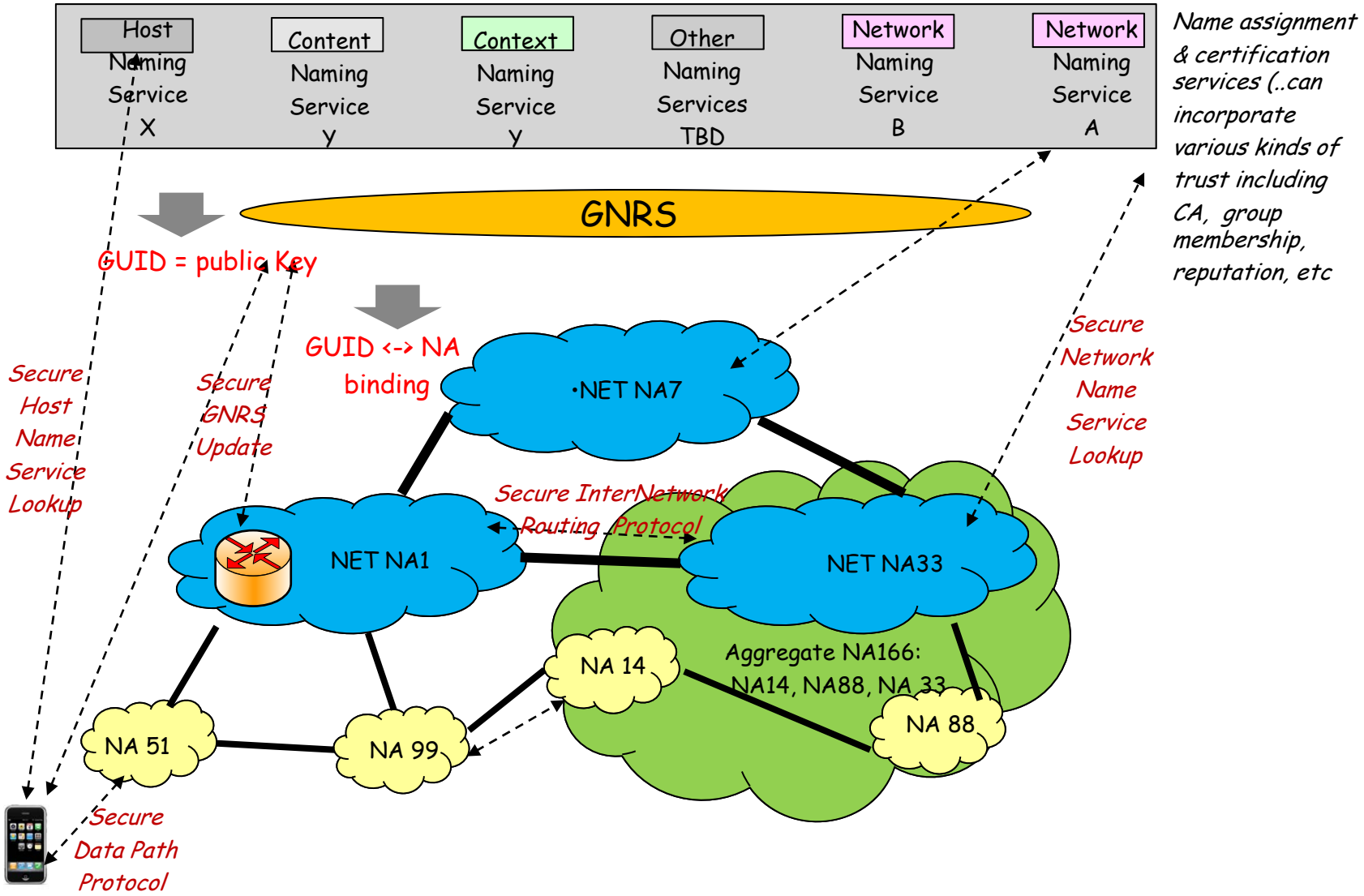
MobilityFirst: Security Analysis for the Architecture

Wade Trappe

Security Considerations: Trust Model



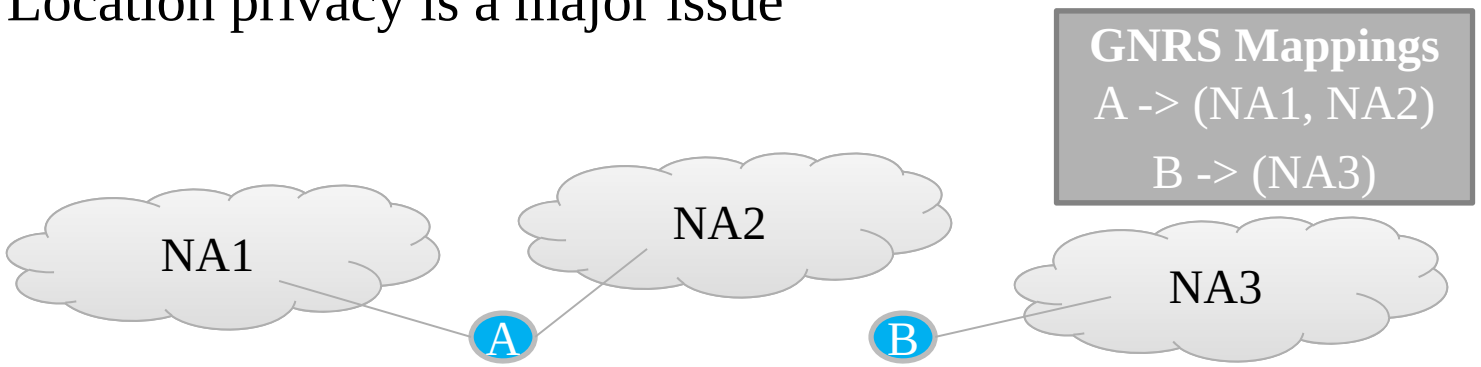
- *Public Key object and network names enable us to build secure protocols for each interface shown*

Specific Mobility First Security Mechanisms

Access Control	• GUID to NA mappings (GNRS) • Network resources (e.g., storage)
Service Integrity	• Secure routing protocols • Network monitoring (watchdog) • Multipath routing
Confidentiality/ Privacy	• GUID-based cryptography • Support for path randomization • GUID Pseudonymous

Name Resolution

- Fast, in-network name resolution is needed to allow flexible name/address separation
  - GNRS will be a *large-scale*, *distributed system* running over Internet routers
  - Updates and queries to a GNRS must not significantly delay messages
- Security related to name resolution
  - Attacks on name resolution can cause large-scale problems
  - Location privacy is a major issue

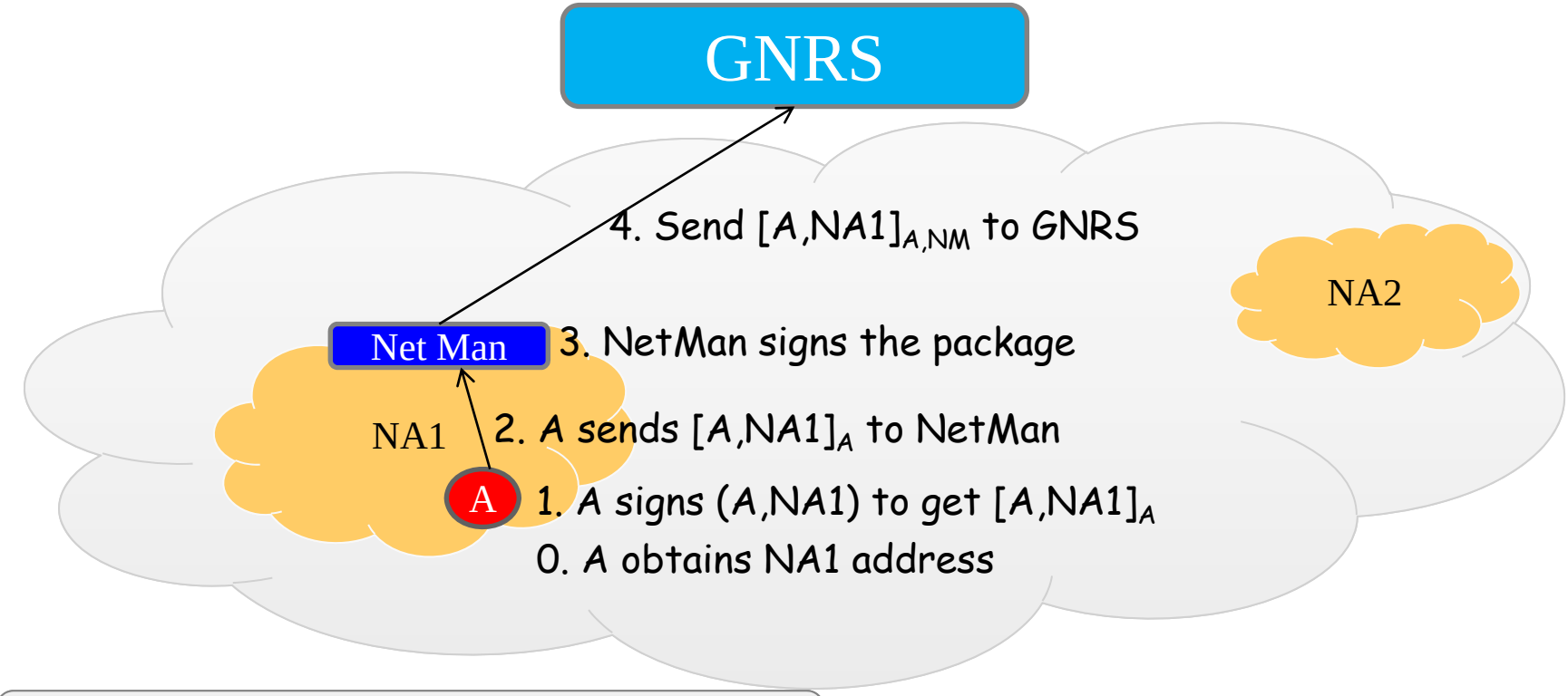


Attacks on the GNRS

1. False GUID
   - Malicious user claims wrong GUID binds to his address
   - Somewhat analogous to prefix hijacking
   - Solution: End devices sign their GNRS updates with their name
2. False NA
   - Malicious user claims his GUID binds to wrong address
   - Type of DoS attack
   - Solution: Network must also sign updates to the GNRS, after it verifies that the device belongs to it
3. Privacy – Repeated location queries for a GUID
   - Solution #1: Do nothing; this is inherent and not a concern
   - Solution #2: Access control in the GNRS
   - Solution #3: Allow for “forwarding agents” to be used if desired

Baseline GNRS Update Protocol

- To protect against attacks (1) and (2):



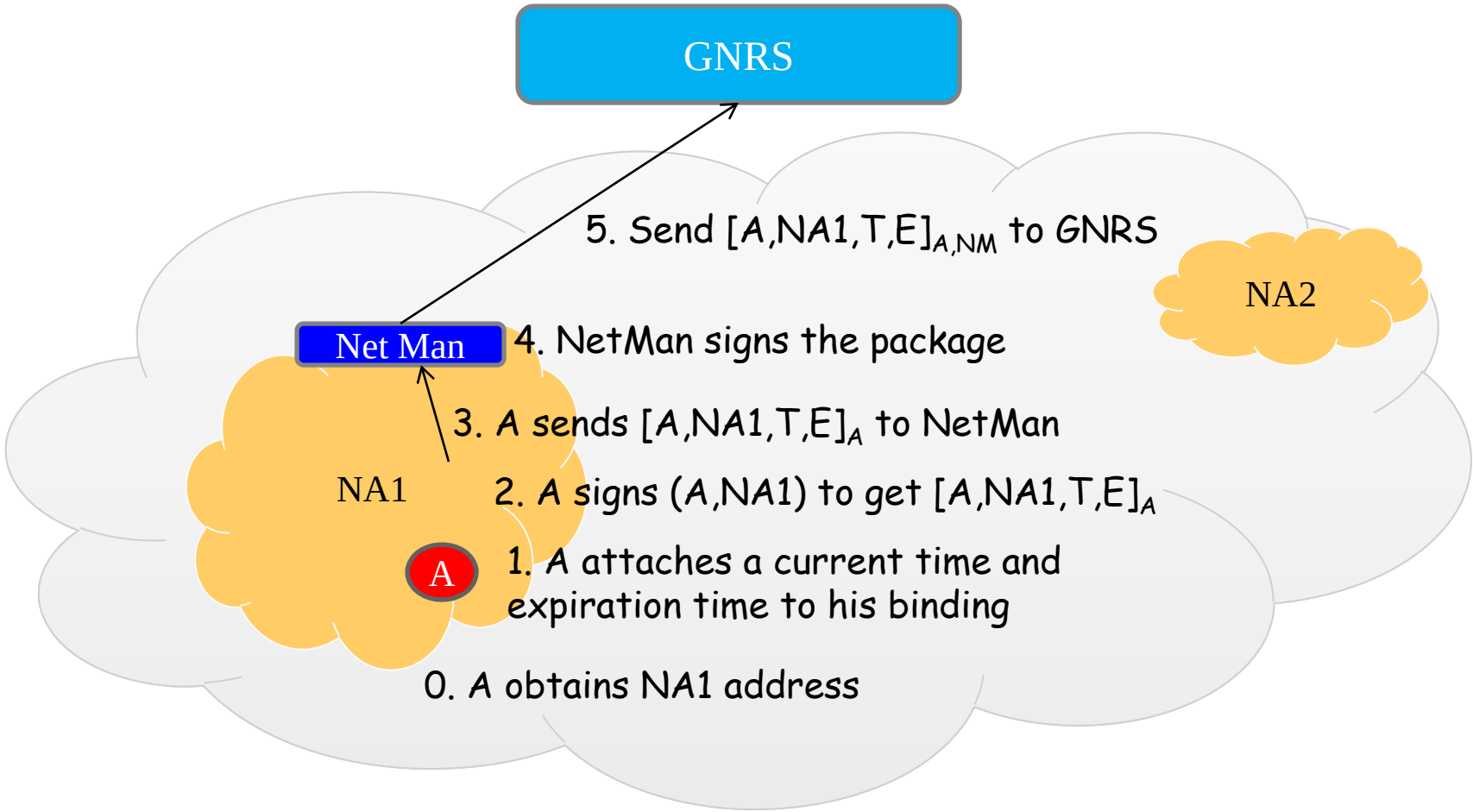
Open question: Can everyone validate a network signature?

What if the GNRS is Not Trustworthy?

- Since updates are signed, the GNRS **cannot** break the name/address binding.
  - Therefore, the GNRS cannot outright lie…
  - However, it can tell *stale truths*
- Attacks based on stale bindings:
  - If a device moves, a GNRS can purposely ignore the update and claim it still has the most recent one
  - Perhaps worse, a GNRS can selectively choose which (possibly stale) binding to give out during queries.

Security Decision: Binding updates must have generation time and expiration time *inside* the package

Adjusted GNRS Update Protocol

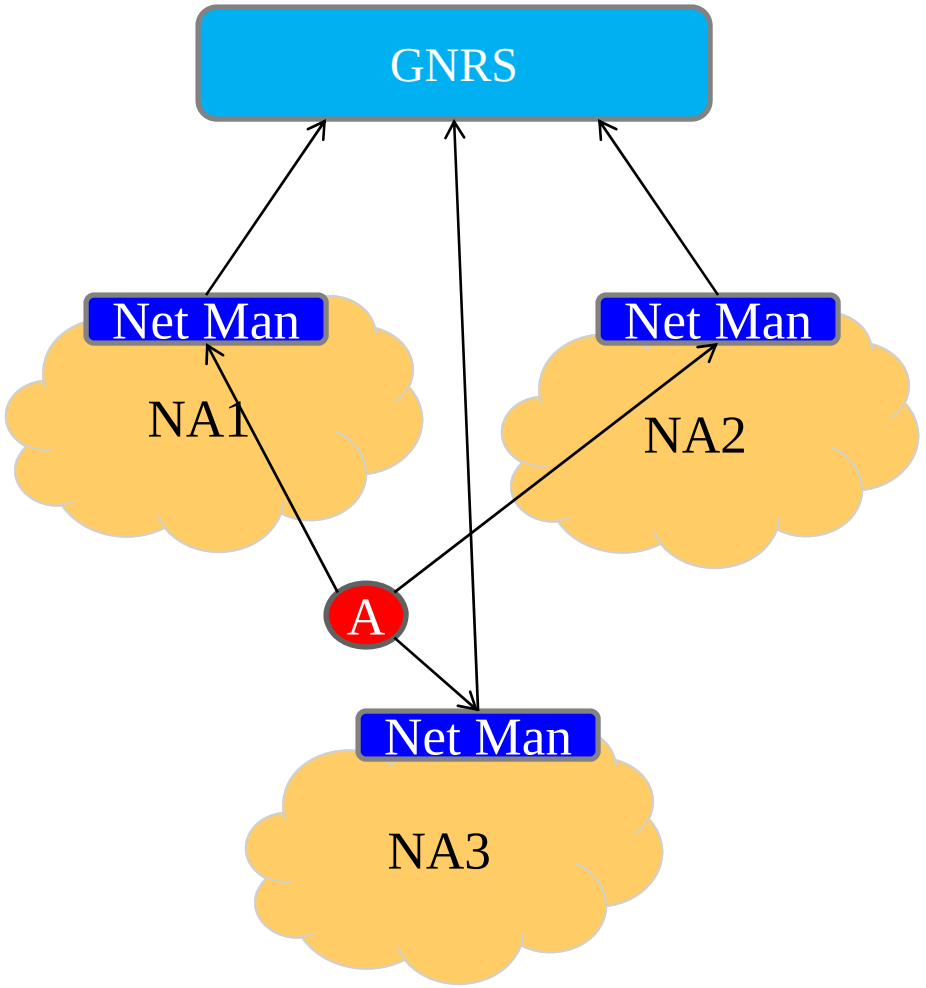


Updates for Multi-Homed Devices

- If a device has multiple homes, then problems arise:
  - Does [GUID, NA1, NA2, NA3] have to be signed by NA1, NA2, and NA3? How can these signatures be collected?
  - Or is it sufficient to have [GUID,NA1], [GUID,NA2], [GUID, NA3] as separate update messages?
    - *Note that this opens a new attack with an untrustworthy GNRS – the GNRS can selectively drop some messages to force data over certain interfaces*
  - What if I don't want NA1 to know about NA2 membership?
    - *Do we even want the GNRS to know where we are attached to?*

Possible Solution for Multi-Homed Updates

- Have three separate messages; however, indicate all interfaces in each message:
  - $[A, NA1, (NA2\&NA3)]_{A,NA1}$
  - $[A, NA2, (NA1\&NA3)]_{A,NA2}$
  - $[A, NA3, (NA1\&NA2)]_{A,NA3}$
- Queries should return all three messages
  - If any of the messages are missing then, the querying node can detect the corruption

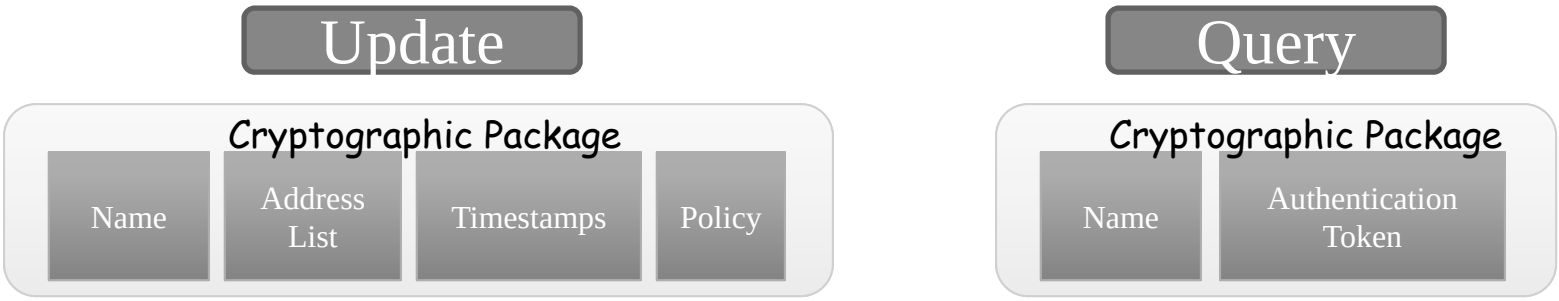


GNRS Query Protocol

- Users wishing to find the current address(es) of a name should simply query for the GNRS for that name
  - *Get(name)* returns 1 or more *signed packages*
- Verify that each returned package is properly signed
- Verify that the creation time on each package is *exactly* the same
- Verify that the expiration times are in the future
- Verify that the NA lists match for each package

Controlling Access to GNRS Information

- User should be able to specify:
  - Which people can see any information about the user's name
  - Which people can see which set of available interfaces mapped to the user's name
  - How frequently people are allowed to receive information about the user's name (similar to location privacy)
- User-initiated cryptographic techniques:
  - Encrypt specific updates with a group key only available to a target group
    - *Leads to key distribution problems*
- GNRS-based access control:
  - Updates contain a *policy* that specifies who can access what
  - Queries contain an *authentication token* that can be used in conjunction with the policy to supply appropriate information



Other Security Fronts

- Inter-domain routing
  - How will the future BGP be secured?
  - How much functionality do we take out of BGP and put into the GNRS?
    - *For example, BGP may only be responsible for AS reachability (path vector creation and maintenance)*
- Storage-capable routing
  - Necessary for any DTN functionality
  - Opens the door to storage-based attacks
- Context and content generation
- Name assignment services and GUID generation

Storage-Based Attacks

- If storage availability is used as a metric in path selection, then:
  - Malicious nodes can announce *infinite storage* and redirect all traffic through them
  - Malicious nodes can fill buffers on parallel paths and redirect all traffic through them
- Possible solution:
  - Limit the amount of influence a single node has on the path storage metric
    - *Average is bad (1 node changes everything)*
    - *Median is better (need at least n/2 nodes to arbitrarily change)*
  - Messages going into storage must be signed so they can be kept track of

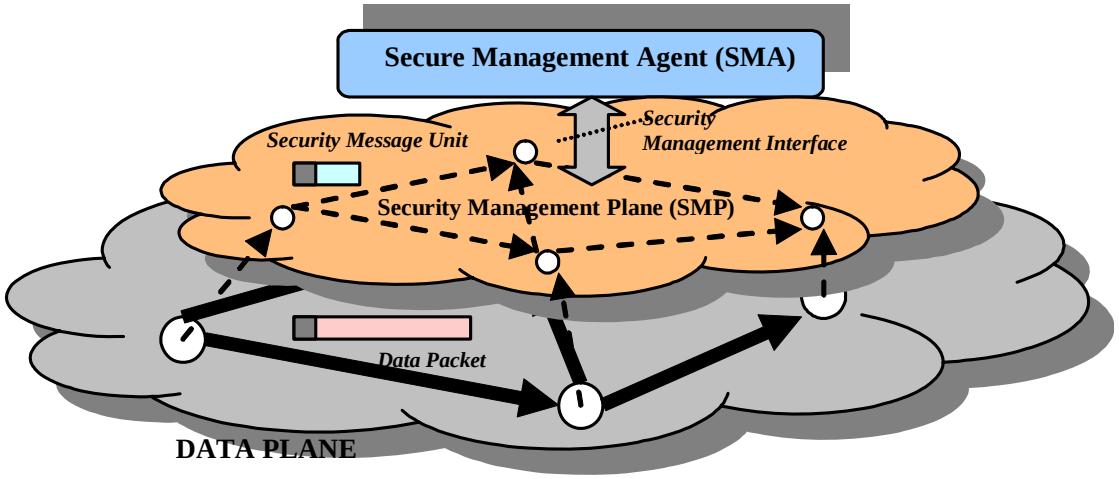
Appendix

Privacy Attack Solutions

Now let's consider privacy

- Solution #1: Do nothing.
  - This is inherently a problem in name/location mappings, and nothing to worry about.
- Solution #2: Access control in the GNRS
  - Either via end users encryption their updates with a group key only know to certain people or via a password-based GNRS system. The problem with the later is that the GNRS need to be trustworthy
- Solution #3: Allow for "forwarding agents" to be used if desired.
  - Users are free to bind their name to a forwarding agent, which forwards all traffic to the user. The downside is the forwarding agent may need the private key, the traffic route will be sub-optimal, and the forwarding agent may get overloaded

A Security Sub-Plane of the Management Plane Will Facilitate Security Services



- Security management plane will allow for the dissemination of management messages needed for:
  - Control of network resources
  - Reputation
  - Security Alarm
  - Software Attestation
- Management plane is distinct from routing and protocol control functions
  - Will be architected to use authenticated management frames

The use of public key naming addressing schemes facilitates access control through pairing-based (ID) cryptosystems

- Public key addressing allows the use identity-based cryptography to define access control policies
  - ID-based cryptography: a name or an identifier serves as the public key, which is used to encrypt data
  - The entity (or entities) associated with an identifier possess a private key issued by a trusted authority
  - Decryption can only be performed by entities in possession of the corresponding private key
- *MobilityFirst* packets could have addresses of the form (NA,HA) where NA is the network public key and HA is the host public key
  - The mathematics of pairing upon which ID-crypto is built allows for addresses and public keys to be specified in hierarchical manners using conjunctive and disjunctive forms
    - *Example 1: An NA may be {nsf.gov OR comcast.net OR WashDC OR USA}*
    - *Example 2: An HA may be {darleen.fisher OR victor.frost OR 703-292-8950}*
    - *Example 3: A complete address may be:*

      {(darleen.fisher@nsf.gov AND darleen.fisher@DC AND darleen.fisher@USA) OR (victor.frost@nsf.gov AND victor.frost@comcast.net)}
  - Packet payloads are encrypted using the address (which is also the public key) of the destination(s)
- Using such ID-crypto in public key addressing allows for flexible access control to data:
  - Data is encrypted at the source using the (single) public key that is derived by the logical conjunction and disjunction of destinations' identities (public keys)
    - *Example: Packet payloads can be encrypted so that either Darleen or Victor can access, but only the Darleen who is at NSF and in DC and in the USA, or the Victor who is at NSF and also has a Comcast account*
- Advantages:
  - Receivers can specify that they will only accept/decrypt packets that meet *their* policies
    - *Example: Darleen might say "I will only accept packets from those who know I am at NSF and currently in DC"*
    - *Such "stateful" policies can prevent receipt of unsolicited messages(i.e. spam)*

Overview of Project Security Objectives

- Identification of potential security threats and risks
  - The methods of such intrusions/subversions
  - The risks that may result from a successful attack
- Identification of potential services that could address threats and mitigate risks
  - Centered around core security goals
- Categorize security mechanisms and *specific* architectural and protocols that can yield security gains

(Some) Potential Security Threats

Unauthorized Access	– An intruder gains access or gathers information from a resource it is not entitled to – Confidential information can be examined, removed, modified
Eavesdropping	◆ **Intruder able to interact with the channel (e.g. wireless)** ◆ **In wireless mobile case, eavesdropping is untraceable**
Masquerading	– Occurs when an intruder is able to mimic an authorized user – Network resource/protocol believes the intruder is authorized user (e.g. impersonating source address, forging signatures, etc).
Modification of Information	◆ **Unauthorized information is injected into the network or its resources** ◆ **Modification can involve injection of false transmissions, or manipulations of network storage** ◆ **Routers may run "code" or instructions contained in falsified control messages**
Repudiation	◆ **Verification that a service was performed** ◆ **Either sender or receiver could try to deny that a service was provided** ◆ **Could potentially lead to disputes related to billing**
Replay, Misroute, Delete Messages	◆ **Replay: Intruder copies valid messages and attempts to reuse it for nefarious purposes** ◆ **Misrouting: Intruder sends messages to a wrong destination, perhaps to support traffic analysis** ◆ **Deletion: Intruder prevents messages from arriving to destination**
Network Flooding	◆ **Intruder sends an abundance of bogus messages** ◆ **Wastes network resources, leads to false allocation of resources to legitimate flows**

(Some) Potential Security Risks

Information Loss of Confidentiality	– Adversary has gained access to restricted information
	– Can be accomplished either at a host or on an network link
	– Occurs as a result of:
	  – Unauthorized access
	  – Masquerading
	  – Eavesdropping

Illegitimate Resource Consumption	◆ **Intruder uses resources that it is not entitled to**
	◆ **Occurs as a result of**
	  ◆ **Unauthorized access**
	  ◆ **Masquerading**
	  ◆ **Modification of Information**
	  ◆ **Replay, Misroute Messages**

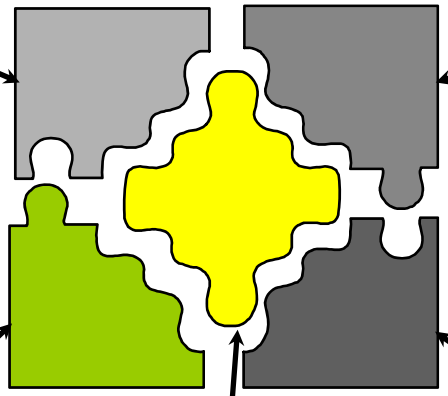
Stealing Services	– Adversary has obtained use of a service without proper privileges
	– Occurs as a result of:
	  – Unauthorized access
	  – Masquerading
	  – Modification of Information
	  – Repudiation
	  – Replay, Misroute, Deletion of Messages

Denial of Service	◆ **Adversary prevents a network entity from providing service as expected**
	◆ **Occurs as a result of:**
	  ◆ **Unauthorized access**
	  ◆ **Masquerade**
	  ◆ **Misrouting and Deletion of Messages**
	  ◆ **Network Flooding**

Security Services Can Be Built Around Security Goals

Access Control:
- Ensures that only legitimate network entitites can establish sessions with other entities
- Control access to network resources (e.g. GNRS or network storage)

Authentication:
- Entity authentication allows communicating parties to identify each other
  - Assures the responder of an association request that the request came from the correct entity
- Data origin authentication ensures that all messages in a session come from same origin (no hijacking of a session)



Confidentiality (and Privacy):
- Protects against passive monitoring/eavesdropping
- Adversaries may monitor messages in whole or in part
- In some cases, the context of a transaction (e.g. end points and their locations) are important to keep private

Non-repudiation:
- Prevents an entity from falsely claiming it did not participate in a service
- Non-repudiation of origin provides proof to a third party of an originator being involved
- Non-repudiation of reception provides proof to a third party of a recipient receiving a service

Integrity:
- Assures that network messages were not modified in transit
- Adversaries may attempt to manipulate messages in whole or in part
- Adversaries may also seek to disrupt the "integrity" of a service by delaying, deleting, reordering, misrouting, etc. messages through the network

How Security Services Address Threats

			Security	Threats			
Security Services	Unauthorized Access	Eavesdrop	Masquerade	Modification of Information	Repudiation	Replay, Misroute, Deletion	Network Flooding
Access Control	★			★			★
Authentication	★		★				
Integrity			★	★		★	
Confidentiality		★	★				
Non-repudation			★		★		