PART THREE:

IDEAL ADDRESS TRANSLATION

less formal, less complete, more pragmatic than the previous lecture on connection paths

this lecture uses DFC, because ordinary network routing is not rich enough
ADDRESS TRANSLATION AND FEATURE AMBIGUITY

ADDRESS TRANSLATION IS A VERY COMMON FEATURE FUNCTION
ADDRESS TRANSLATION CAUSES A WIDE VARIETY OF FEATURE INTERACTIONS

A, B, and C are addresses
a typical address-translation feature
If calls from A to B are being forwarded to C, then . . .

typical questions about feature interaction
. . . what caller identification does C receive?
. . . if C has forwarding active, does it apply to this call?

To give good answers to such questions, you would have to know . . .

. . . who or what do the addresses represent?

. . . on whose behalf is the forwarding being performed?

. . . and for what purpose?

. . . how does the network guarantee authentic identification?
EXAMPLE

X is forwarding to Y
Y is forwarding to Z
if X is called, should the call be forwarded to Z?

X is on vacation, Y is X's secretary, . . .
Y is on vacation, X is using Y's office,...

. . . and the answer is "yes"
. . . and the answer is "no"
DFC ROUTING (VERSION 1)

`new method creates setup signal`

interface module `s1`

`regn=src`

`src=s1`

`trg=t3`

`route=full`

```
source feature module `s1`
```

`src=s2`

`route=full`

`route=empty`

```
source feature module `s2`
```

`route does not change because `src` does not change`

```
target feature module `t3`
```

`regn=trg`

`src=s2`

`trg=t2`

`route=full`

```
target feature module `t2`
```

`t1 has no target feature module`

```
target feature module `t1`
```

`regn=trg`

`src=s2`

`trg=t3`

`route=empty`

```
target feature module `t3`
```

`regn=trg`

`src=s2`

`trg=t2`

`route=empty`

```
target feature module `t2`
```

`regn=trg`

`src=s2`

`trg=t1`

`route=full`

```
target feature module `t1`
```

`route changes because `src` changes`

`regn changes because source region is exhausted`

`route changes because `trg` changes`

if target region is exhausted, route to interface
ADDRESS-TRANSLATION FUNCTIONS

WHAT FUNCTIONS ARE BEING PERFORMED?  WHY ARE THEY BEING PERFORMED?  ON WHOMS 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.

- **r1** hides **d1** as source
- **d1** is not observable downstream
- **src =d1**
- **src =r1**
- **d2** is not observable upstream
- **r2** hides **d2** as target
- **trg =r2**
- **trg =d2**
- **src =d1**
- **trg =d2**

**Authentication dialogues**

- **r1**
- **d1**
- **r2**
- **d2**
INTERACTION: CONTACT

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

RETURNABILITY

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.

RETURNABILITY

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.

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

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

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

TFM src=s TFM src=s IM
**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.

---

**SOURCE REGION**

concrete

abstract

Each feature module knows where the more abstract and more concrete features are.

---

**TARGET REGION**

abstract

concrete

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.

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.

NEW! mobile service . . .

access to mobile service . . . conflicts with the location function
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 \( m2 \).

**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.

**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.

Real properties are more complex because of signaling.

Informal proofs, some also checked with Alloy Analyzer.
A BAD FEATURE INTERACTION: MULTIPLE TARGET ADDRESSES

Alice calls the number of a sales group to Sales

Sales feature selects a representative on duty

call is answered by Bob's voicemail

the correct behavior is to select another sales representative

Bob's cellphone is turned off

to Bob

Select Representative Sales

Voice Mail Bob
EXAMPLE: THE SALES REPRESENTATIVE

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.

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

Blocking of certain outgoing calls applies only when no identification function applies.
A BAD FEATURE INTERACTION: ABSENCE OF DUALITY

Bob@host2 wishes to be anonymous to Alice@host1

contains features of Bob@host2, including an Autoresponse feature

"I'm on vacation"
EXAMPLE: ANONYMOUS ELECTRONIC MAIL

SOURCE REGION

TARGET REGION

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

resolves anonymous role address to normal address

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

SOURCE REGION

TARGET REGION

autenticates use of role

mail user agent user1@host1

mail host user1@host1

src = user1@host1

trg = anon2@remailer

mail host anon2@remailer

src = user1@host1

trg = user1@host1

mail host user1@host1

src = user2@host2

trg = user1@host1

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

mail user agent user1@host1

mail host user1@host1

src = user1@host1

trg = anon2@remailer

mail host anon2@remailer

src = user1@host1

trg = user1@host1

mail host user1@host1

src = user2@host2

trg = user1@host1

mail host user2@host2

src = user2@host2

trg = user1@host1
cannot implement this solution with today's electronic-mail protocols

this approximation of it is routinely used in electronic mail and telephony

all of the property reasoning can be adapted (mostly, refined) for this special case:

- assumptions are stronger (more specialized)
- conclusions are weaker (more specialized)
VALIDITY OF IDEAL ADDRESS TRANSLATION

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.

VOICE-OVER-IP SERVICES DEVELOPED AT AT&T

- We have built services for demonstration, for small-scale deployment, and for large-scale deployment.
- We always use ideal address translation.
- If the product management does not let us use the right abstract addresses overtly, we have to insert them covertly to make the features interact correctly.

HALL 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 by and would be corrected by ideal address translation.

HELPS US THINK ABOUT FEATURES

"How about a feature that lets a subscriber block all calls from payphones?"

"Ideal address translation doesn't allow that, but you can block all calls from payphones that haven't been identified as having a more abstract source address."

"That's much better! I wouldn't want to block a call from a friend just because he is calling from a payphone."