IP Mobility:
Threat Models and Security Requirements

Vidya Narayanan (vidyan@qualcomm.com)
Lakshminath Dondeti (ldondeti@qualcomm.com)

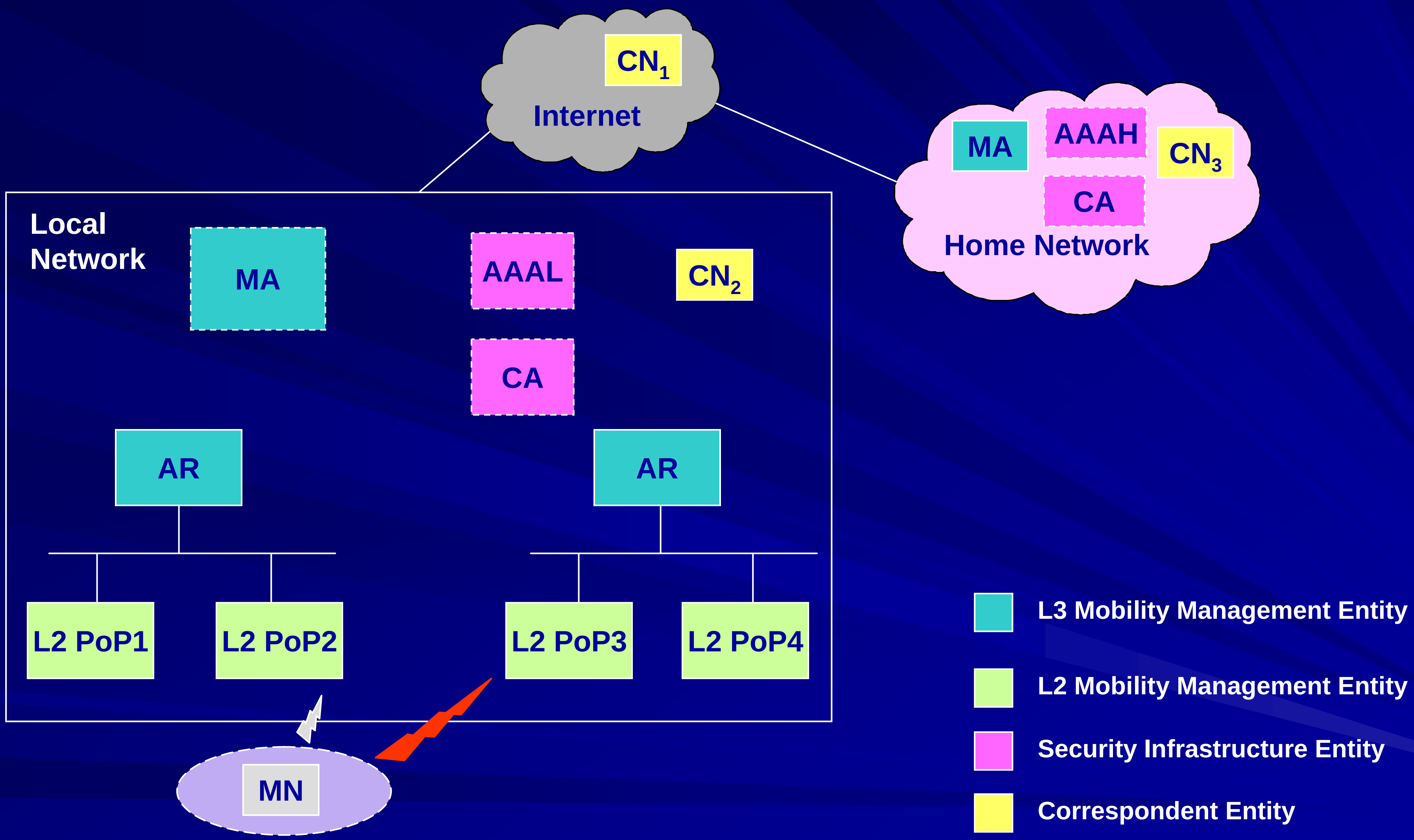
Outline

- Introduction and Goals
- Typical network architecture
- Assets
- Internet Threat Model – A Recap
- Routing and IP Mobility
- Security analysis of IP mobility protocols
- Security Requirements
- Security Models

Introduction and Goals

- IP Mobility handles changes to the IP point of presence (PoP)
  - Forwards packets meant for an “anchor” IP address to a “transient” IP address
  - Several models (global, local, host-based, network-based)
- Aid analysis of threat models for IP mobility protocols
- Remove the guesswork in threats
- Provide high level security requirements for IP mobility protocols
- Allow evaluation of a security solution

Overall Mobility Architecture



Definitions

- Mobility Agent
  - Entity maintaining state on location of mobile nodes
    - E.g., MIP HA, FMIP pAR, HMIP MAP, NETLMM LMA, MIP RO-enabled CN
- Mobility Facilitators
  - Other entities that facilitate IP mobility
    - E.g., NETLMM MAG, MIP4 FA, HMIP AR
  - It is plausible for these to fail/be compromised without denial of service
- Mobility Provider
  - Mobility Agent or Mobility Facilitator
- Mobility Recipient
  - Entity receiving the IP mobility service
  - Mobile node is the recipient

Assets

- Critical Assets
  - Failure/compromise of these assets leads to failed mobility sessions
    - Mobile Node
    - Mobility Agent
    - Security Infrastructure Entities
- Non-critical Assets
  - The mobility session can continue despite failure/compromise of these assets
    - Network infrastructure, including links
    - Mobility facilitators (e.g., ARs, routers)
- Other Assets
  - Correspondent Nodes
  - Other nodes (mobile or fixed) attaching to the mobility domain
- Not all assets are applicable for all mobility models

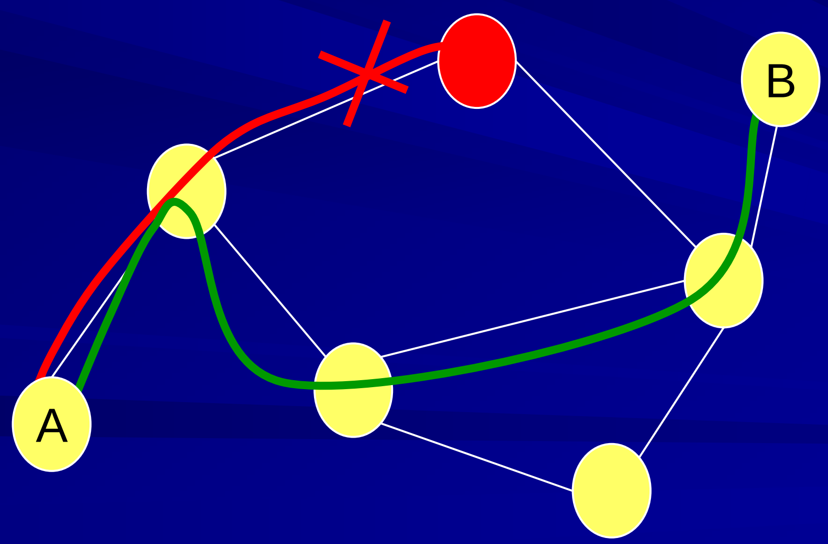
The Internet Threat Model – A Recap

- Assumption 1: Critical assets are not compromised
- Assumption 2: The attacker has full control of the communication channel
  - Attacker can read, inject, remove, modify any packets without detection
- Types of attacks
  - Passive attacks
  - Active attacks
  - Off-path Attacks
  - On-path Attacks
    - Superset of Off-path attacks
- Reference: RFC3552
- *Are all these assumptions and/or attacks applicable to IP mobility protocols?*
- *Are there other assumptions and/or attacks that are applicable to IP mobility protocols?*

Routing and Byzantine Failures

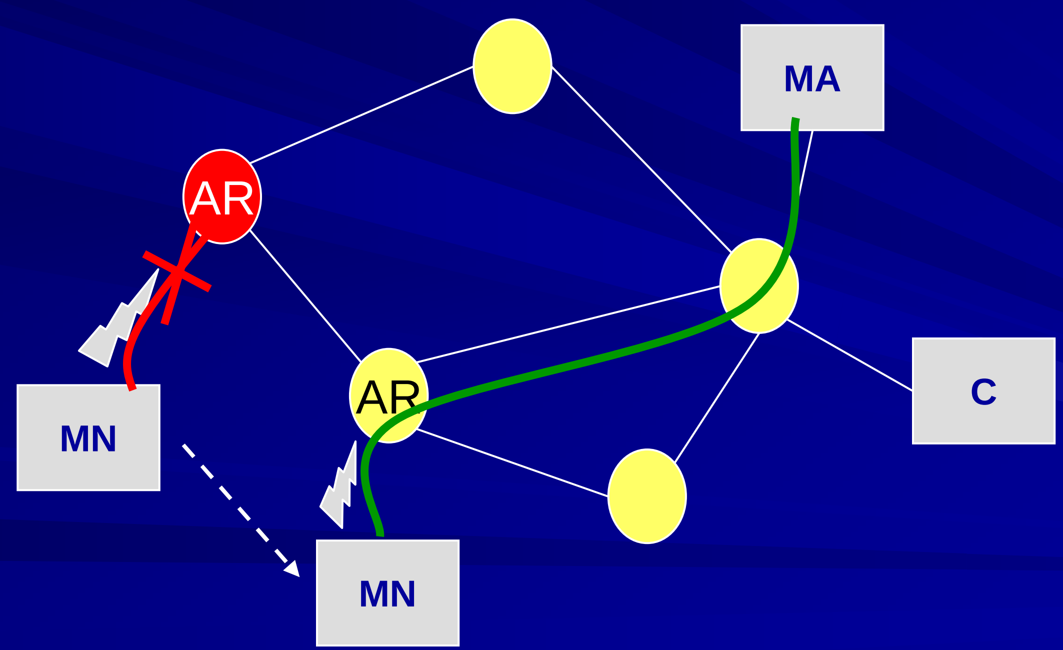
- A network can function in the presence of Byzantine failures
  - Entities lying about routing or other information selectively, while appearing to function correctly (due to compromise, mis-configuration)

- As long as there is a non-faulty path between nodes A and B, they can communicate
  - Even if the adversary sends bogus and disparate information to legitimate infrastructure entities, e.g., routers



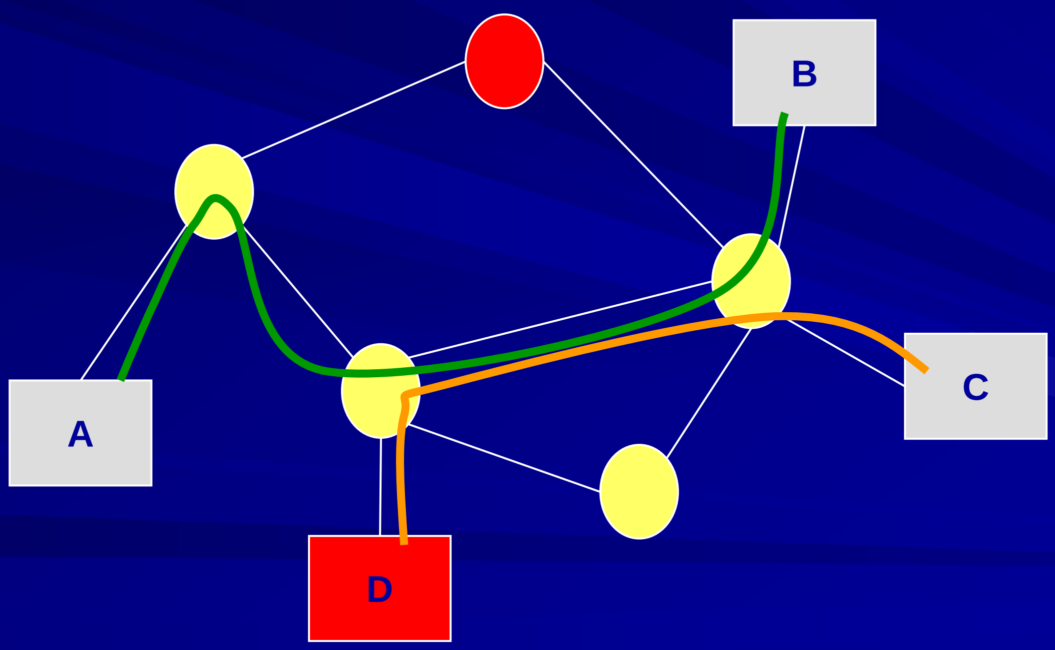
Mobility and Failure of Non-critical Nodes

- Mobility signaling is possible even if one a few non-critical assets fail in an adversarial fashion
- Mobility facilitators may fail in a Byzantine fashion, yet MNs can and should be able to get service



Don’t Mess With Routing!

- A protocol among a given set of entities must not impact routing for unrelated entities
  - D’s malicious use of a protocol between C and D MUST not impact communication between A and B



Outline

- Introduction and Goals
- Defining IP Mobility
- IP Mobility Models
- Typical network architecture
- Assets
- Internet Threat Model – A Recap
- Routing and IP Mobility
- Security analysis of IP mobility protocols
  - Threats to IP mobility "providers"
  - Threats to IP mobility "recipients"
  - Off-path vs. on-path attacks
  - Threats enabled by mobility protocols
- Security Requirements
- Security Models

Threats to IP Mobility Provider

- Provider's interests
  - Ensuring that only authorized entities obtain the service
    - Ensuring that service is provided as intended
  - Only entities served by the provider are able to create state at the mobility agent
- Threats to mobility "agents"
  - Creation of state by unauthorized nodes
  - Creation of incorrect state for valid nodes
- Threats to mobility "facilitators"
  - Creation of spurious state at the facilitator
  - Use of facilitator to disrupt IP mobility

Threats to IP Mobility Recipient

- Recipient’s interests
  - Ensuring undisrupted IP mobility service
- Threats to recipients
  - Redirection
    - Recipient’s traffic being redirected elsewhere
  - DDoS
    - Recipient being victim to a DDoS attack and receiving spurious traffic
  - DoS
    - Disruption in IP mobility service
    - Redirection may lead to DoS

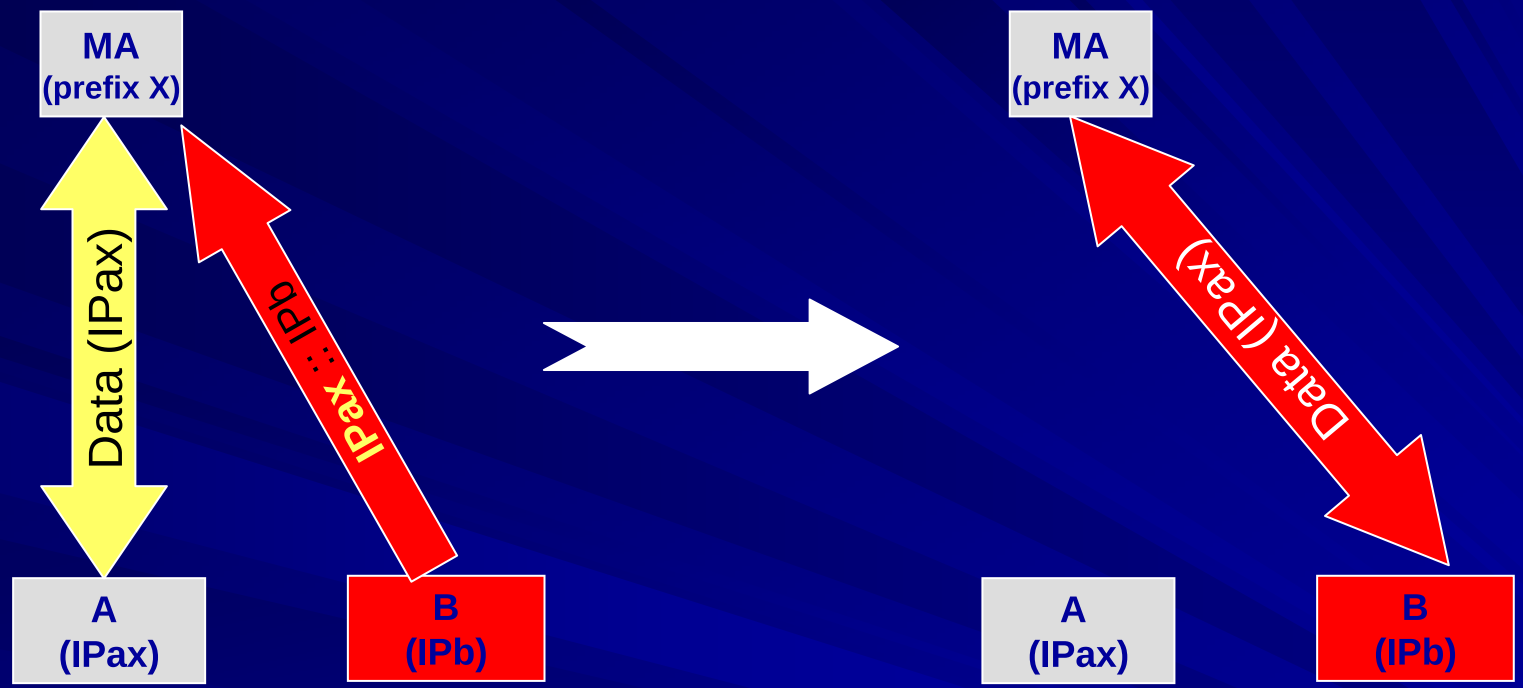
Mobility Protocols Facilitate Attacks

- Mobility protocols have a unique feature ☺
  - ***Any node on the network is a potential victim***
    - Mobility signaling supplants routing state!
- Set of assets expanded beyond mobility providers and recipients
- Redirection of traffic belonging to other nodes
- DDoS on any node in the Internet
  - IP mobility provides one more way of realizing a DDoS attack
  - Is it significantly easier to launch a DDoS using IP mobility protocols?
    - Perhaps!
    - Traceability factors into the equation

The Power of an Off-path Attacker

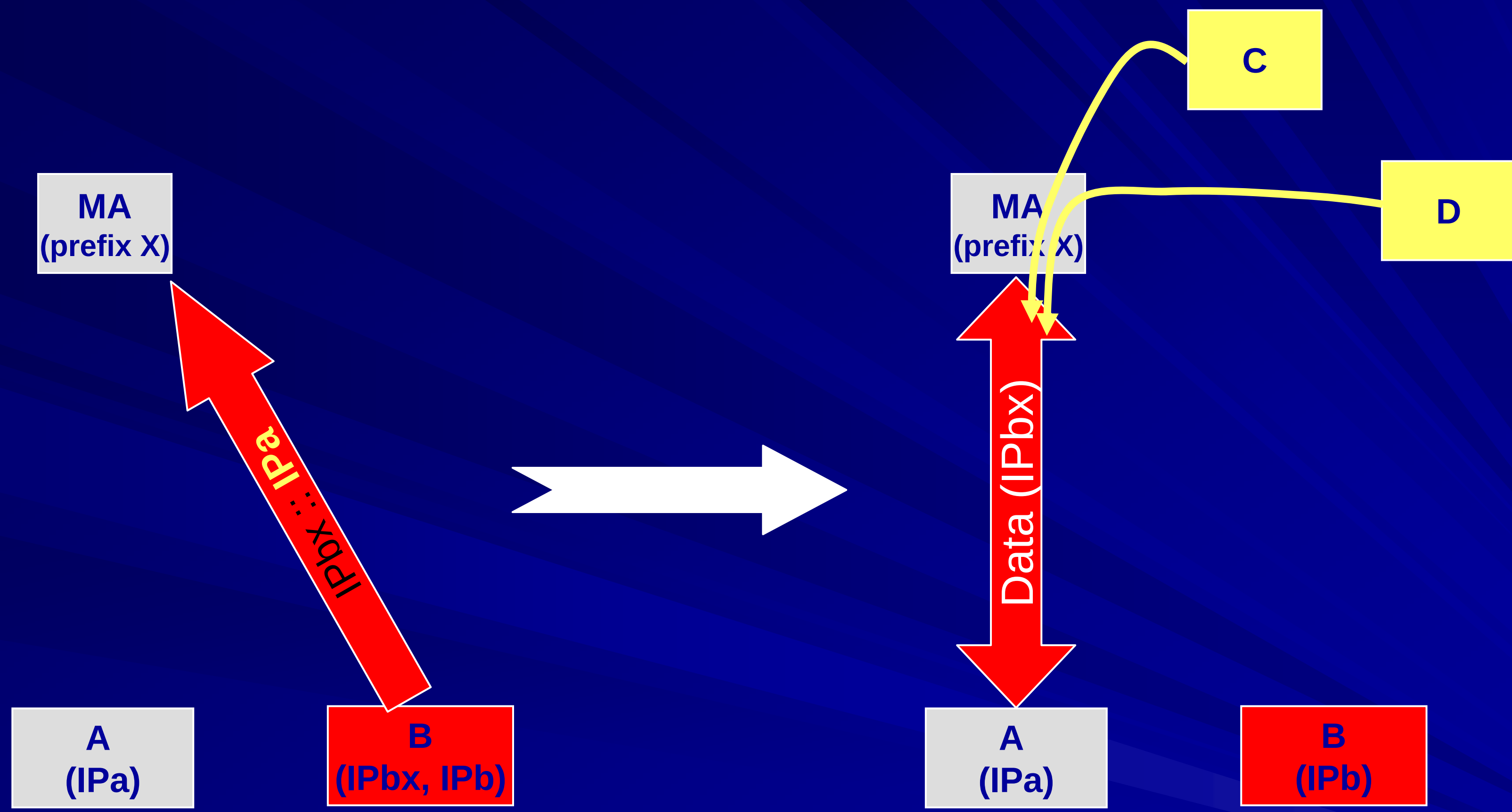
- ***IP mobility protocols make an off-path attacker as powerful as an on-path attacker***
- Redirection
  - Attacker registers victim's address as the "anchor" address
- Distributed DoS
  - Attacker registers victim's address as the "transient" address
- DoS attack on a mobile node
- Reflection attacks
- Passive attacks alone are not a concern
  - Mobility protocols themselves don't require confidentiality
    - Confidentiality for IP location privacy may change this
  - Data confidentiality can be achieved using end-to-end security

Redirection Attacks



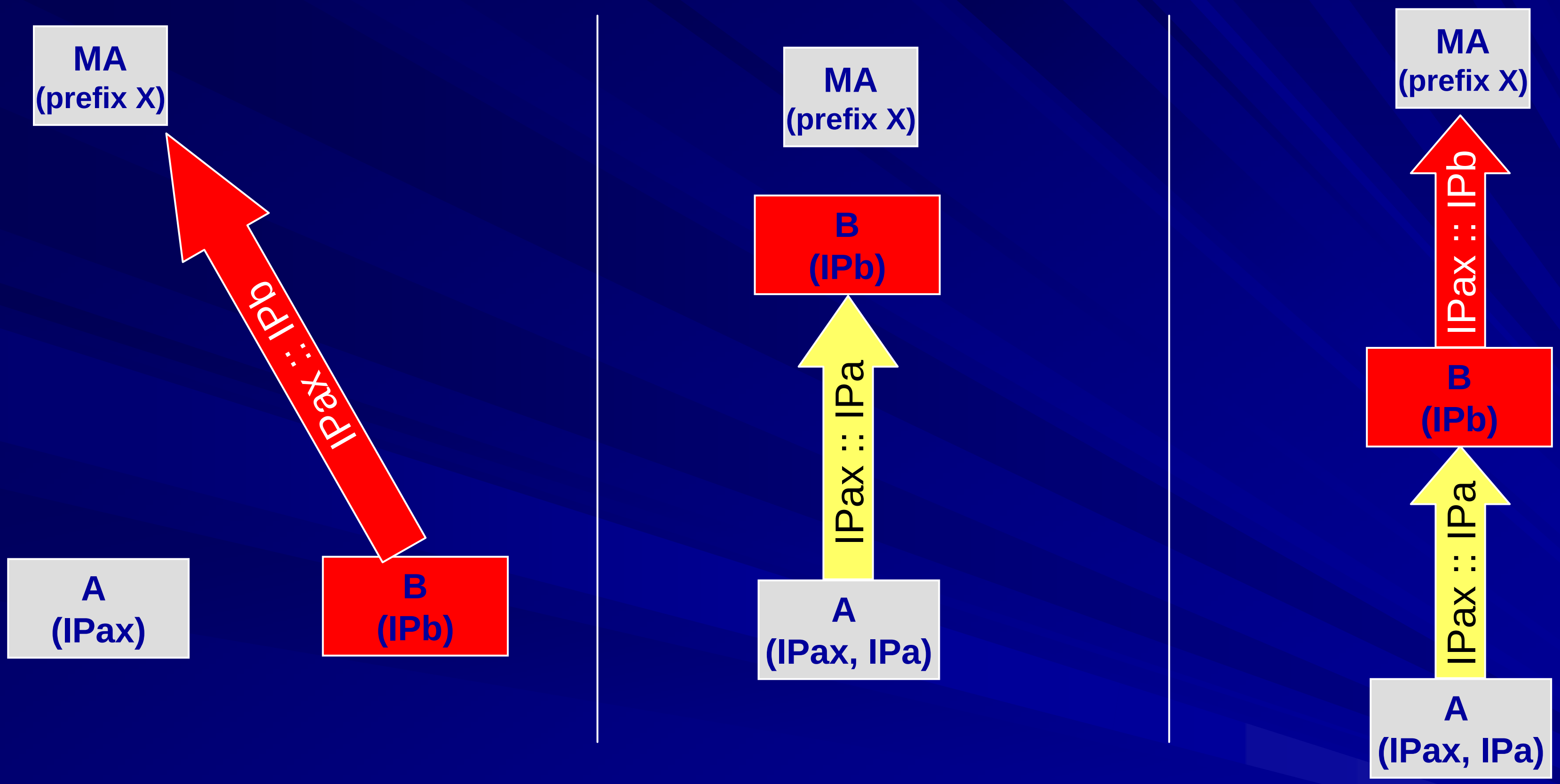
- Redirection of a victim's traffic to the attacker
- Target victims are nodes (fixed & mobile) on the prefix of the mobility agent

Distributed DoS Attacks



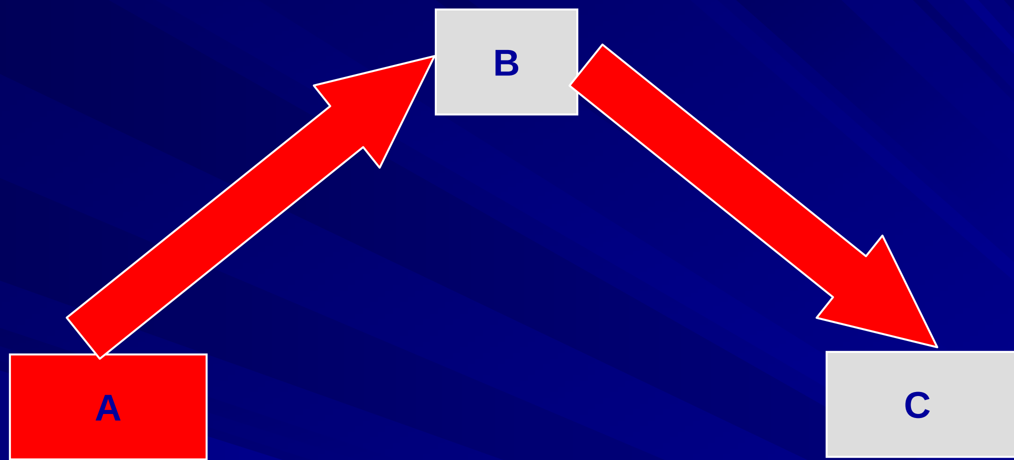
- Redirection of the attacker’s traffic to the victim
- DDoS can be caused by a variety of other ways, but IP mobility allows amplification

Denial of Service Attacks



- Disruption of service for an MN due to packet deletion/ modification/ bogus registrations

Reflection Attacks



- Cause responses to be sent to a victim (DDoS)
- Cause packets meant for the wrong address to be sent to the victim (forced redirection)

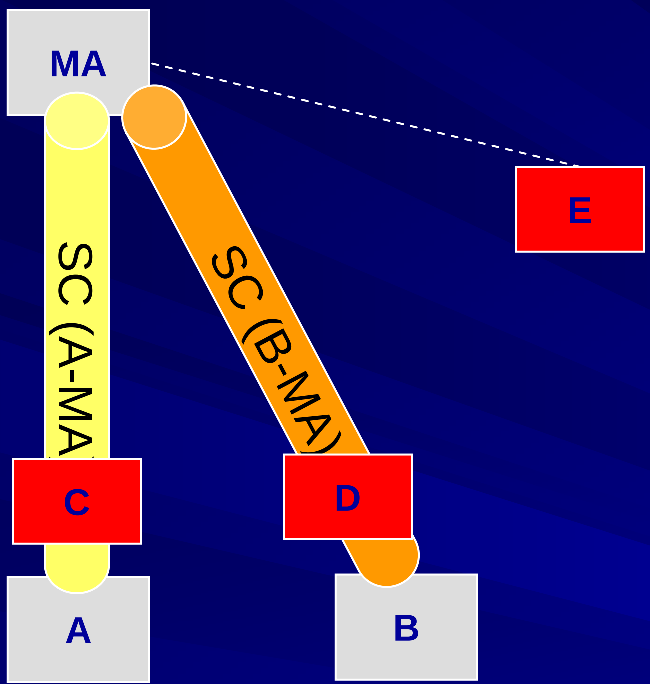
Outline

- Introduction and Goals
- Defining IP Mobility
- IP Mobility Models
- Typical network architecture
- Assets
- Internet Threat Model – A Recap
- Routing and IP Mobility
- Security analysis of IP mobility protocols
- Security Requirements
  - Channel security
  - IP Address Authorization
  - Entity Authorization
  - Protection against unrelated entities
  - Protection for unrelated entities
- Security Models

Security Requirements

- Channel Security
  - Data Origin Authentication
    - Integrity Protection
  - Replay Protection
- IP Address Authorization
- Entity Authorization
- Protection against compromise of non-critical assets
- Protection for non-participants

Channel Security

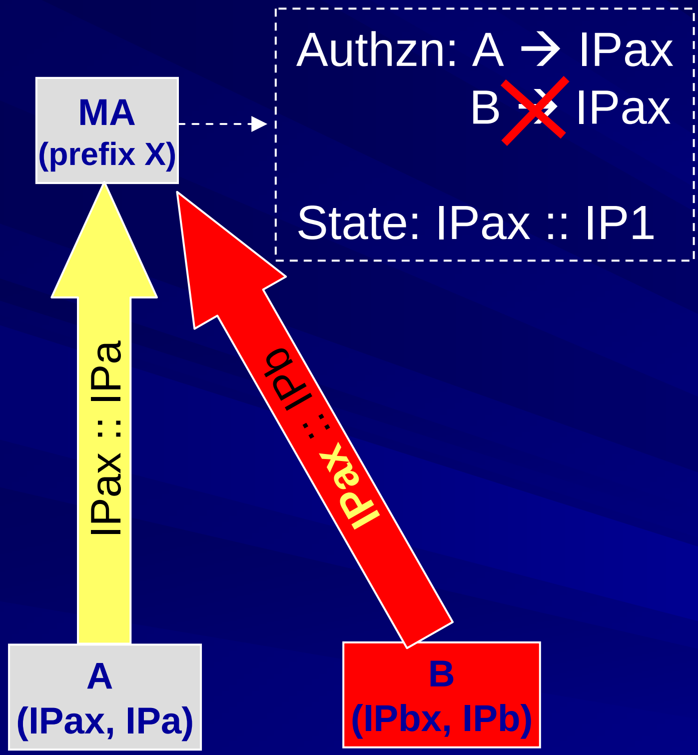


- Data Origin Authentication
  - Ensures creation of state at the mobility agent strictly by authorized nodes
- Integrity Protection
  - Really the same as data origin authentication!
  - Protects against redirection, MiTM, DoS and DDoS attacks
- Replay Protection
  - Protects against redirection, MiTM, DoS and DDoS attacks

A, B, MA – Signaling Endpoints
C, D – On-path Attackers
E – Off-path Attacker
SC (A-MA) – Unique Secure Channel b/w A & MA
SC (B-MA) – Unique Secure Channel b/w B & MA

Shared secure channels do not provide channel security!

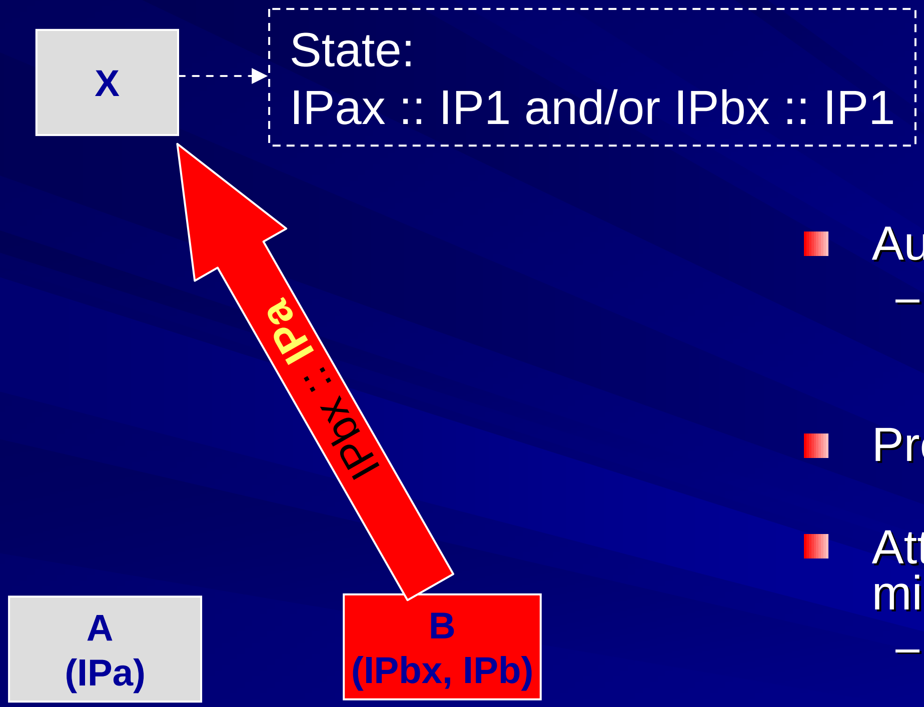
IP Address Authorization (1/2)



- Authorization for “anchor” address
  - MIP HoA, FMIP pCoA, HMIP RCoA, NETLMM LoA
- Ensures IP mobility service only for authorized nodes
- Protects against redirection, MiTM, and DoS attacks

Without authorization on the address being served, a lot breaks!

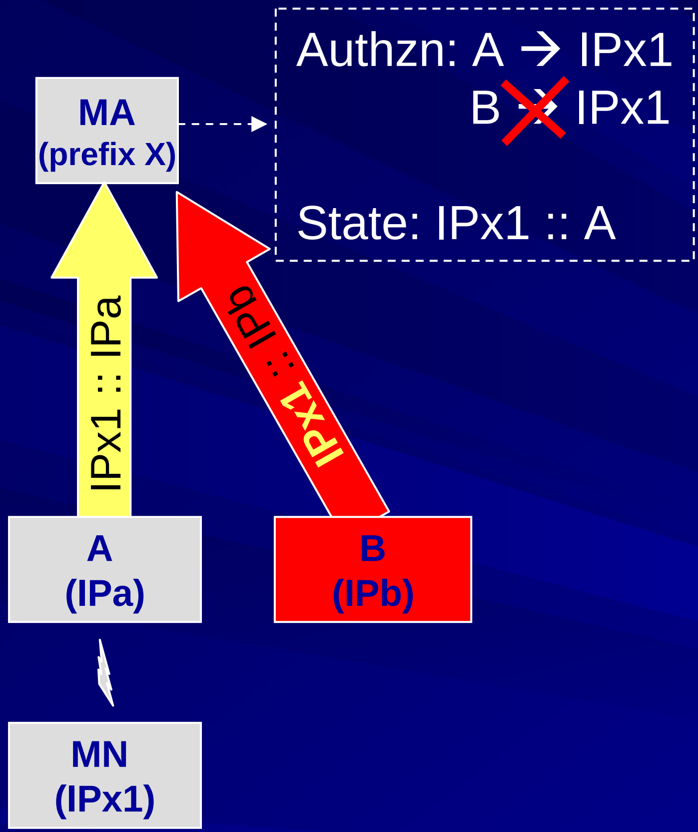
IP Address Authorization (2/2)



- Authorization for “transient” address
  - MIP CoA, FMIP nCoA, HMIP LCoA, NETLMM MAG
- Prevents a DDoS attack
- Attack needs to be detectable at a minimum
  - Authorization of “anchor” address allows detection of attack

If not protected or detectable, this would be an easier way to launch a DDoS attack on any node!

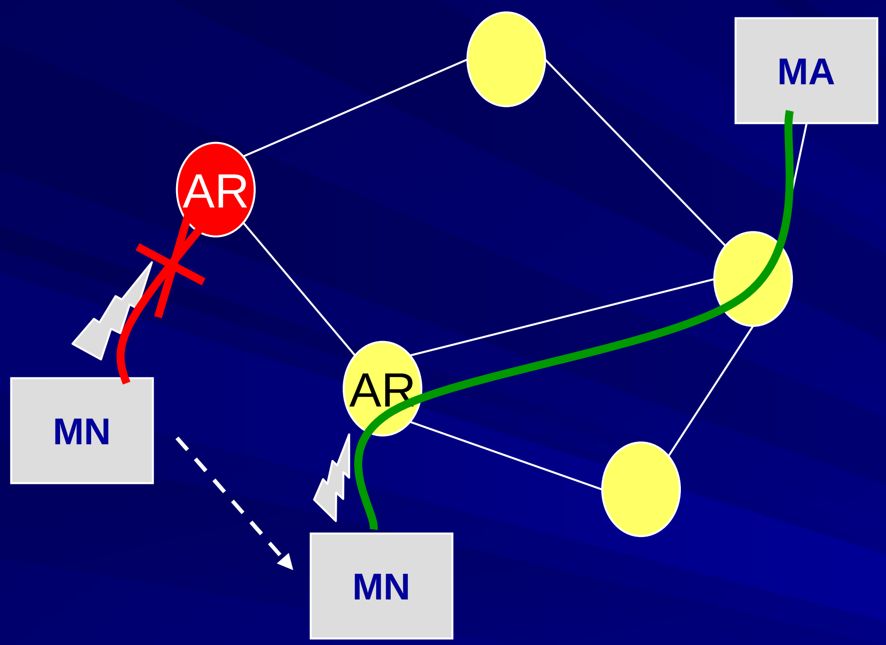
Entity Authorization



- Entity: Signaling endpoint
  - A and B are the "entities"
- Ensures IP mobility service for a given node only by authorized nodes
- Two parts to entity authorization
  - Is the entity part of the domain?
  - Is the MN actually at the entity?
- Particularly a concern in network-based mobility

Without entity authorization, compromise of the entity leads to compromise of any mobility session in the domain!

Protection Against Non-Critical Asset Compromise



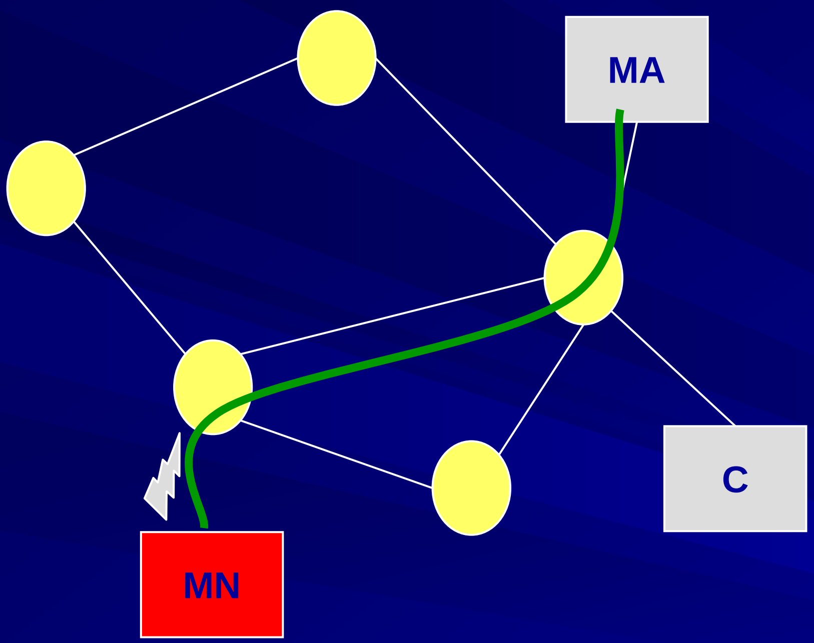
- Ensures service is not disrupted by non signaling entities
- Mitigates domino effects
- Ensures service via uncompromised entities
  - Entities: AR, HMIP AR, MIP4 FA, NETLMM MAG, FMIP nAR

Compromise of one entity MUST NOT impact sessions traversing other entities!

Domino Effect Mitigation

- Keys MUST be scoped for a given purpose
  - Same key must not be used for different purposes
- Keys MUST be scoped to the signaling endpoints
  - No key sharing!
- Non-critical assets MUST NOT be key distributors or trust anchors!

Protection for Unrelated Entities



- Ensures non-participants are unaffected by IP mobility sessions
- Allows routing and IP mobility to co-exist

IP mobility must not cause vulnerabilities to nodes not employing the protocol!

Takeaways

1. Channel security
2. IP address authorization
3. Entity authorization
4. Trust anchors should be security infrastructure entities
5. Key distributor must be located “above” the key recipient
6. Key scoping
7. No key sharing
8. Prevent domino effects
9. Analyze applicable threat and security models
10. Adhere to security model-specific guidelines

Backup Slides

Outline

- Introduction and Goals
- Defining IP Mobility
- IP Mobility Models
- Typical network architecture
- Assets
- Internet Threat Model – A Recap
- Routing and IP Mobility
- Security analysis of IP mobility protocols
- Security Requirements
- Security Models
  - AAA-based model
  - Role of EAP in IP mobility
  - Role of IPsec in IP mobility
  - CGA-based model

Security Models

- Various security models in use in different networks
- Security Model Considerations
  - Presence of infrastructure entity
    - E.g., AAA, PKI
  - Need for infrastructure-less security
    - E.g., CGA, self-signed certs
  - Use of existing security protocols
    - E.g., IPsec, IKEv2, EAP
  - End-to-end vs. hop-by-hop security
    - E.g., TLS, IPsec
- Popular security models
  - AAA-based authentication/authorization
  - Use of EAP for authentication
  - Use of IPsec for channel security and address authorization
  - Use of CGAs for infrastructure-less SA creation
- ***Threat analysis and security requirements conformance are vital***

AAA-based Authentication/Authorization

- Why AAA?
  - Allows re-use of AAA-based credentials
  - Several managed networks use AAA
  - Authentication and authorization are AAA functions
    - Authorization in AAA is different from IP address authorization
- What should AAA-based solutions conform to?
  - draft-housley-aaa-key-management (soon to be a BCP)

EAP in IP Mobility Protocol Security

- Why EAP?
  - EAP-based network-access authentication is popular
  - Re-use protocol supported by the MN and infrastructure
- Trends in using EAP
  - Minimize the number of authentications
    - Given, same credentials and the same server
  - Leveraging keys produced by one run of EAP for other purposes
  - Limiting re-use to protocol and performing another EAP run for IP mobility protocol security
- So, what usages of EAP for IP mobility protocol security are appropriate?

EAP Usage Guidelines

- Distinguish network access from IP mobility
  - One occurs *prior* to obtaining IP access; the other occurs after
- Use of EAP in IKEv2 for authentication is allowed and recommended
- Follow EAP guidelines on key usages
  - EAP MSK is provided to the authenticator for network access control
    - ***Usage of MSK for other purposes gets into bad cryptographic practices***
    - ***Usage of MSK involves the NAS in IP mobility protocol security***
- Use of EMSK-based keys for IP mobility protocol security is yet to be evaluated
  - General concerns on layer violations
  - Efforts underway to make the EMSK hierarchy generic to ensure future usage
  - No consensus yet on whether this is good or bad

IPsec in IP Mobility Protocol Security

- IPsec typically provides channel security
- Tying IP address authorization to IPsec
  - Assign IP address using IKEv2 and tie the IPsec SA to it
    - Limited flexibility in address assignment
- IPsec with Dynamic Keying
  - Use of IKEv2 is a recommended approach
- IPsec with Manual Keying
  - Cumbersome
  - No Replay protection
  - Address authorization needs static address provisioning
- The necessary security properties are realizable using IPsec and IKEv2
- Limitations of IKEv2 and IPsec
  - Frequent signaling endpoint changes (e.g., FMIP) needs new IKE_SAs
  - IKEv2 exchanges add undesirable overhead

CGA in IP Mobility Protocol Security

- Allows infrastructure-less operation
  - Useful in networks that care less about access control and more about address authorization
- Considerations in using CGAs
  - Differentiate between CGAs and SeND
    - SeND uses CGAs
      - CGAs provide the infrastructure-less security
    - CGAs do not mean AR involvement
  - Consider use of CGAs in IKEv2 to re-use IPsec
    - Currently undocumented
  - Consider if use of self-signed certificates will work
    - Currently documented for IKEv2
  - Evaluate if use of CGAs satisfies all security requirements