IDEAL ADDRESS TRANSLATION:

PRINCIPLES, PROPERTIES, AND APPLICATIONS

Pamela Zave

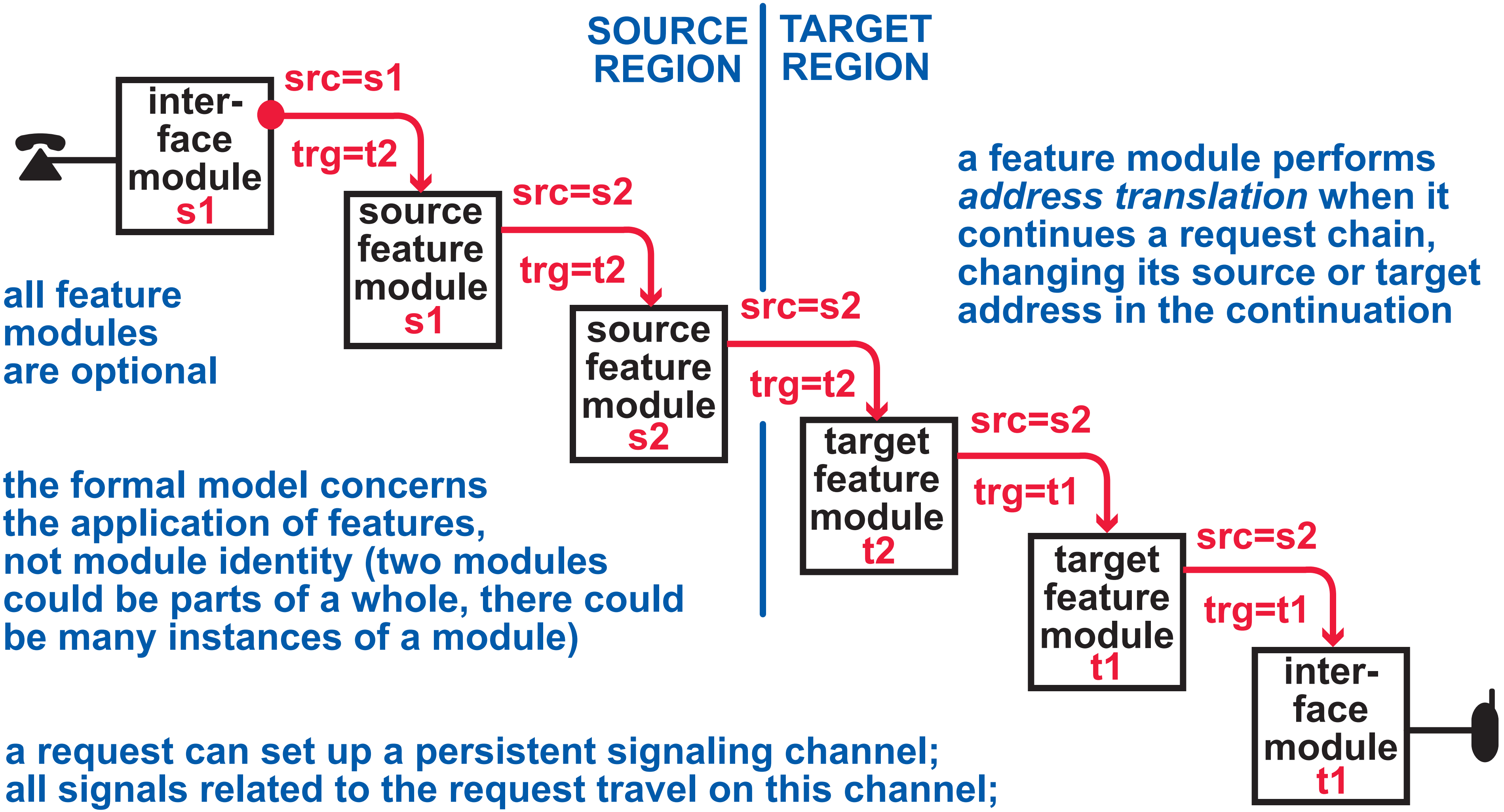
AT&T Laboratories—Research

Florham Park, New Jersey, USA

pamela@research.att.com

FORMAL MODEL: REQUEST CHAINS

A TELECOMMUNICATION NETWORK CONNECTS DEVICES BY CREATING REQUEST CHAINS



SOURCE REGION

TARGET REGION

interface module s1

src=s1

trg=t2

source feature module s1

src=s2

trg=t2

source feature module s2

src=s2

trg=t2

target feature module t2

src=s2

trg=t1

target feature module t1

src=s2

trg=t1

interface module t1

a feature module performs *address translation* when it continues a request chain, changing its source or target address in the continuation

all feature modules are optional

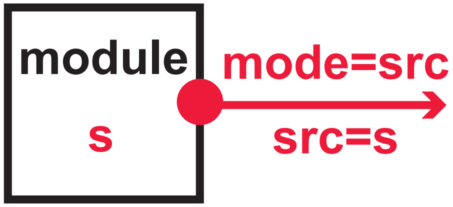
the formal model concerns the application of features, not module identity (two modules could be parts of a whole, there could be many instances of a module)

a request can set up a persistent signaling channel;
all signals related to the request travel on this channel;
media is controlled logically (but not physically) by these signals

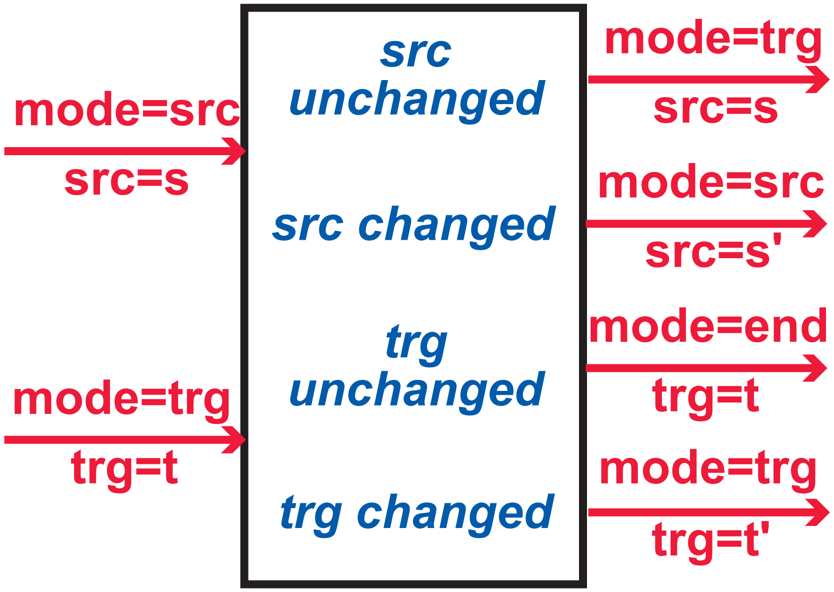
any part of a signaling channel can be torn down at any time

FORMAL MODEL: ROUTING ALGORITHM

INITIATING MODULE



CONTINUING MODULE

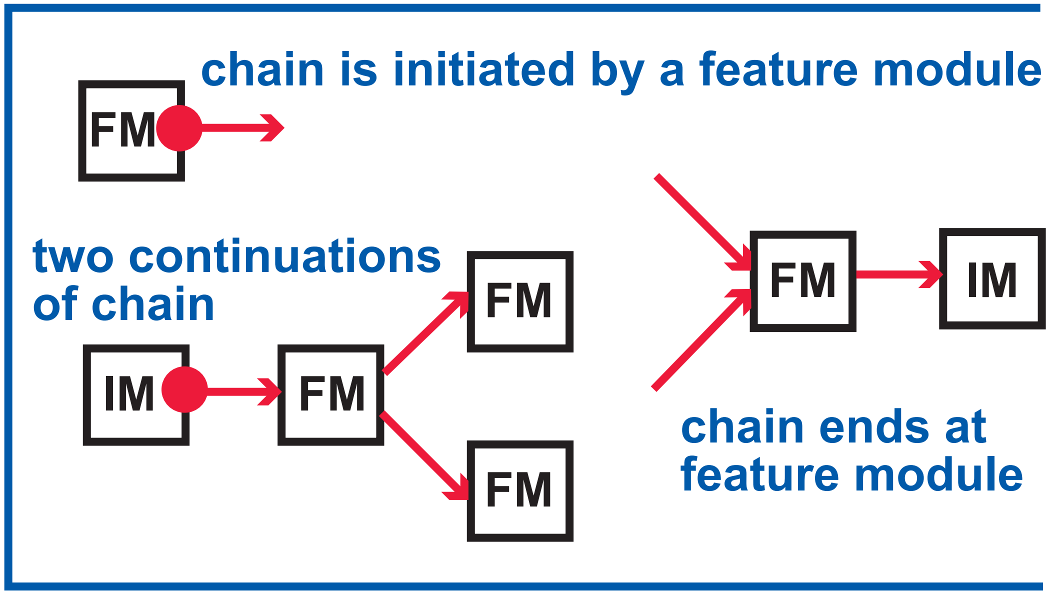


NETWORK ROUTER

```
if (mode==src) then
   if (src has SFM m) then route to m
   else {mode:=trg; restart routing}

if (mode==trg) then
   if (trg has TFM m) then route to m
   else {mode:= end; restart routing}

else (mode==end)
   if (trg has IM m) then route to m
   else route to error module
```



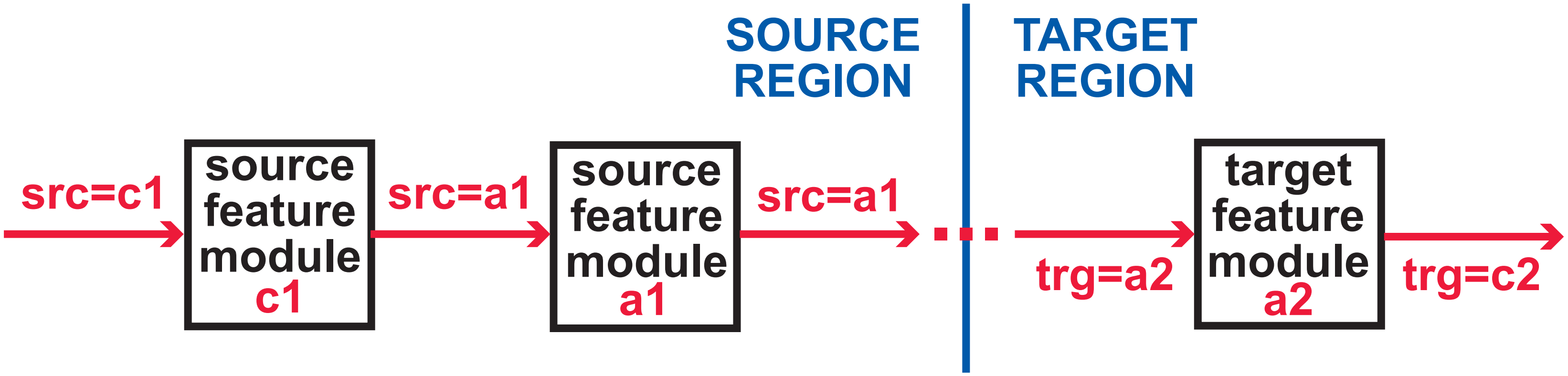
There is a bit of solution in this formulation of the problem,
but it is similar enough to all telecommunication protocols.

ADDRESS-TRANSLATION FUNCTIONS

WHAT FUNCTIONS ARE BEING PERFORMED?

WHY ARE THEY BEING PERFORMED?

ON WHOSE BEHALF ARE THEY BEING PERFORMED?



if a1 and a2 identify:	then the source translation is:	and the target translation is:
groups	*affiliation:* affiliate the caller with the group	*representation:* find a representative of the group
mobile entities	*positioning:* position the mobile entity at the location of the calling device	*location:* find the location of the mobile entity
roles	*assumption:* assume the role for the caller	*resolution:* translate the role to the entity playing the role

ORGANIZATION OF ADDRESSES

EACH ADDRESS HAS ONE OR MORE OWNERS

- an owner has rights and responsibilities
- an owner knows the authentication secret

ADDRESSES MUST BE CATEGORIZED ACCORDING TO WHAT THEY IDENTIFY OR REPRESENT

for example:

- device
- person
- group
- role

and combinations thereof

ADDRESS CATEGORIES MUST BE PARTIALLY ORDERED BY "ABSTRACTION"

by definition:

- a group is more abstract than a person representing the group
- a person is more abstract than a device where he is located
- a public role is more abstract than a private identity

THE PRIMARY PURPOSE OF ADDRESS TRANSLATION IS TO CHANGE LEVEL OF ABSTRACTION

- in the source region, source addresses become successively more abstract
- in the target region, target addresses become successively more concrete

INTERACTION: IDENTIFICATION

PEOPLE AND FEATURE MODULES USE ADDRESSES TO IDENTIFY THE PARTIES WITH WHOM THEY ARE COMMUNICATING

A FEATURE THAT PERFORMS ADDRESS TRANSLATION INTERACTS WITH OTHER FEATURES BY AFFECTING THE IDENTIFICATION INFORMATION THEY RECEIVE

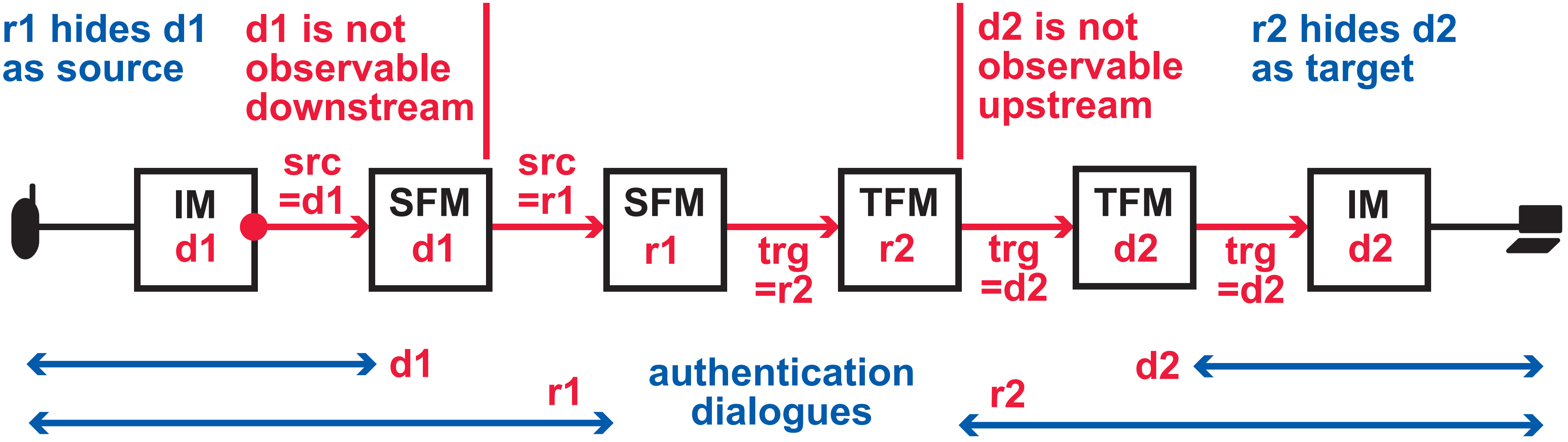
These principles balance conflicting goals:

PRIVACY

A person should be able to conceal a more private address that he owns behind a more public address that he owns.

AUTHENTICITY

A person should not be able to pose as an owner of an address he does not own.



INTERACTION: CONTACT

PEOPLE AND FEATURE MODULES USE ADDRESSES TO CONTACT THE PARTIES WITH WHOM THEY WISH TO COMMUNICATE

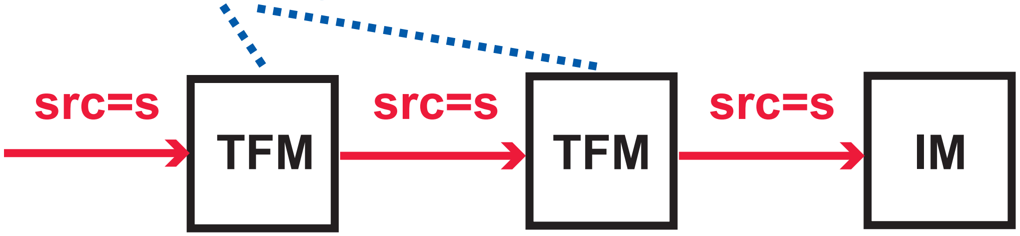
A FEATURE THAT PERFORMS ADDRESS TRANSLATION INTERACTS WITH OTHER FEATURES BY AFFECTING THE CONTACT INFORMATION THEY RECEIVE

REVERSIBILITY

A target feature module or callee should be able to call the source address of a request chain and and thereby target the entity that initiated it.

this is the most abstract source address, not the caller device

feature modules in the target region do not change the src address



~~REPRODUCIBILITY~~

~~A feature module or person should be able to call the same entity twice and be connected to the same representative of that entity.~~

conflicts with mobility and the freedom of representation functions

INTERACTION: INVOCATION

THE ADDRESSES IN A REQUEST CHAIN DETERMINE WHICH FEATURE MODULES ARE IN THE CHAIN

A FEATURE THAT PERFORMS ADDRESS TRANSLATION INTERACTS WITH OTHER FEATURES BY AFFECTING WHICH FEATURES ARE INVOKED

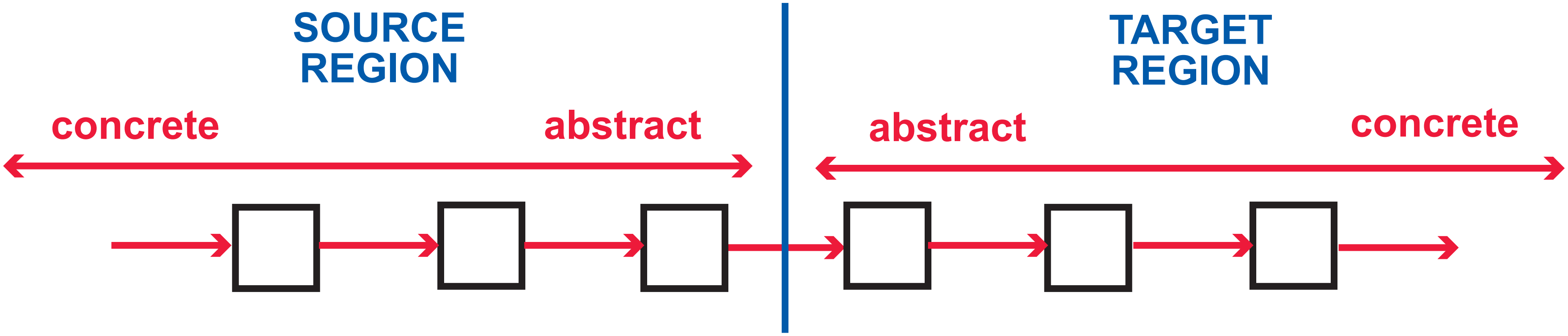
BOUNDEDNESS

The numbers of source and target feature modules in a chain should be bounded.

MONOTONICITY

In a region, the feature modules of more concrete addresses should be closer to the outer end of the region than feature modules of more abstract addresses.

leads to



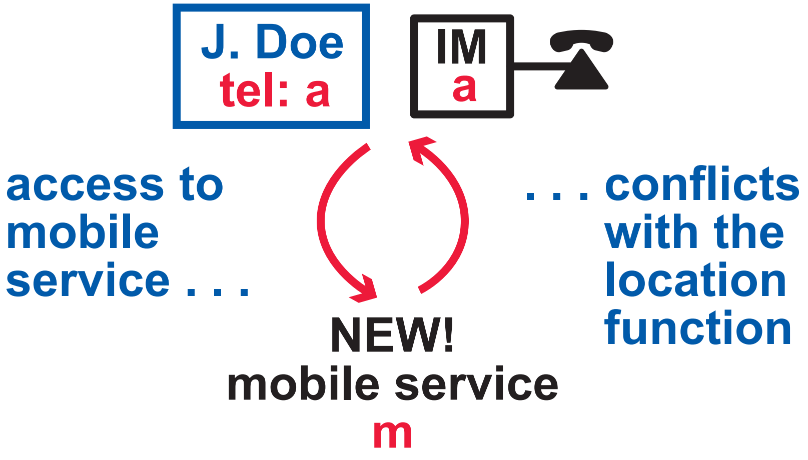
each feature module knows where the more abstract and more concrete features are

features can be prioritized and coordinated (e.g., by token passing) without knowledge of other features

ASSUMPTIONS AND BEHAVIORAL CONSTRAINTS

ASSUMPTIONS

- there is a global, one-to-one mapping between addresses and meanings
- there is a finite set of address categories
- each address belongs to exactly one category
- the abstraction relation on address categories is an irreflexive partial order



J. Doe
tel: a

IM
a

access to mobile service . . .

NEW!
mobile service
m

. . . conflicts with the location function

CONSTRAINTS

Constraint 1:

A target feature module in a request chain does not change the source address of the chain.

Constraint 2s:

If a source feature module in a request chain changes the source address, the new address is more abstract than the old one.

Constraint 2t:

If a target feature module in a request chain changes the target address, the new address is more concrete than the old one.

Constraints 3s and 3t: other signaling maintains the spirit of these constraints

PROPERTIES FORMALIZE THE PRINCIPLES, ARE GUARANTEED BY THE CONSTRAINTS

MONOTONICITY

In a request chain that satisfies Constraint 2s [2t], if *m1* and *m2* are feature modules in its source [target] region, and *m1* precedes *m2*, then the address of *m1* is more concrete [abstract] than the address of *m2*.

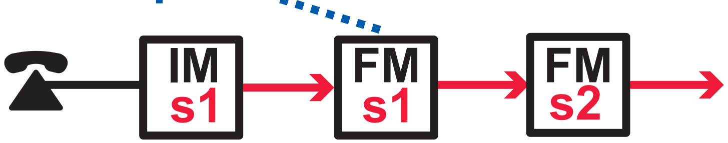
PRIVACY (target side not given)

If *s1* is a source address in a request chain that satisfies Constraints 1 and 2s, and if *s1* has a source feature module that changes the source to *s2* in this chain, then *s1* is not observable as a source of this chain downstream of its own source feature module.

AUTHENTICITY (target side not given)

If *s2* is a source address in the target region of a request chain that satisfies Constraints 1 and 2s, and if *s2* has a source feature module with unconditional authentication, then either an owner of *s2* is present at the initiating device, or its owner also owns a more concrete source address *s1* in the chain.

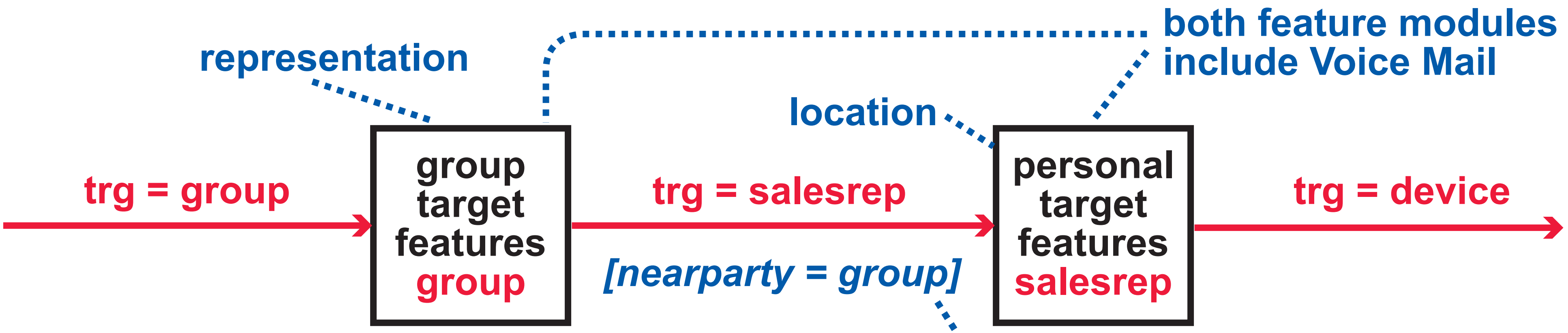
owner of both addresses put secret of *s2* in here



real properties are more complex because of signaling

proofs are mostly automated with the Alloy constraint analyzer (there are some manual steps)

EXAMPLE: THE SALES REPRESENTATIVE



representation

both feature modules include Voice Mail

location

trg = group

group target features group

trg = salesrep

[nearparty = group]

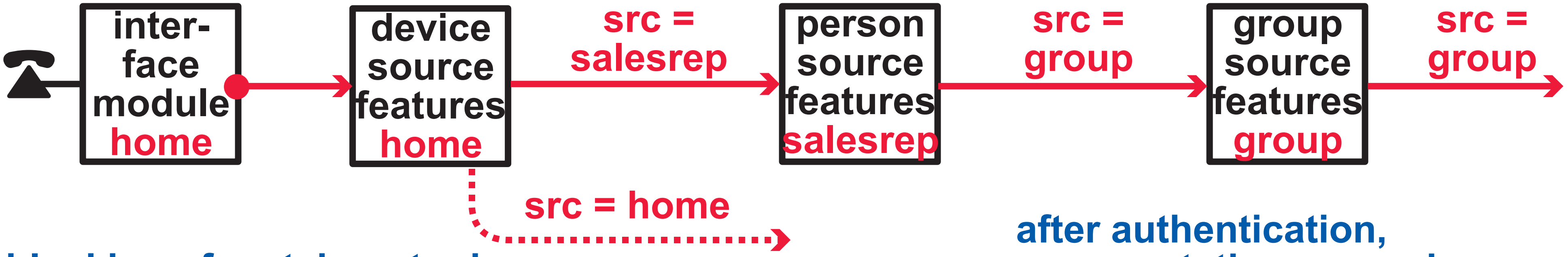
personal target features salesrep

trg = device

group features (including Voice Mail) should take priority over personal failure treatments (including Voice Mail) because:

- if a representative is not available, the best failure treatment is to find another one
- if no one is available, should record a message accessible to the whole group

signal tells cooperating features to abdicate; it does not violate privacy, and there is no assumption that personal features are present



inter-face module home

device source features home

src = salesrep

person source features salesrep

src = group

group source features group

src = group

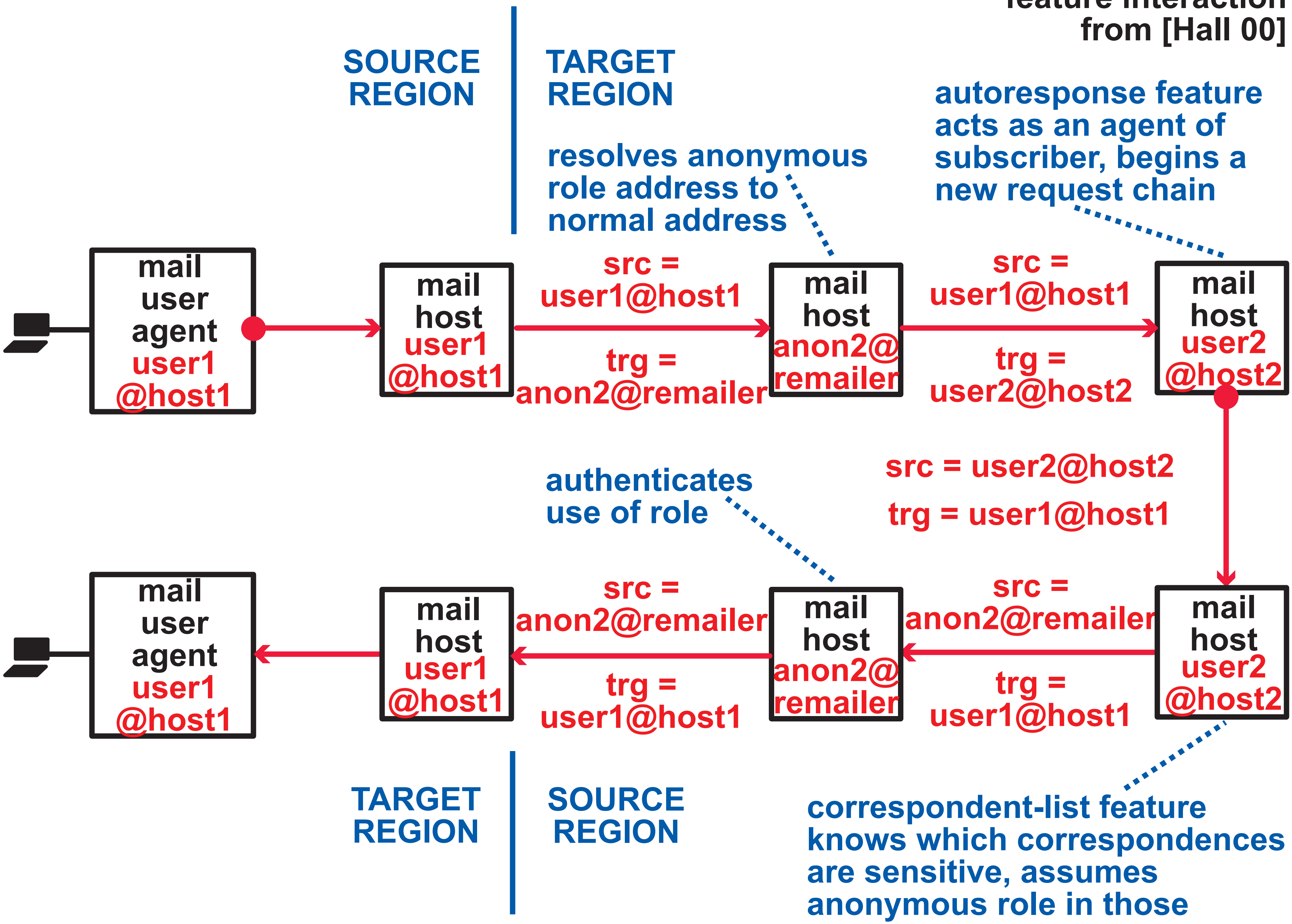
src = home

blocking of certain outgoing calls applies only when no identification function applies

after authentication, representative can make personal and business calls from shared home telephone

EXAMPLE: ANONYMOUS ELECTRONIC MAIL

fixing a bad
feature interaction
from [Hall 00]



SOURCE REGION

TARGET REGION

resolves anonymous role address to normal address

autoresponse feature acts as an agent of subscriber, begins a new request chain

mail user agent user1 @host1

mail host user1 @host1

src = user1@host1

trg = anon2@remailer

mail host anon2@ remailer

src = user1@host1

trg = user2@host2

mail host user2 @host2

src = user2@host2

trg = user1@host1

authenticates use of role

mail host user2 @host2

src = anon2@remailer

trg = user1@host1

mail host anon2@ remailer

src = anon2@remailer

trg = user1@host1

mail host user1 @host1

mail user agent user1 @host1

TARGET REGION

SOURCE REGION

correspondent-list feature knows which correspondences are sensitive, assumes anonymous role in those

VALIDITY OF IDEAL ADDRESS TRANSLATION

VOICE-OVER-IP SERVICES DEVELOPED AT AT&T

- Distributed Feature Composition (DFC, [Jackson & Zave 98]) is a feature-modular architecture

- BoxOS [Bond *et al.* 02] is a voice-over-IP platform that is an implementation of DFC

- we have built a variety of innovative services on this platform

- we always adhere to ideal address translation—it is the only way we can make sense of the interactions in our complex feature sets

MODULARITY AND EXTENSIBILITY

- a feature module does not need to cooperate explicitly with others, or know which others are present

- adding (or deleting) compliant features does not require changing existing (or remaining) features

HALL [Hall 00] ON FEATURE INTERACTIONS IN ELECTRONIC MAIL

- 26 undesirable feature interactions, of which 12 have nothing to do with address translation

- the remaining 14 are predicted and would be corrected by ideal address translation

APHRODITE AGENT-BASED ARCHITECTURE [Pinard 03]

- has three address categories, which are totally ordered

- architecture seems to comply with ideal address translation

RELATION OF IDEAL ADDRESS TRANSLATION TO THE REAL WORLD OF NETWORKING

THERE ARE MANY REASONS WHY THE REAL WORLD MIGHT NOT CONFORM TO THE IDEAL

- inadequate infrastructure
- legacy of noncompliant features or address mappings
- interoperation with untrusted networks
- unwise optimizations
- one legitimate case in which a constraint is (deliberately) too strong

THERE ARE MANY WAYS TO COPE WITH THESE EXCEPTIONS

- refine or adapt the reasoning
- trace which properties do and do not hold
- enforce the constraints in a subnetwork only

DESPITE THE EXCEPTIONS, IDEAL ADDRESS TRANSLATION HAS PROVEN VERY USEFUL BECAUSE . . .

. . . even a subnetwork can have very complex feature interactions

. . . principles, constraints, properties, and reasoning are all models that we approximate as closely as possible

. . . it helps us understand infrastructure requirements

FOR MORE DETAILS:

http://www.research.att.com/projects/dfc