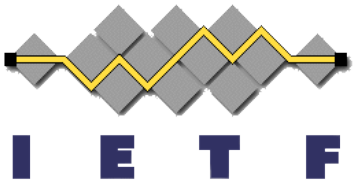
IETF90
24 July 2014
Toronto
DNSSD WG

mDNS Threat Model & Security Considerations

draft-rafiee-dnssd-mdns-threatmodel

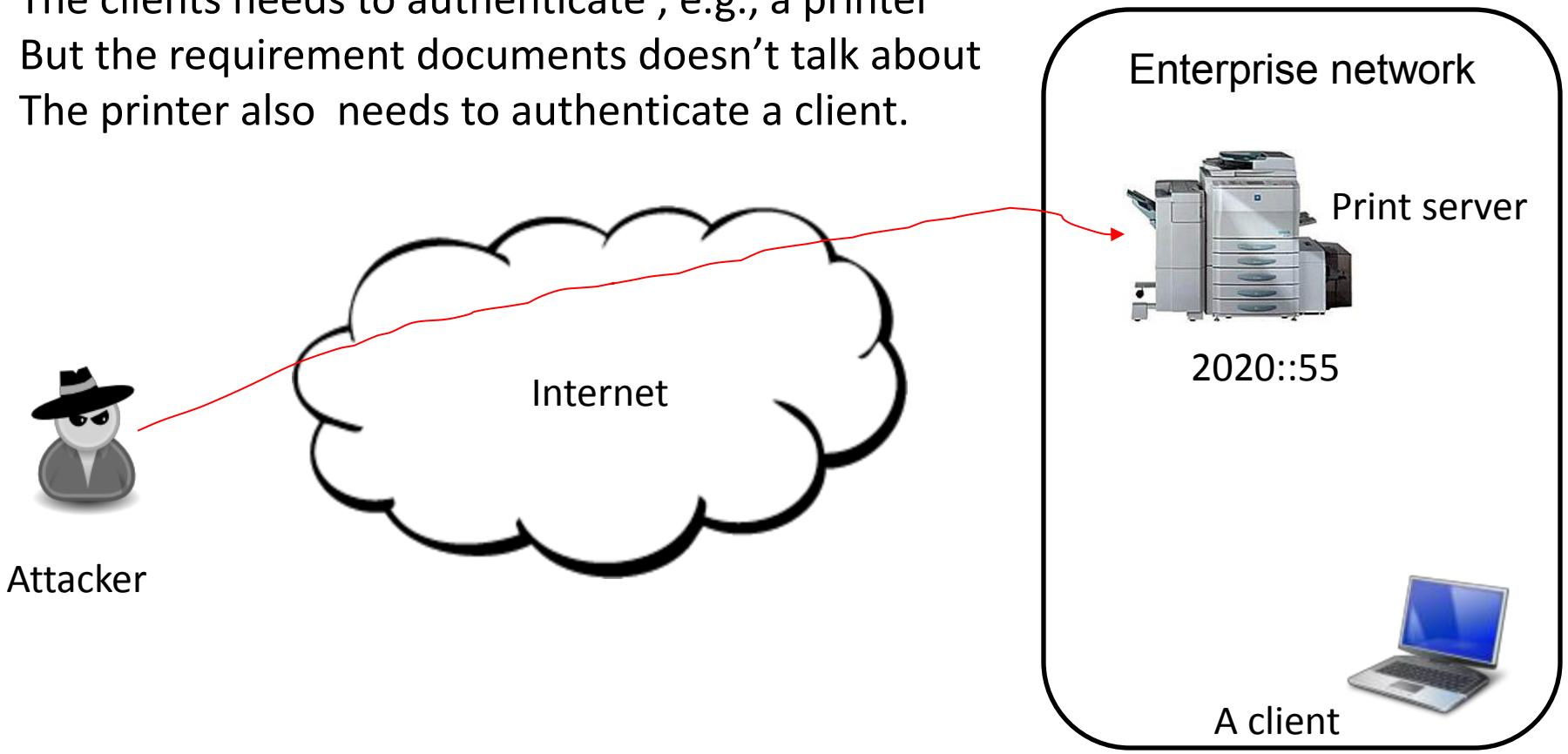
Author:
Hosnieh Rafiee

HUAWEI TECHNOLOGIES Duesseldorf GmbH, Munich, Germany



SSD and Security Considerations - I

The clients needs to authenticate , e.g., a printer
But the requirement documents doesn't talk about
The printer also needs to authenticate a client.



Problem: How to authenticate a node with dynamic IP address in a secure manner?

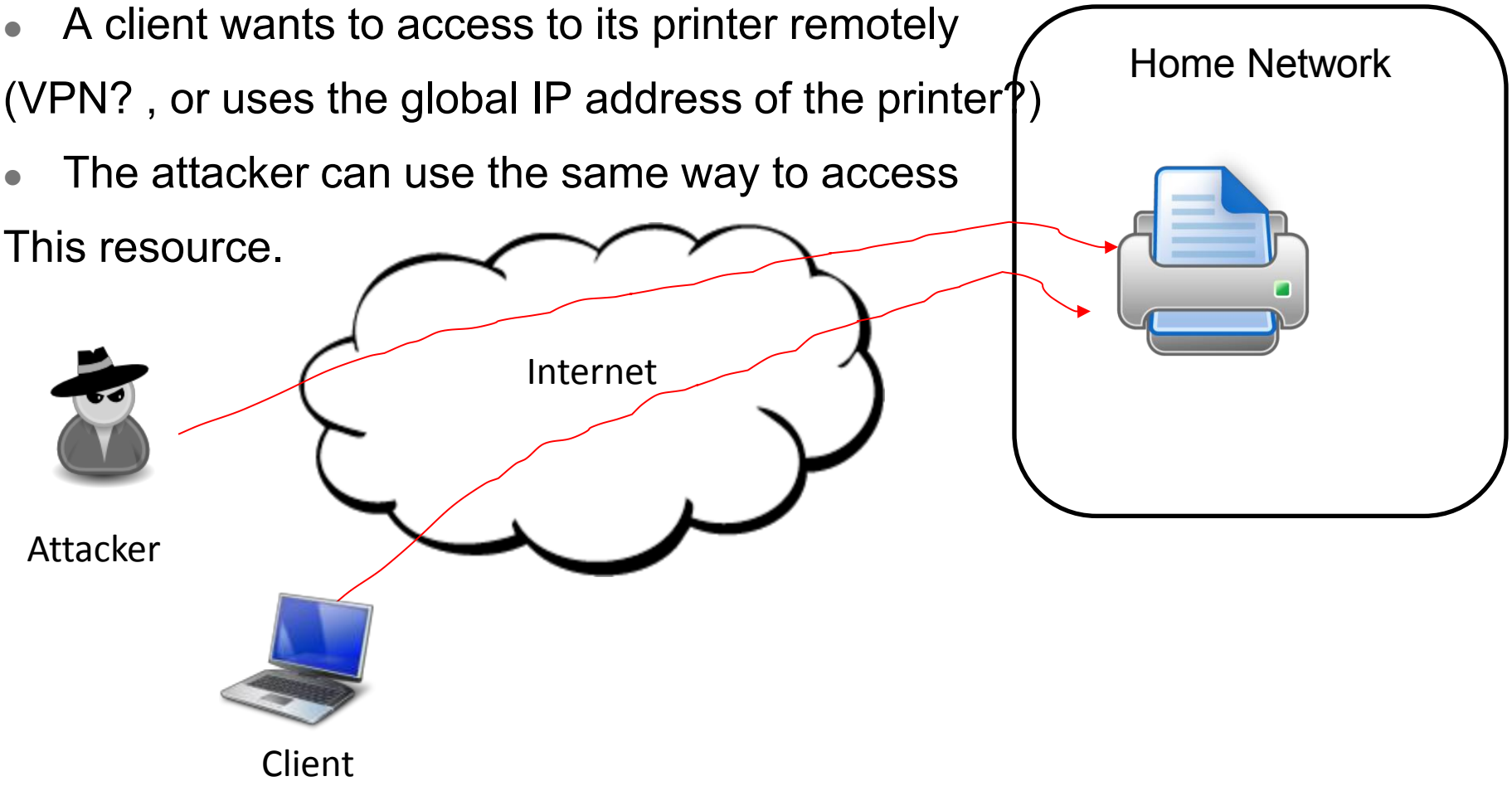
SSD and Security Considerations - II

- A client wants to access to its printer remotely

(VPN? , or uses the global IP address of the printer?)

- The attacker can use the same way to access

This resource.



SSD and Security Considerations - III

- Prevention of propagating SSD messages to unwanted networks and devices
  - Inbound and Outbound filtering on the edge devices
- Dual stack security considerations
  - Might be able to by pass firewalls and other security devices

SSD and Security Considerations - IV

- SSD can update a record on a unicast DNS (preferable dynamically)
  - What are the requirements here?
    - Would it be possible to update similar names on a unicast DNS
      - Different printers registered in a unicast DNS with similar names but different IP addresses
    - How to distinguish the SSD updated records with other records of a zone?
      - What is the differences between a printer and a client's name on a local DNS server?
    - Is there any need to change the DNS protocol to set a flag for these records to be distinguishable?

SSD and Privacy Considerations - I

- SSD can update a record on a unicast DNS (preferable dynamically)
  - Records are updated on a unicast DNS might be available outside of the current network.

The attacker might be able to have the name of services including the IP addresses

We might propagate the service information to “unwanted” networks via unicast DNS

SSD and Privacy Considerations - II

- What sensitive data might be carried with mDNS/DNS-SD protocol?
  - Label <instance>.<service>.<domain>
    - What type of device is it?
    - What kind of service does it offer? (print server, video streaming server, etc.)
    - How this device can be compromised?
    - Is there any known vulnerabilities against this device?
    - Can this device used as a entry point to attack other devices?
    - What is the capacity of this device? (DoS attack is possible??)
  - Source and Destination IP addresses
  - Any other plain text in the SSD message

Solutions For Privacy Attacks - I

- The use of random data without encryption
  - Frequently generate new random data
    - Advantage
      - Not possible to guess the type of service
    - Disadvantage
      - Users must be informed about the type of service (might require user interactions)
  - Once generate a random data and use it permanently
    - Advantages
      - Not possible to guess the type of service
    - Disadvantage
      - Once known to attacker, it is not a hidden service anymore

Solutions For Privacy Attacks - II

- Data Encryption
  - Advantages
    - Hide the whole sensitive data from attackers
  - Disadvantages
    - SSD services are available to any node in the network. If the attacker has a possibility to ask the SSD service provider, then encryption does not make sense.
    - Key exchange and management doesn’t fit to zero config nature of SSD

Solutions For Security Attacks

- Authorization and Authentication (a client on a print server)
  - The use of an access list (IP based or finger print of the client's keys)
    - CGA-TSIG draft-rafiee-intarea-cga-tsig (it can use the combination of SAVI-DHCP with hash of client's key's + IP address)
  - Other Possible authentication Mechanisms
    - DNS over DTLS (authentication of the print server)
    - DNSSEC (authentication of the print server)
  - The use of shared secret (a client authentication)
    - Shared secret exchange might be a problem
    - Security of this shared secret is a problem

My Question from WG?

- Scope of the Threat model document
  - Detail explanation of each threats
  - Possible security solutions for these threats
- Scope of the Requirement document
  - Requirements
  - Use cases
  - Briefly explanation of possible threats (only as some category)
- **Do we want to merge the threat model with the requirement documents?**

Or

- **Do we want to have separate documents for threat model and solutions & the requirements?**

Latest Version:
http://editor.rozanak.com/show.aspx?u=AZA480F5860A181786C3B7TAM

Thank you