Zeroconf and their numerous MITM attacks

Dhia Farrah, Marc Dacier

{dhia.farrah, Marc.dacier}@eurecom.fr

Introduction

- Popularity of IOT Devices
- Zeroconf series of protocols ensures usability
- Usability oriented , plug and play
- Devices speak at least one of these protocols
- putting at risk millions of devices

Outline

- Zeroconf : MDNS and DNS-SD
- MITM attacks
- Experiments and Results
- Detection

Zeroconf: MDNS and DNS-SD

MDNS: Local domain Name announcing and resolution

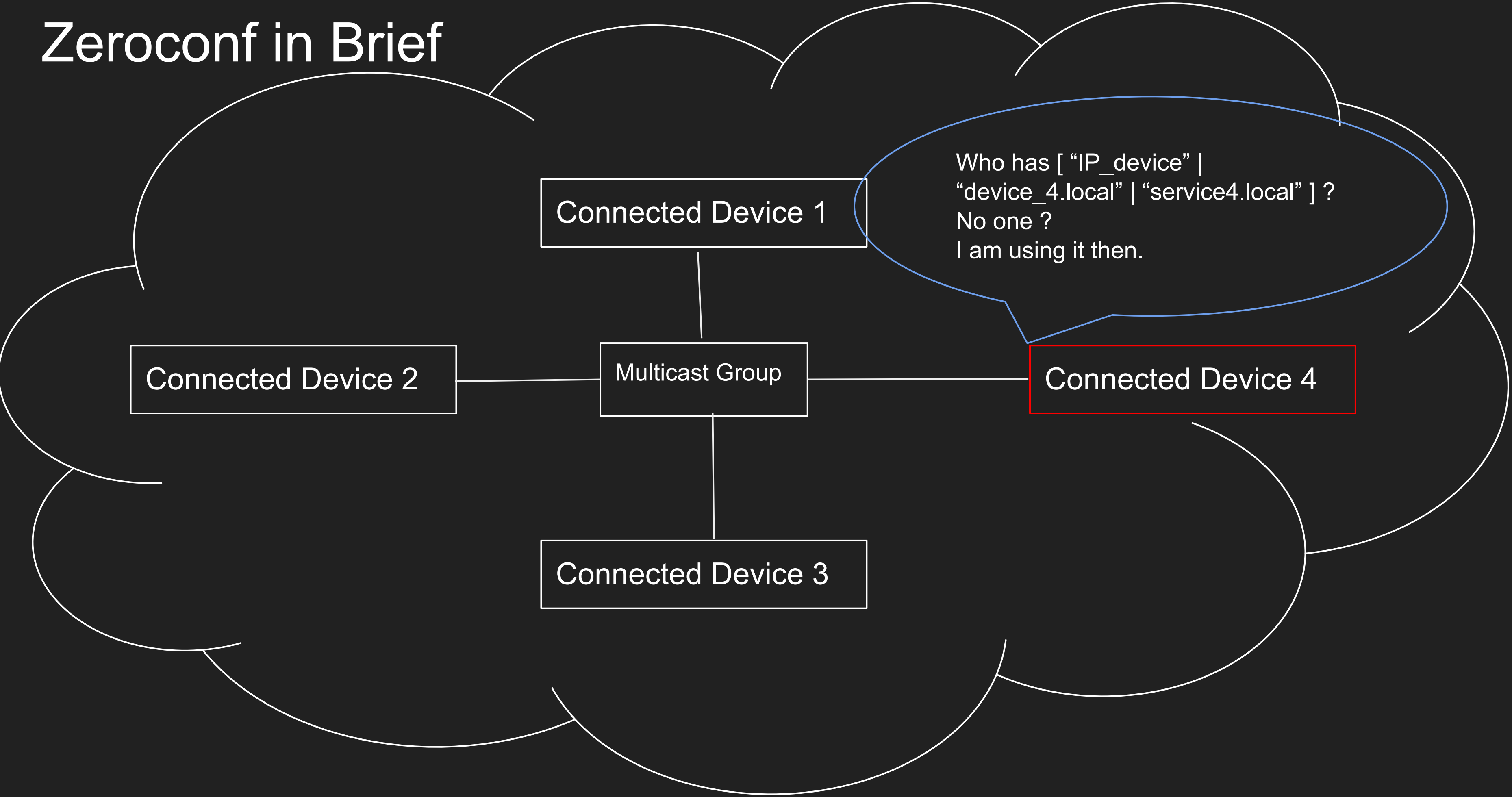
DNS-SD: Service Discovery

Multicast address 224.0.0.251

MDNS and DNS-SD

- IP Address
- Local Domain Name “HP 6362 [A51456].local”
- Local Service Name “HP Printer._ipp._tcp.local”

Zeroconf in Brief



Connected Device 1

Connected Device 2

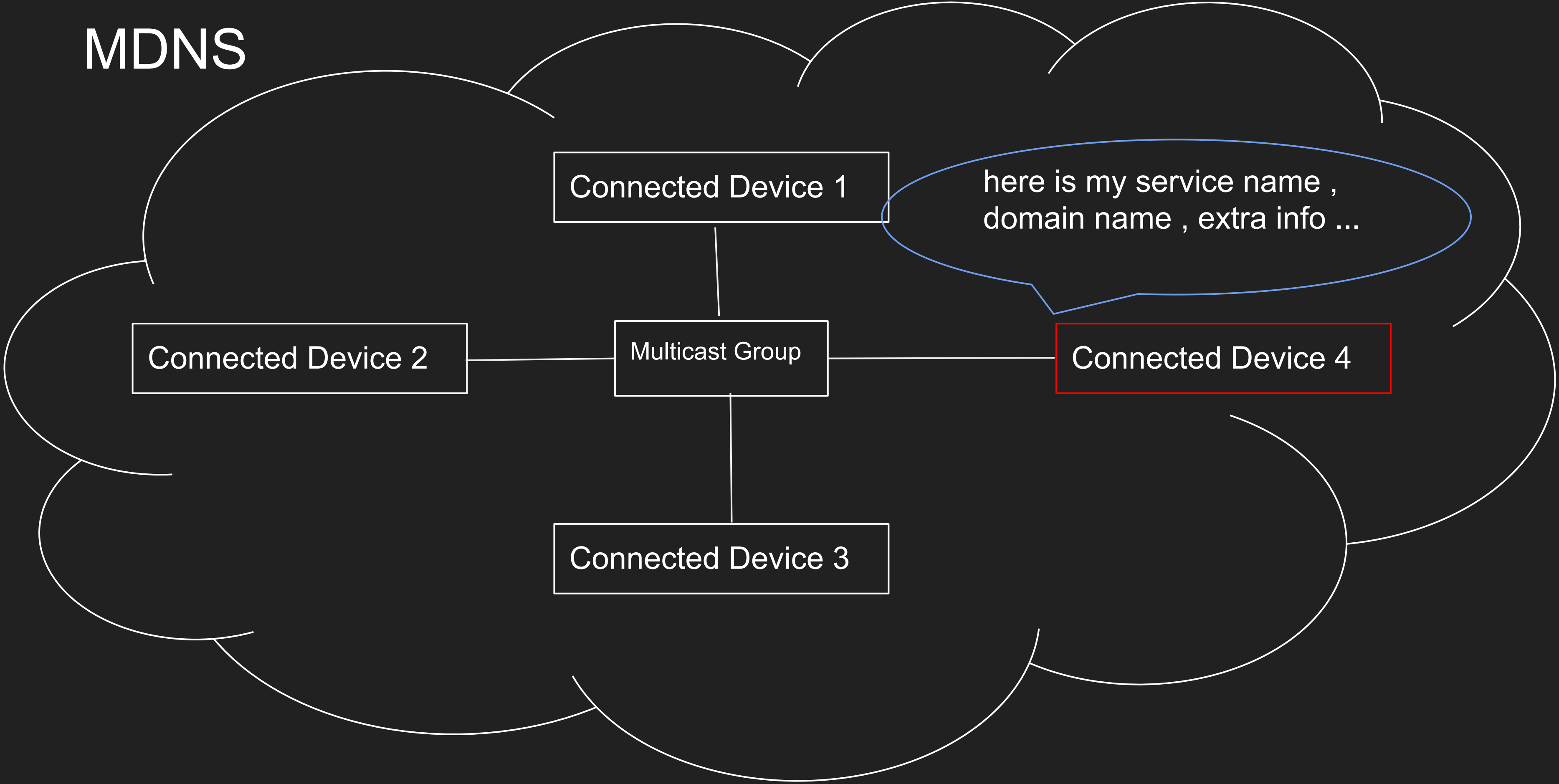
Multicast Group

Connected Device 4

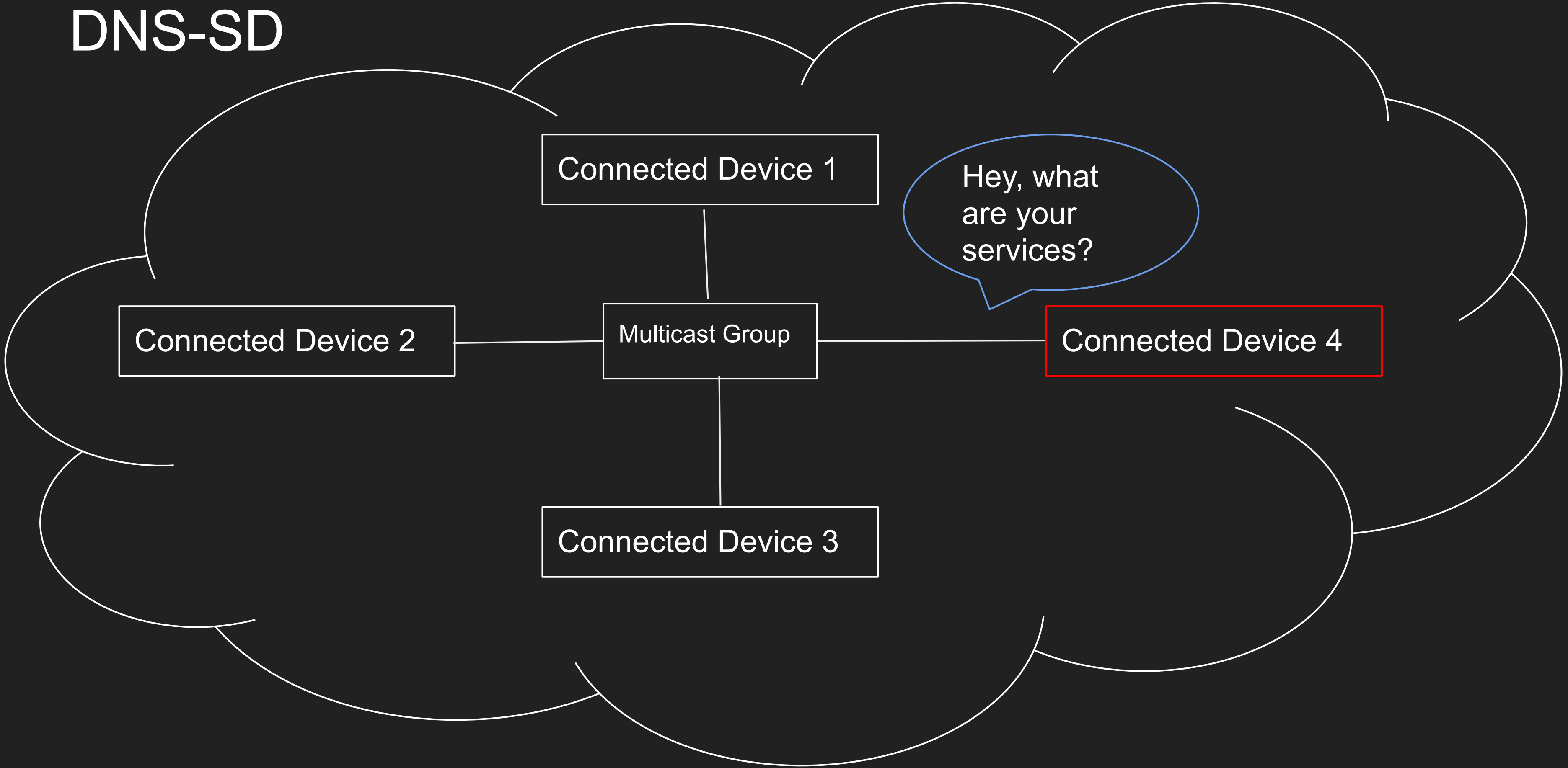
Connected Device 3

Who has [“IP_device” |
“device_4.local” | “service4.local”] ?
No one ?
I am using it then.

MDNS


Connected Device 1
here is my service name , domain name , extra info ...
Connected Device 2
Multicast Group
Connected Device 4
Connected Device 3

DNS-SD



Connected Device 1

Connected Device 2

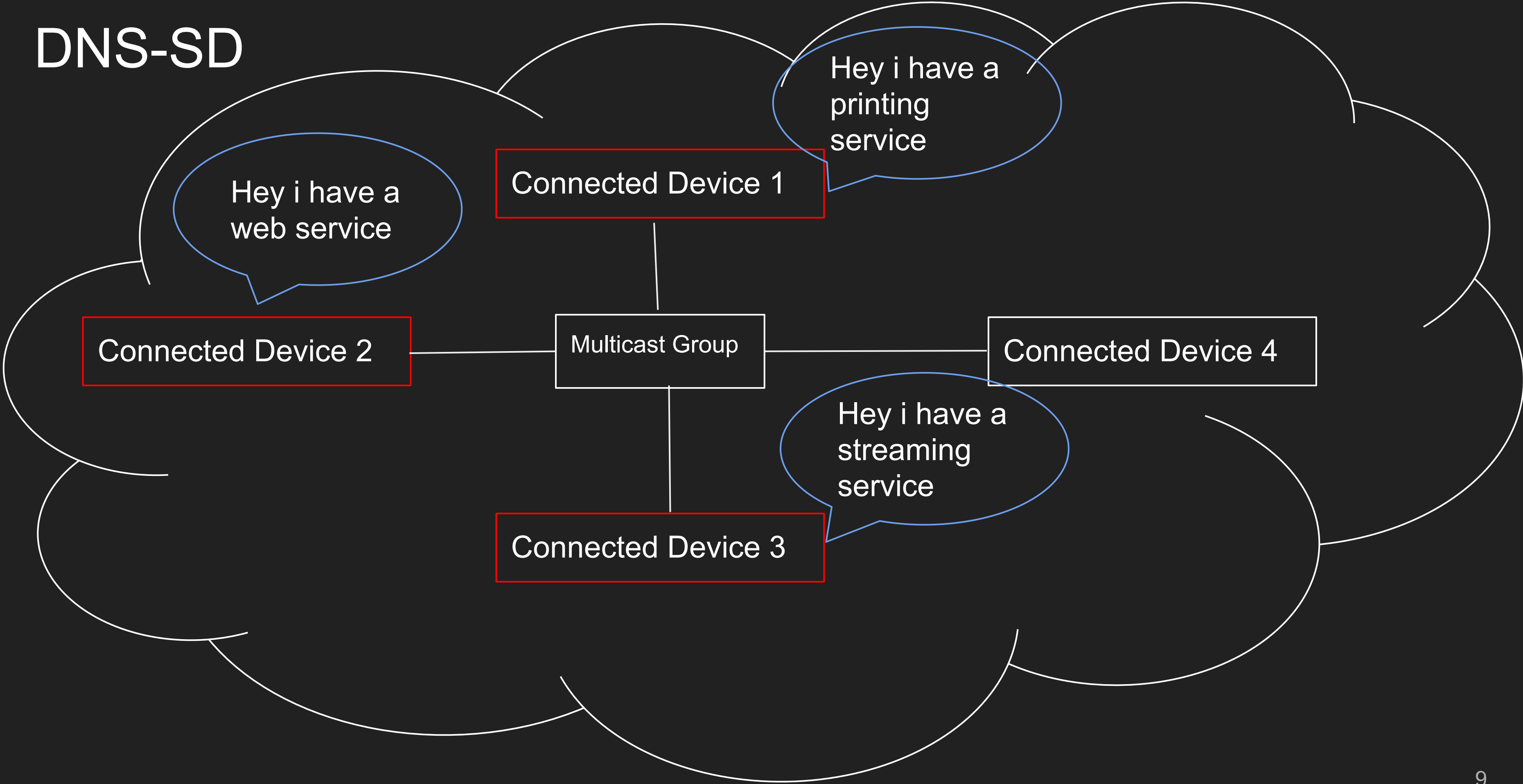
Multicast Group

Connected Device 4

Connected Device 3

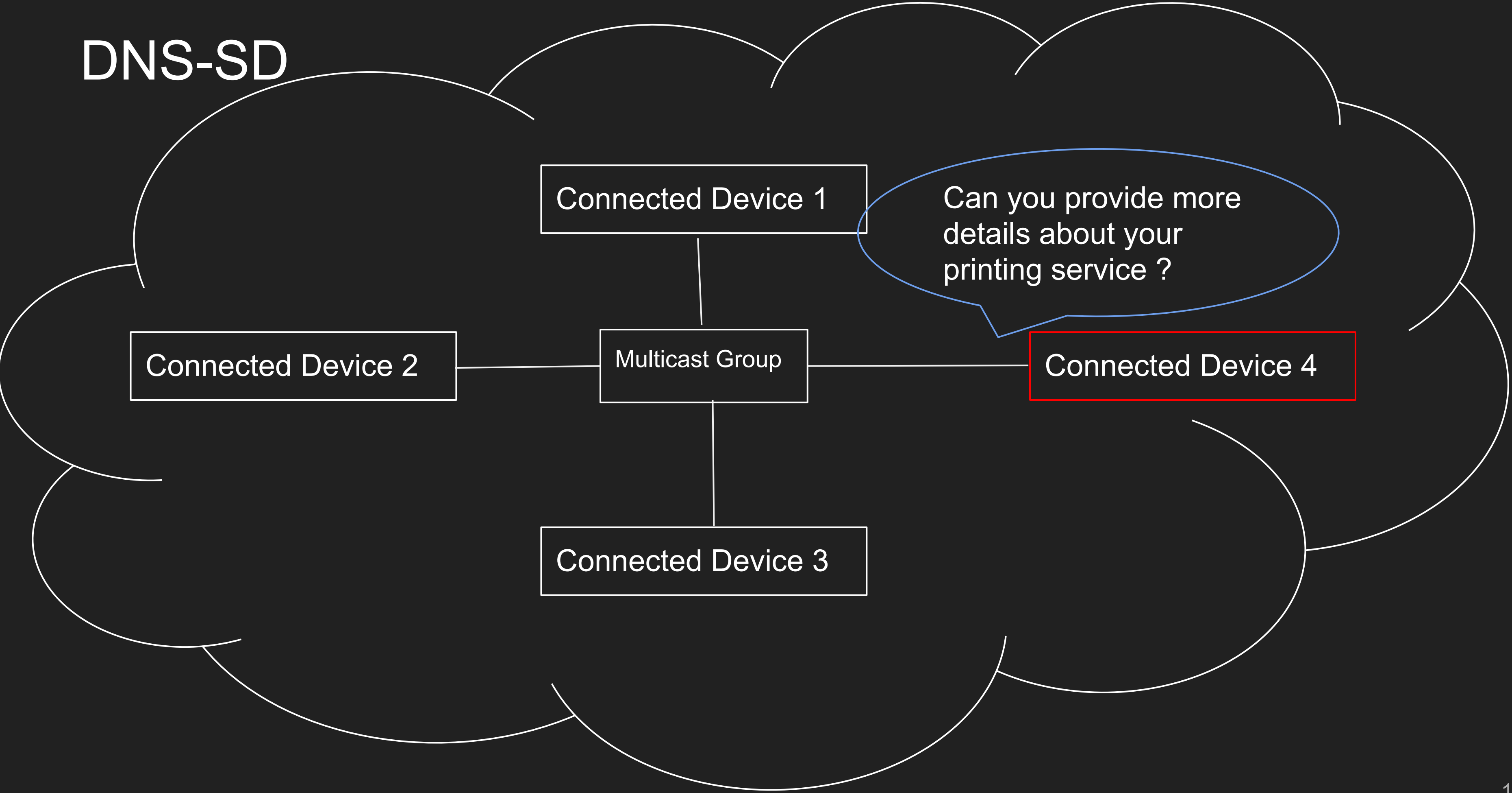
Hey, what are your services?

DNS-SD

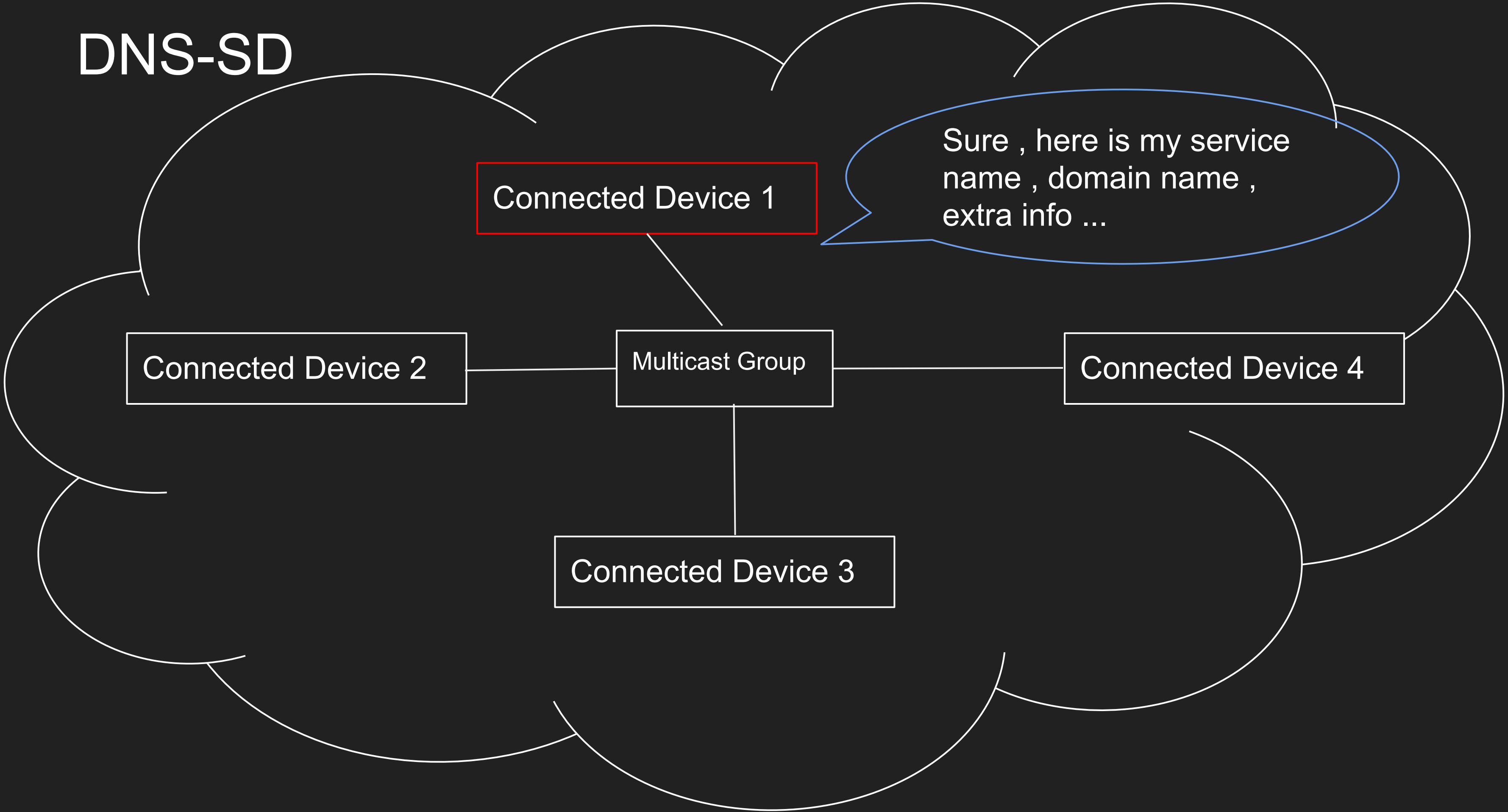


Hey i have a printing service
Hey i have a web service
Connected Device 1
Connected Device 2
Multicast Group
Connected Device 4
Hey i have a streaming service
Connected Device 3

DNS-SD

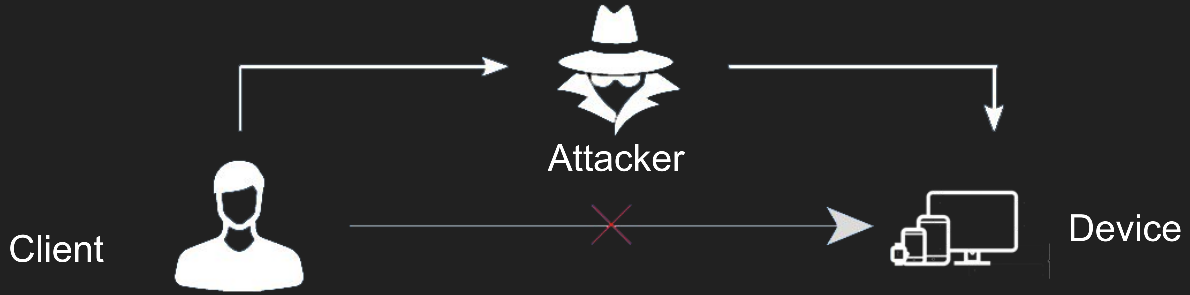

Connected Device 1
Can you provide more details about your printing service ?
Connected Device 2
Multicast Group
Connected Device 4
Connected Device 3

DNS-SD

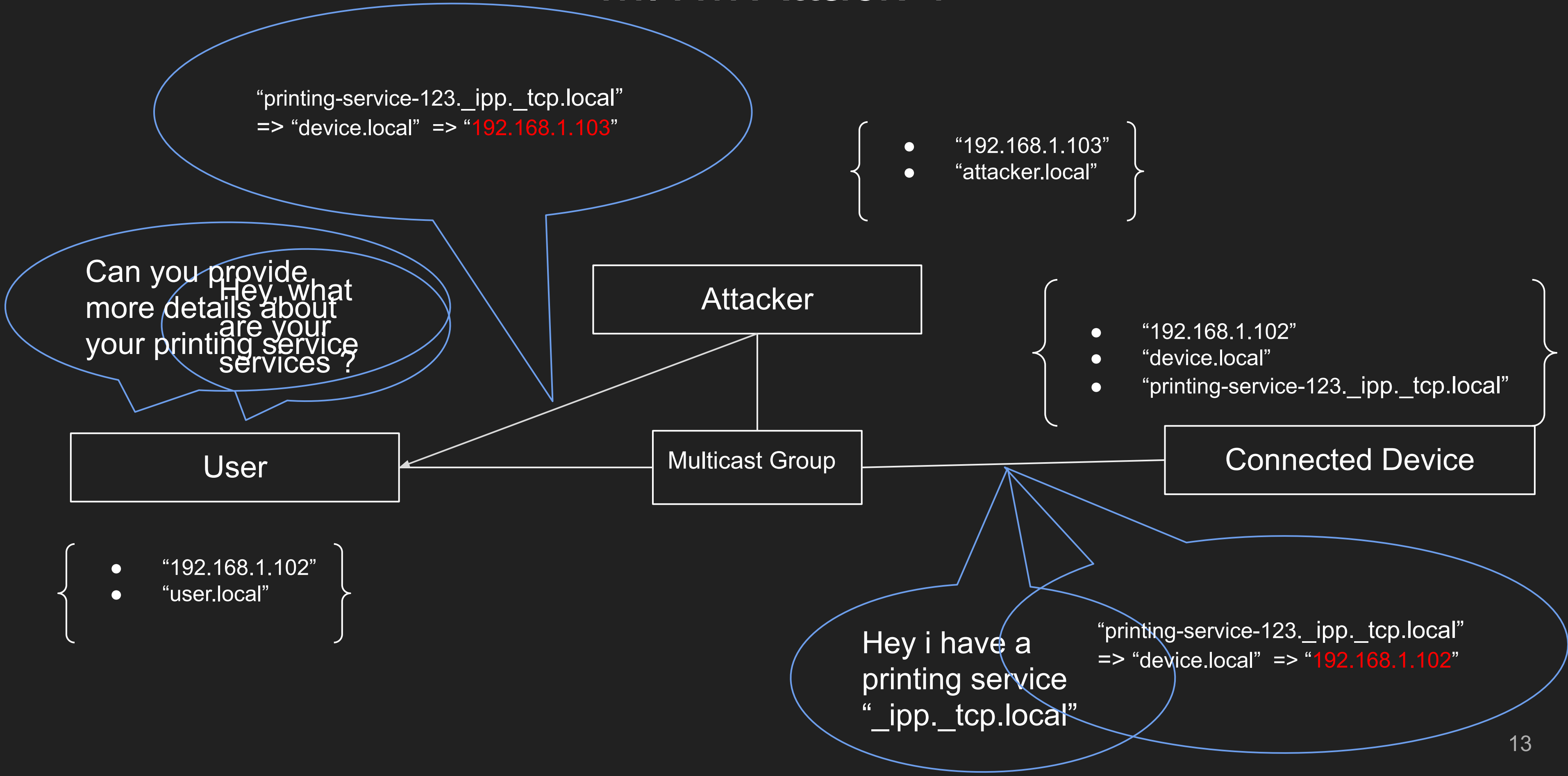

Connected Device 1
Sure , here is my service name , domain name , extra info ...
Connected Device 2
Multicast Group
Connected Device 4
Connected Device 3

Man in the middle attacks

- “Convincing the client that the device’s local domain name is resolved to the attacker IP”
- “Convincing the client that the device’s local service name is reachable via the attacker local domain name”
- “Hijack the local service name and force the device to change it.”
- “Annonce a similar local service name and bait the client into picking it ”



MITM Attack 1



"printing-service-123._ipp._tcp.local"
=> "device.local" => "192.168.1.103"

- "192.168.1.103"
- "attacker.local"

Can you provide more details about your printing service

Hey, what are your services ?

Attacker

- "192.168.1.102"
- "device.local"
- "printing-service-123._ipp._tcp.local"

User

Multicast Group

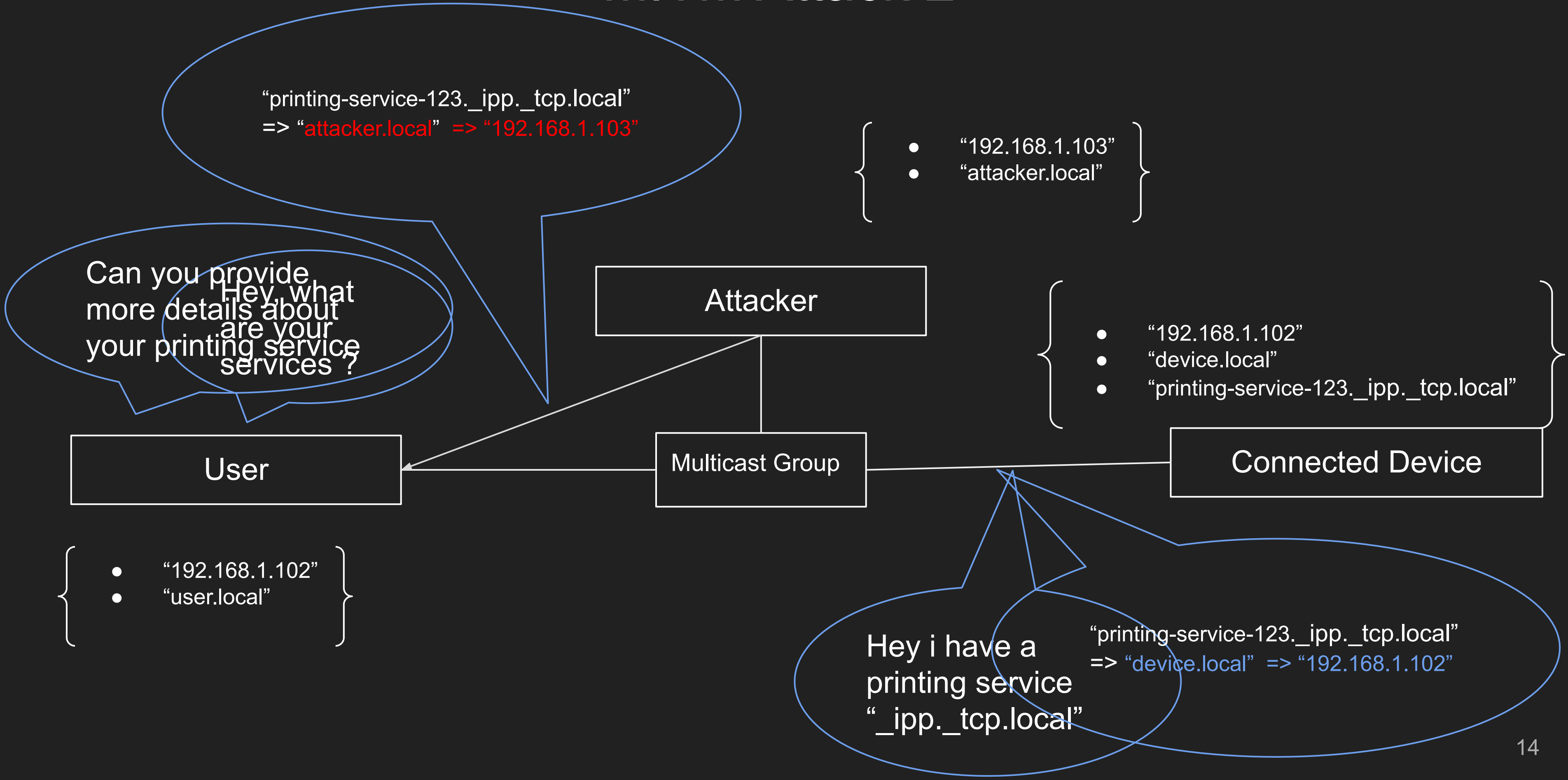
Connected Device

- "192.168.1.102"
- "user.local"

Hey i have a printing service "_ipp._tcp.local"

"printing-service-123._ipp._tcp.local"
=> "device.local" => "192.168.1.102"

MITM Attack 2



Hey, what are your services ?

Can you provide more details about your printing service

"printing-service-123._ipp._tcp.local"
=> "attacker.local" => "192.168.1.103"

- "192.168.1.103"
- "attacker.local"

Attacker

User

Multicast Group

Connected Device

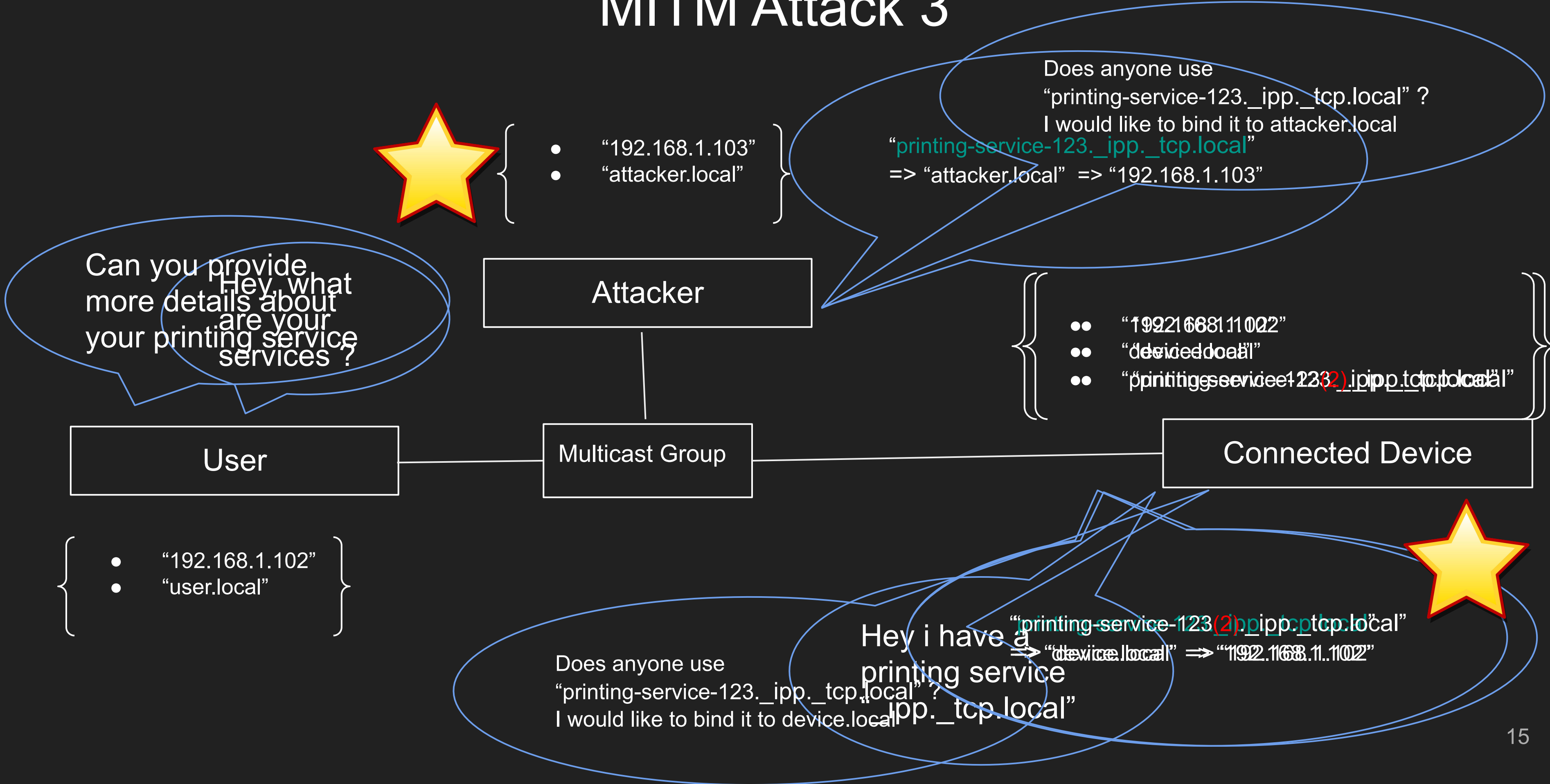
- "192.168.1.102"
- "device.local"
- "printing-service-123._ipp._tcp.local"

- "192.168.1.102"
- "user.local"

Hey i have a printing service "_ipp._tcp.local"

"printing-service-123._ipp._tcp.local"
=> "device.local" => "192.168.1.102"

MITM Attack 3



Attacker

- “192.168.1.103”
- “attacker.local”

Does anyone use “printing-service-123._ipp._tcp.local” ? I would like to bind it to attacker.local

“printing-service-123._ipp._tcp.local” => “attacker.local” => “192.168.1.103”

User

- “192.168.1.102”
- “user.local”

Can you provide more details about your printing service

Hey, what are your services ?

Multicast Group

Connected Device

- “192.168.1.102”
- “device.local”
- “printing-service-123._ipp._tcp.local”

- “192.168.1.102”
- “device.local”
- “printing-service-123(2)._ipp._tcp.local”

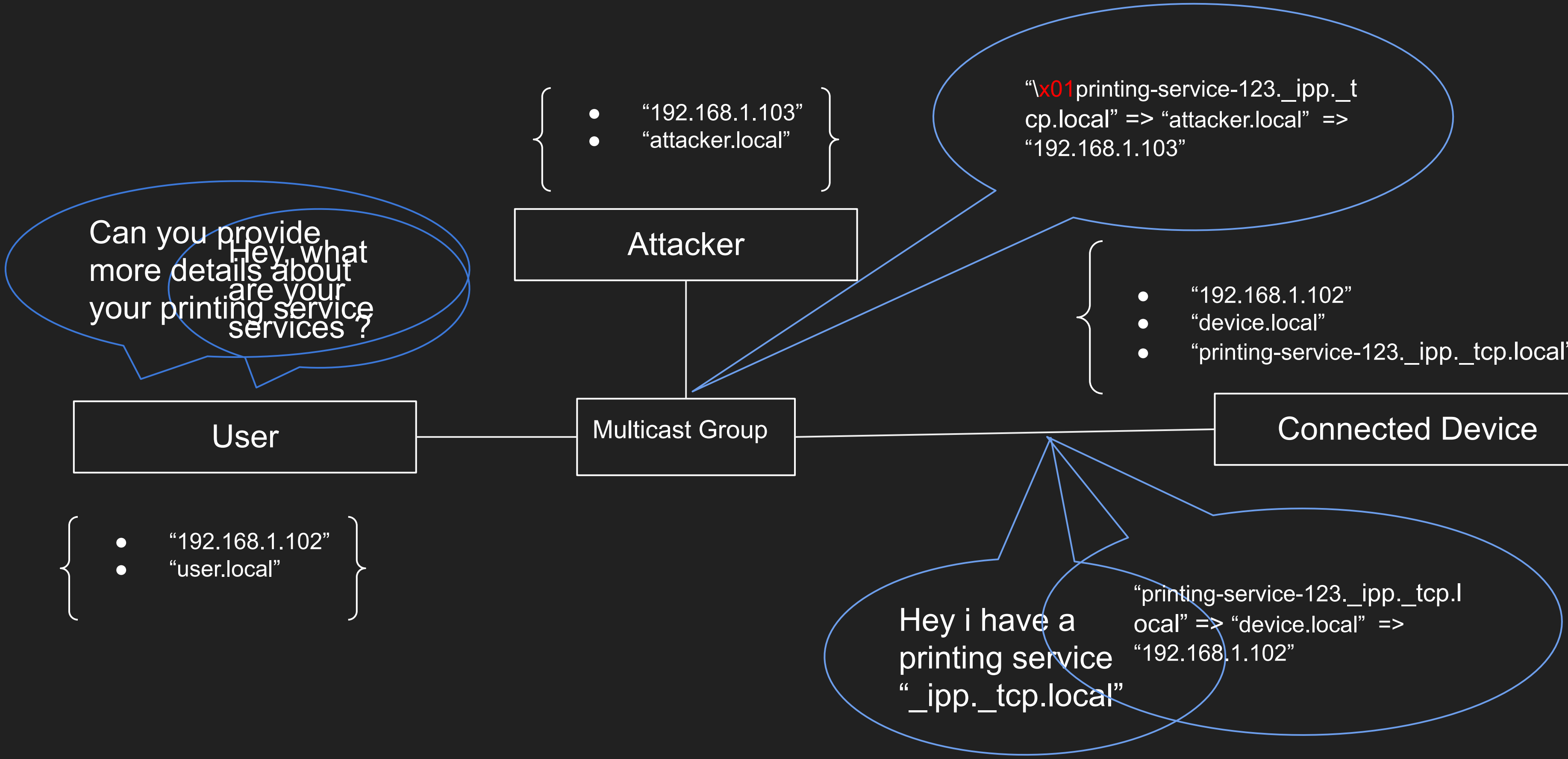
Does anyone use “printing-service-123._ipp._tcp.local” ? I would like to bind it to device.local

Hey i have a printing service “_ipp._tcp.local”

“printing-service-123._ipp._tcp.local” => “device.local” => “192.168.1.102”

“printing-service-123(2)._ipp._tcp.local” => “device.local” => “192.168.1.102”

MITM Attack 4



- "192.168.1.103"
- "attacker.local"

Attacker

"\x01printing-service-123._ipp._tcp.local" => "attacker.local" => "192.168.1.103"

Can you provide more details about your printing service

Hey, what are your services ?

- "192.168.1.102"
- "device.local"
- "printing-service-123._ipp._tcp.local"

User

Multicast Group

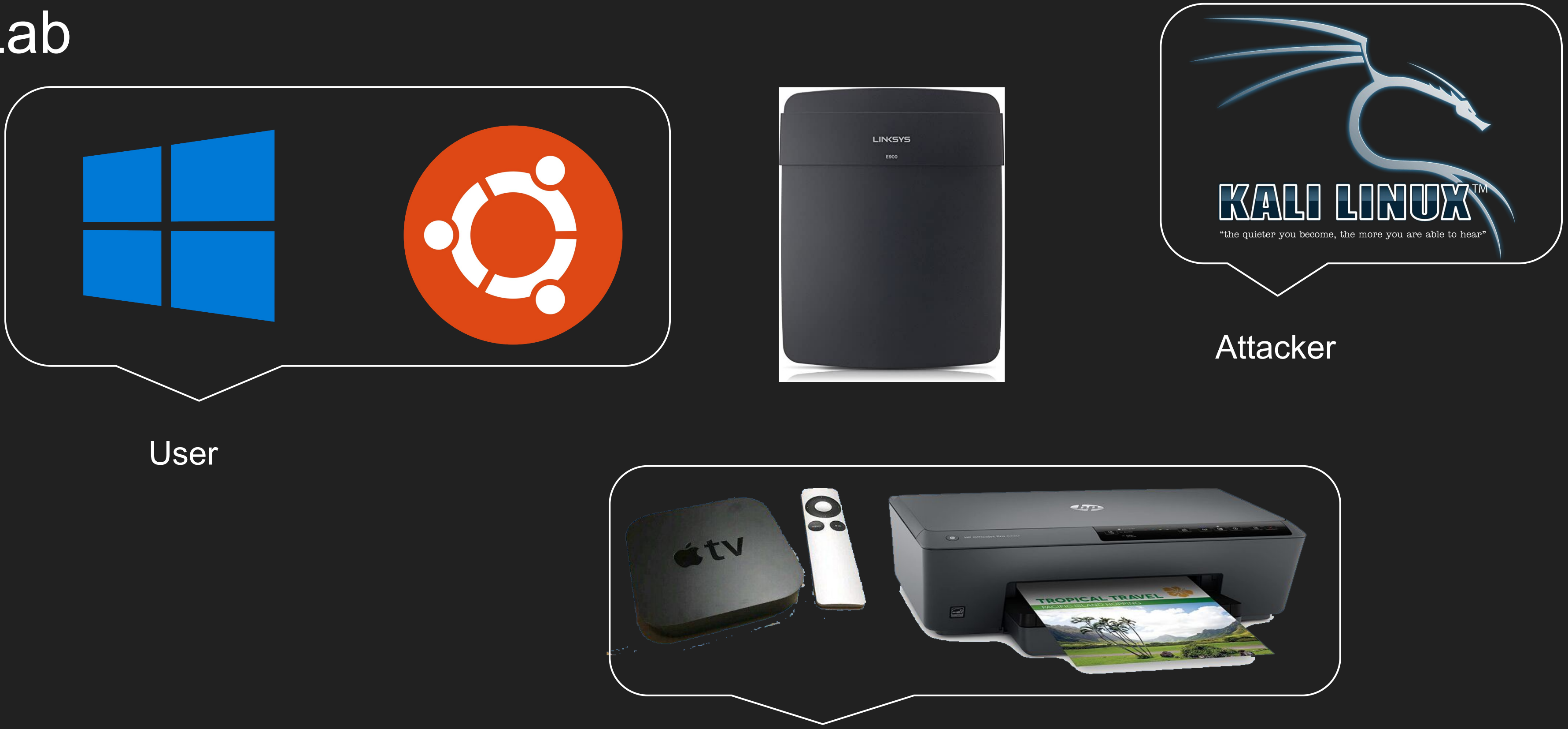
Connected Device

- "192.168.1.102"
- "user.local"

Hey i have a printing service "_ipp._tcp.local"

"printing-service-123._ipp._tcp.local" => "device.local" => "192.168.1.102"

Lab



User

Attacker

Devices

Take away

- A non-compliant adversary can …
  - … generate DOS against genuine participant;
  - … Steal the properties of a genuine participant.

- Unicast replies make the task of the attacker easier by hiding his replies.

- A non compliant implementation makes it even easier !

- RFC 791 , IP (1981) : “The implementation of a protocol must be robust. [...] In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior”

- should we consider all the possibilities or just consider just how it should works ?

Conclusion

- Protocols used a lot (Even in a well configured network)!
- The use of these protocols makes the devices vulnerable
- Covering every outcome may not be a solution
- Delegate the protection for an other entity

Thank you

My “Bro” script is watching you

and it Zeeks to find you