Supporting Imprecise Delegation in KeyNote using Similarity Measures

Simon N. Foley
Department of Computer Science,
University College, Cork, Ireland.

(*NordSec 2001, November 1:2, 2001*)

Motivation

Compare Phones by Feature

Features of Eircell Approved Handsets										
Phones	WAP	Data Comp-atible	Triband	Vibra Alert	Voice Activated Dialing	Light-weight	Budget Price	New	Long battery life	MP3 Player
Nokia 3310	–	–	–	✓	✓	–	✓	–	–	–
Nokia 3330	✓	–	–	✓	✓	–	✓	–	–	–
Nokia 6210	✓	✓	–	✓	✓	–	–	–	–	–
Nokia 6250	✓	✓	–	✓	✓	–	–	–	–	–
Nokia 8210	–	✓	–	✓	✓	✓	–	–	–	–
Nokia 8850	–	✓	–	✓	✓	✓	–	–	–	–
Nokia 8890 World	–	✓	–	✓	✓	✓	–	–	–	–
Motorola T250	✓	✓	✓	✓	✓	–	–	✓	–	–
Motorola V50	✓	✓	–	✓	✓	✓	–	✓	–	–
Siemens C35	✓	✓	–	✓	–	✓	✓	–	–	–
Siemens S35	✓	✓	–	✓	✓	✓	✓	–	✓	–
Siemens SL45	✓	✓	–	✓	✓	✓	–	✓	–	✓
Philips Azalis	✓	–	–	✓	✓	–	✓	✓	✓	–
Sony J6	✓	✓	–	✓	–	✓	✓	✓	✓	–

Our Tariffs

New Pay Monthly Options
The best value ever from Eircell. These New Pay Monthly Options are available from 1st October 2001. If you are an existing Eircell Eirtime customer you can move onto New Pay Monthly Options on your next bill date from 1st October 2001.

New Pay Monthly Globe
Eircell's New Pay Monthly Globe options include calls to Near/Mid Europe, USA, Canada, Australia and New Zealand in your monthly minutes. You can also avail of a reduced flat rate roaming tariff within Europe with Vodafone Eurocall.

Eirtime Options*
With Eirtime Options you pay a monthly charge which includes free inclusive minutes. Select the one that suits your lifestyle needs and get talking.

Call a Friend for FREE
Whatever the number of inclusive minutes in your Option we'll match it with an equivalent number of free minutes to call your friend.

Other Charges
International rates, Playback, text messaging and other service charges clearly laid out.

Controlling Costs
Helps you choose the Pay Monthly Option plan that is right for you so there is nothing extra to pay at the end of each month.

Ready to Go
Eircell's prepaid mobile service that puts you in total control. Check out the cost and ways to pay for this service that adapts to your needs.

* Connection and migration to these payment plans is no longer available. View our New Pay Monthly Options.

New Pay Monthly Options

Eircell Personal Prices quoted are VAT inclusive			**Total Inclusive Minutes**		
Option	**Your Lifestyle**	**Monthly Rental**	Peak	Off Peak	Call a Friend for FREE
Light	Ideal if you like to make occasional calls in the evenings or weekend and few daytime calls.	**£15** € 19.05	10	50	50
Active	Ideal if you like to chat outside office hours and make an occasional call during the day.	**£30** € 38.09	30	300	300
Extra	Suited to a busier lifestyle, Extra will enable you to stay in contact around the clock.	**£24** € 30.47	75		75

Eircell Business Prices quoted are VAT exclusive			**Total Inclusive Minutes**		
Option	**Your Lifestyle**	**Monthly Rental**	Peak	Off Peak	Call a Friend for FREE
Extra	Suited to the light business user, Extra will provide you with the flexibility to keep things running smoothly.	**£20** € 25.39	75		75
Performer	Suited to the heavy business user, Performer will provide maximum savings as the more you talk, the less you pay.	**£40** € 50.79	200		200

All Euro amounts are the equivalents of Eircell's IEP Tariffs, converted using the rate € 1 = £0.787564

Manage my Mobile – Logon if you'd like to change your tariff now!

Outline of Talk

Trust Management and Compliance Checking

Imprecise Compliance Checking

Cascading Imprecision

Imprecision in Practice: Feature Sets

Conclusion

Trust Management and Compliance Checking

Example

Assume authorization credentials provide details of a telephone's 'contract'.

	0:Light	1:Active	2:Extra
cp:Personal	×	×	
cb:Business		×	×

Varying service level available to personal/business customers.

```
Authorizer: "POLICY"
Licensees:  "Ksteve"
Conditions:
  ( (Cust=="cp" && 0<=@Qual<=1)
  ||(Cust=="cb" && 1<=@Qual<=2));
```

Trust `Ksteve` to delegate service authorizations.

Credentials specify delegation of authorization between public keys.

```
Authorizer: "Ksteve"
Licensees:  "Kalice"
Conditions: Cust=="cp"
         && @Qual<=1;
```

```
Authorizer: "Kalice"
Licensees:  "Kangela"
Conditions: Cust=="cp"
         && @Qual==0;
```

Is Angela's request for a light personal connection authorized?

Compliance Checking: given authorization policy and collection of credentials, service must determine whether a particular request is authorized.

Imprecise Compliance Checking

Conventional compliance checking based on an absolute similarity measure: reject Alice's request for active business connection `[Cust="cb",Qual=1]` since Alice holds only `[Cust="cp",Qual=1]`

Support degrees of imprecision by using a relative similarity measure:

$$[\texttt{Cust="cp"}, \texttt{Qual=1}] \approx [\texttt{Cust="cb"}, \texttt{Qual=1}] = 0.9$$

$$[\texttt{Cust="cp"}, \texttt{Qual=1}] \approx [\texttt{Cust="cp"}, \texttt{Qual=0}] = 0.8$$

Imprecise Compliance Checking: given request for action X, the service must determine whether credentials authorize action X, where $X \approx X' \geq n$, for degree of similarity $0 \leq n \leq 1$ that is acceptable to the service.

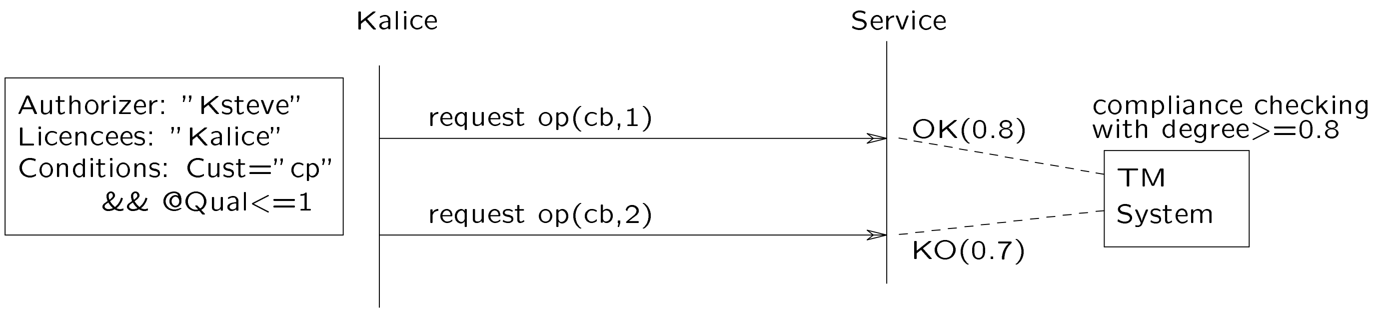
Example

Specifying the similarities between personal and business connections:

$$[\texttt{Cust} = c, \texttt{Qual} = q] \approx [\texttt{Cust} = d, \texttt{Qual} = r]$$

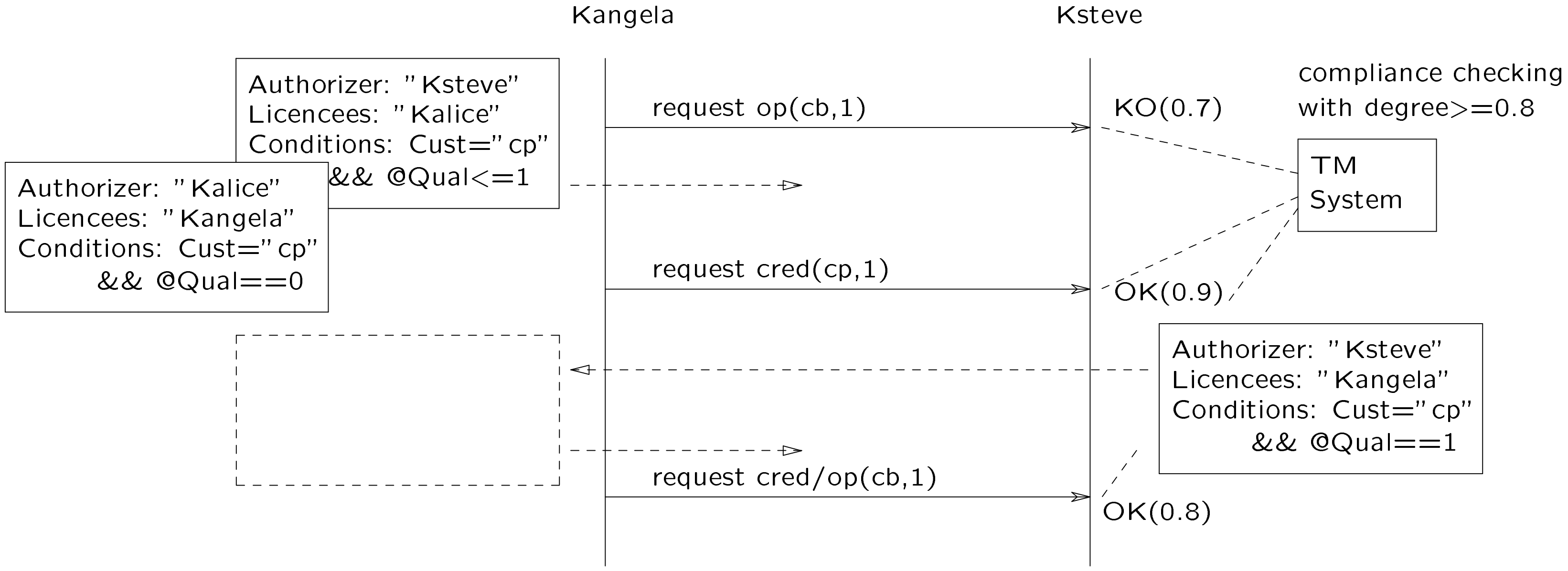
$$\equiv \begin{cases} 1.0 - 0.1 \times |q - r| & \text{if } (c = d) \\ 0.8 - 0.1 \times |q - r| & \text{otherwise} \end{cases}$$

$\approx$	(cp,0)	(cp,1)	(cb,1)	(cb,2)
(cp,0)	1.0	0.9	0.7	0.6
(cp,1)	0.9	1.0	0.8	0.7
(cb,1)	0.7	0.8	1.0	0.9
(cb,1)	0.6	0.7	0.9	1.0



Cascading Imprecision

Compliance check (reduction) may be used to determine whether it is safe to delegate by signing a new credential.



Defacto delegation does not confer additional authorization on requester.

By providing appropriate credentials, a requester can *dejure* acquire additional authorization; authorization that is not defacto.

Managing Cascading Imprecision

Credentials should incorporate conditions relating the degree of similarity for which the credential was signed.

Informal Strategy

Given degree of similarity n : [0..1], include additional attribute within policy:

$$\texttt{\&Degree} >= n$$

For each credential intended to authorize $\texttt{Action}\ X$, codify

$$\texttt{\&Degree} \leq \texttt{Action} \approx X$$

Imprecise Compliance Checking: given request for action X, the service must find a suitable value V such that $[\texttt{Action} = X, \texttt{\&Degree} = V]$ is authorized.

Credential Writing: if a new credential is to be written for this authorization then it should reflect this imprecision:

$$\texttt{\&Degree} \leq (\texttt{Action} \approx X) - (1 - V)$$

Managing Cascades: Example

```
Authorizer: "POLICY"
Licensees:  "Ksteve"
Conditions: &Degree>=0.8 &&
  ( (Cust=="cp" && 0<=@Qual<=1)
  ||(Cust=="cb" && 1<=@Qual<=2));
```

Policy specifies that similarity to a degree of 0.8 or higher is OK.

```
Authorizer: "Ksteve"
Licensees:  "Kalice"
Conditions:
  &Degree<=(Cust,@Qual) ("cp",1);
```

Alice authorized to request action sufficiently similar to ("cp",1), (under constraints of above policy).

```
Authorizer: "Kalice"
Licensees:  "Kangela"
Conditions: Cust=="cp" &&
   &Degree <= 1.0-(0.1*(@Qual));
```

Angela authorized to request action sufficiently similar to ("cp",0). Credential explicitly codifies similarity measure.

```
Authorizer: "Ksteve"
Licensees:  "Kangela"
Conditions: Cust=="private" &&
   &Degree <= 0.9
```

Angela authorized to request action ("cp",1), (approximate degree 0.8). New credential must reflect this.

Imprecision in Practice: Feature Sets

Authorization may be regarded as offering a set of possible features.

A feature set (authorization) is a binary vector of feature settings.

Example. Mobile phone authorization may compose combination of features: send and/or receive, calls/text messages/data/email/etc.

Define similarity between feature sets by averaging difference between the feature A_i and B_i ($0 \leq i < n$) for feature sets A and B.

$$A \approx B \equiv 1 - \sum_{i=0}^{n-1} \frac{(A_i \oplus B_i)}{n})$$

Nearest Neighbor formula includes weights for each feature:

$$A \approx B \equiv 1 - \frac{\sum_{i=0}^{n-1} w_i \times (A_i \oplus B_i)}{\sum_{i=0}^{n-1} w_i}$$

This is one approach to engineering similarity measures.

Conclusions

A delegation request may fail because it was not expressed in precisely the right way. Rather than rejecting such requests it may be preferable to offer a credential with a 'similar' authorization.

Similarity techniques provide degrees of imprecision for delegation.

Details about potential imprecision encoded within credentials.

Imprecise Compliance Checking/Reduction: strategy for casting imprecise trust in terms of a conventional compliance check/reduction.

Strategy provides direction for practical implementation.

Future research will draw on experience of Knowledge Engineers to develop similarity frameworks for authorization.