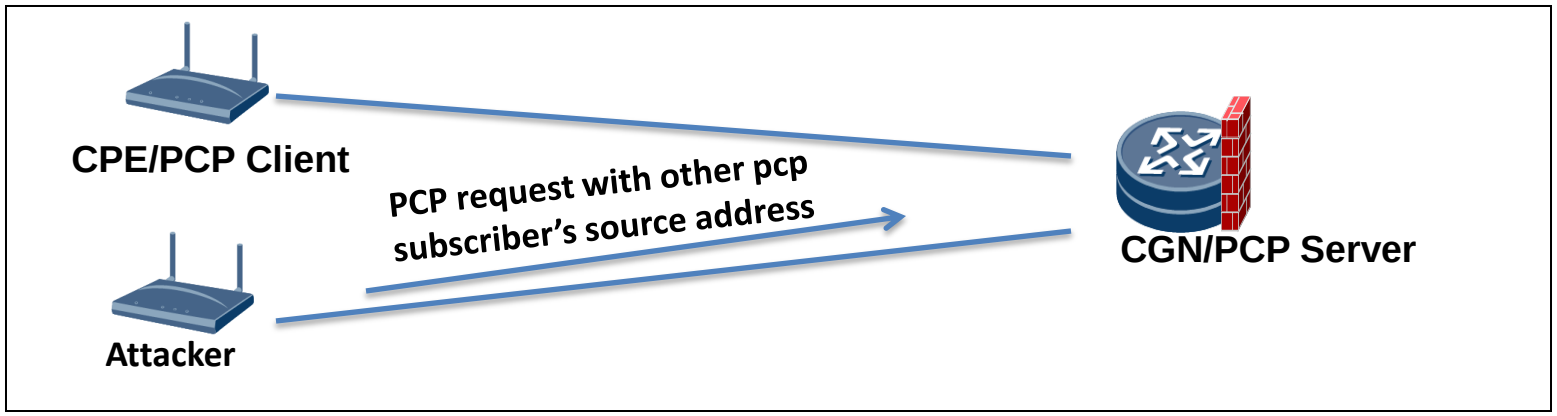
PCP subscriber identification
Draft-cui-pcp-subscriber-identification

Yong Cui, Jiang Dong
Tsinghua University
Dayong Guo
Huawei Technologies Co.

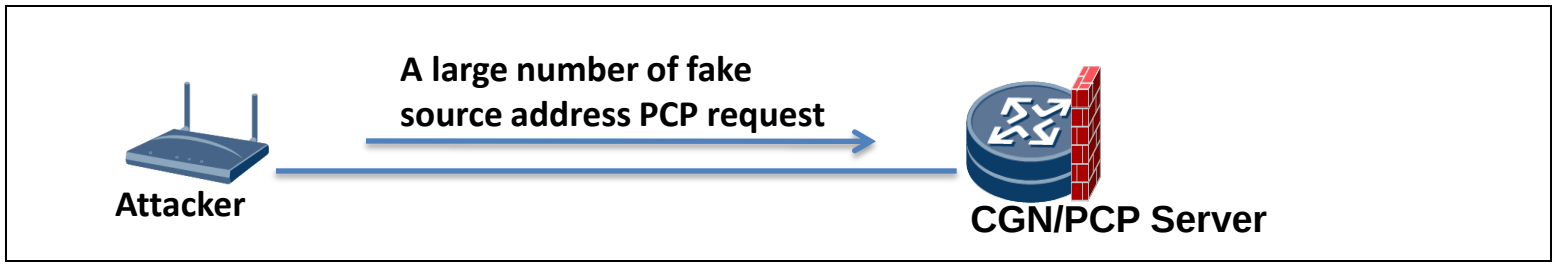
Security problem analysis

- Most of the time an organization deploying a PCP server would want to do source ingress filtering for the NAT
  - With ingress filtering, DoS attack with source address spoofing would be well defended.
- If ingress filtering is based on prefix, attacker can send PCP request with other PCP subscribers' source address within the same prefix



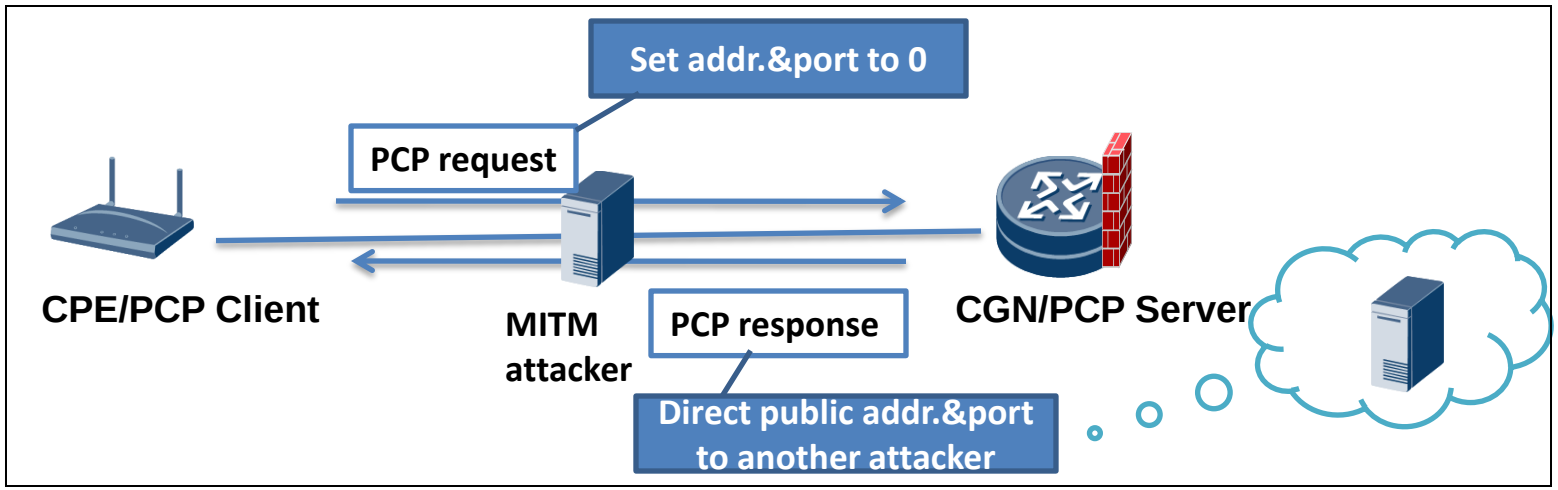
Security problem analysis(Cont.)

- DoS attack
  - Address spoofing. A large number of PCP requests with bogus source address (within the prefix of PCP server)may create lots of unwanted mappings
- Unwanted deleting of mappings
  - Delete legitimate mappings by trying different bogus source addresses



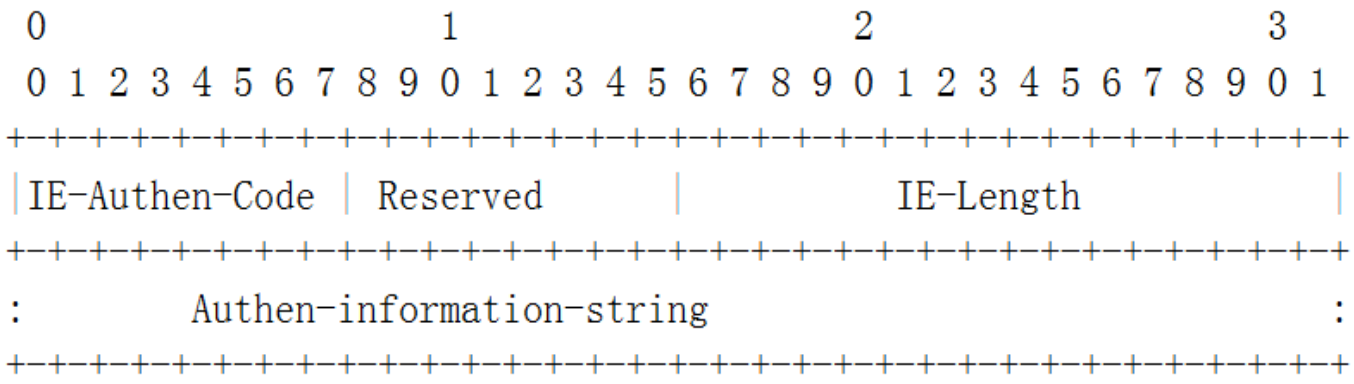
Security problem analysis(Cont.)

- MITM(Man-In-The-Middle) attack
  - Eavesdrop PCP request/response
  - Change request/response information and replay
    - Case 1: Set internal IP address and lifetime of request to zero
    - Case 2: Change the allocated external IP address and port to direct the flow to another attacker



Solution: Authen IE

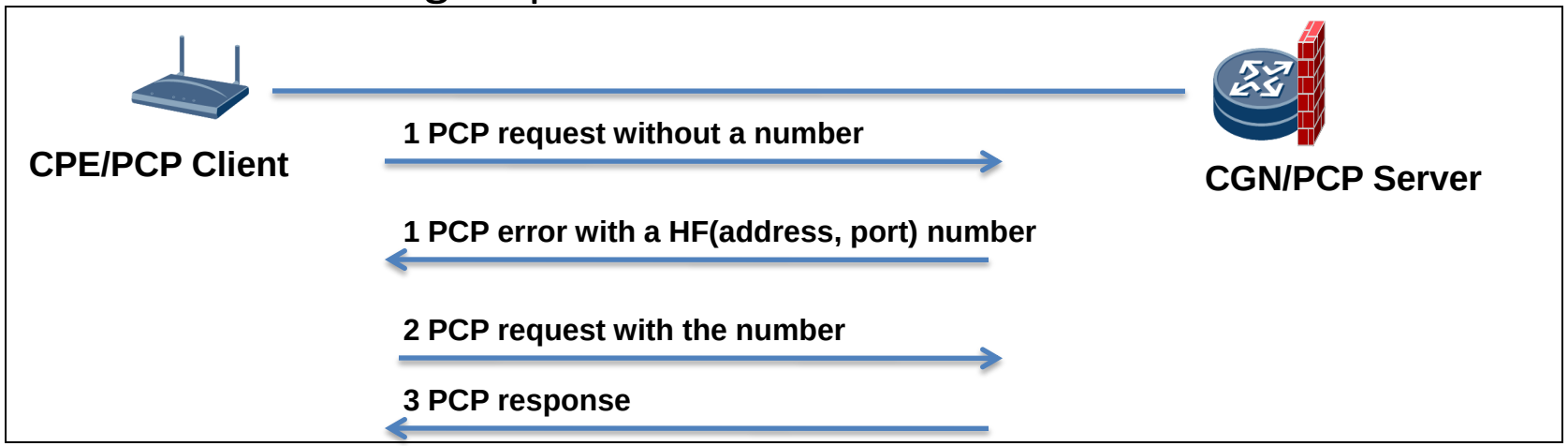
- Extend an authentication Information Element(Authen IE)
  - Authentication information could be a variable string
  - PCP server identifies PCP subscriber with the Authen IE



- Based on operating choice, the Authen IE may be one of the following contents:
  - Number
  - User name and password
  - Digit signature

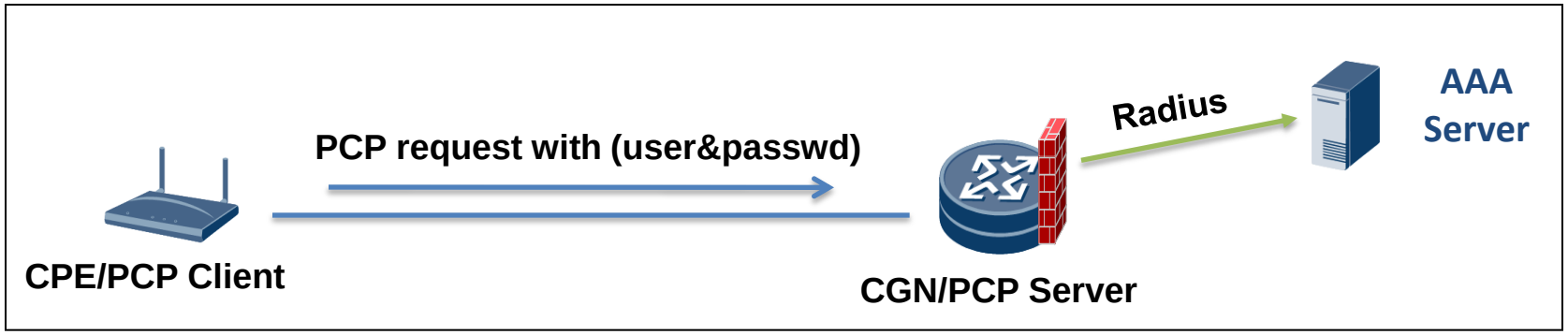
Authen IE Use Case 1: Routability Test

- Authen IE with a number to make sure the source address is true
  - This number can be generated with source address and port of request, can use hash function Hash(address, port)
- Procedure
  1. If the PCP server receives a request without a number or with a error number, it will reply an Error Response with extended IE including the number
  2. PCP client sends request with the allocated number
  3. PCP server normally response the PCP request
- DoS attack and unwanted deleting of mappings can be defended, while increasing steps of PCP communication and MITM not solved



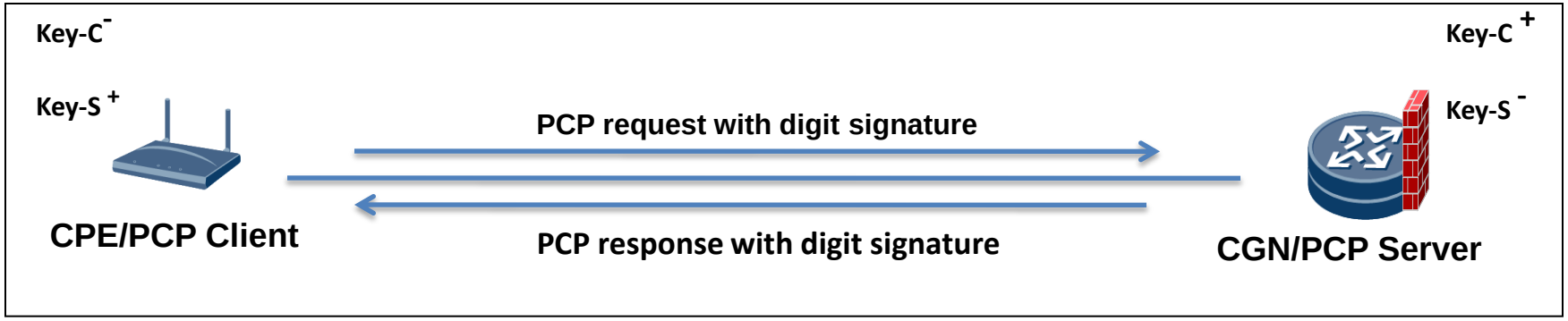
Authen IE Use Case 2: User name and password

- Authen IE with User name and password to meet the management requirements of ISP
- PCP request with extended IE including user name and password. PCP server, as an AAA client, authenticates with AAA server via Radius/Diameter
- DoS attack and unwanted mapping deleting can be defended while adding AAA procedure in the NAT device like CGN



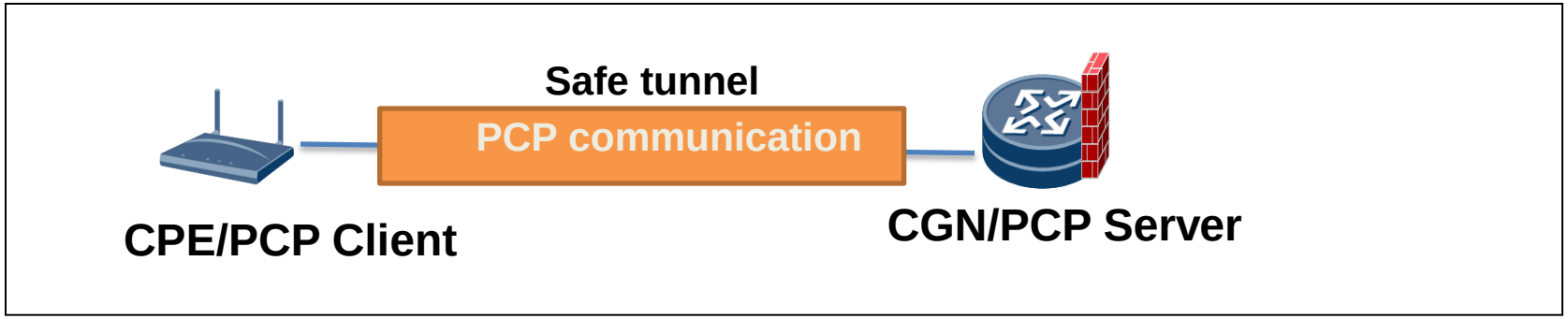
Authen IE Use Case 3: Digit signature

- Authen IE with digit signature to prevent changes in the middle of PCP communication
- Sign the PCP message with public key
  - The digit signature could be contained in extended IE
- The DoS attack, unwanted deleting of mappings and MITM attack can be well defended against.
- This method can combine with the first/second one.



Solution:
Secure channel negotiation

- Used in hostile environment
- Establish a secure channel like DTLS before the starting of PCP communication
  - PCP communication is based on the secure channel
- All the security problem could be solved, but the secure channel negotiation is complicated



Thank You!