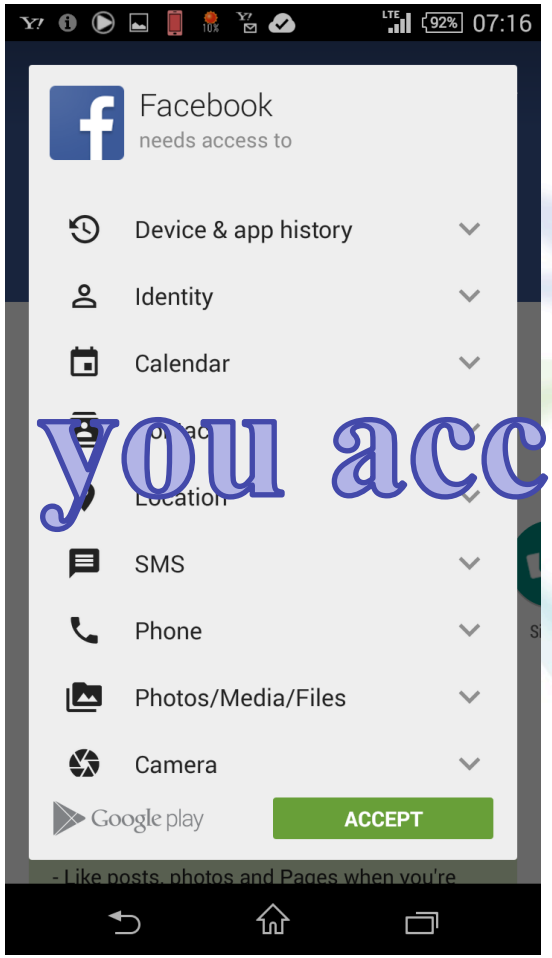
GRACE

CENTER FOR GLOBAL RESEARCH IN ADVANCED SOFTWARE SCIENCE AND ENGINEERING

An Adaptive Privacy Framework for Individual Privacy

Nobukazu Yoshioka,
National Institute of Informatics
9 September 2015 @ EASSy

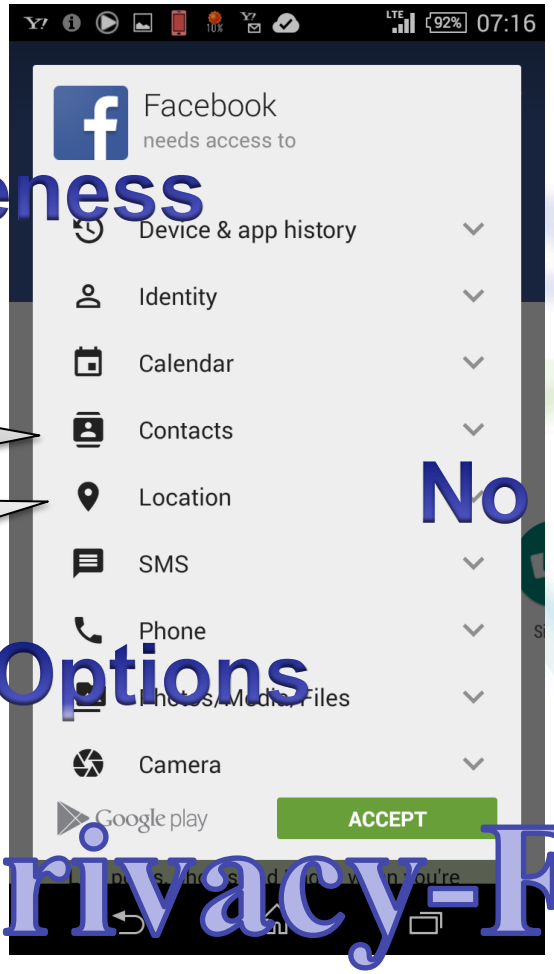
https://flic.kr/p/iSA17W



Will you accept?

All or Nothing

No Risk Awareness



Terrible!

OK

No Preference

No Service Options

More Privacy-Fridenly

All or Nothing

An Motivating Example

Training Gym

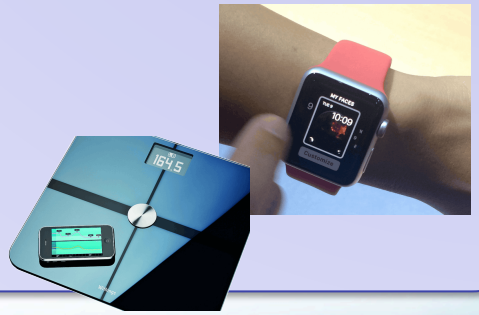
Available Services
(Guidance) Provide Exercise Guidance
(Motivation) Keep up Motivation of Exercise

Alice

Bike lesson

Yoga lesson

Bob: Coach



Health Monitor Devices

Privacy-Friendly Service

Privacy Preference
BMI is not private

Alice

Privacy Preference
BMI is private

Member A

Adjust to individual privacy preferences

Privacy-Friendly Service

Privacy Preference
Age is private

Need to know BMI and age for guidance

Bob: Coach

Service Level for Member B:
Share her age as
Pseudonym information

Member B

Customized Service Level for each Preference

Dave: Boss

Alice

Privacy Preference

~~BMI is not Private~~

Never share BMI with members

Stop sharing

Member A

Privacy-Friendly Service

Adapt to Privacy Context Changes

New Service Level:
Share her age as **Anonymous** information

Bob: Coach

Many Members

Increase Privacy Risks

An Adaptive Framework

Dave: Boss

Alice

Privacy Preference

~~BMI is not Private~~

Never share BMI with members

Subjective

Stop sharing

Member A

Privacy-Friendly Service

Adapt to Privacy Context Changes

New Service Level:
Share her age as **Anonymous** information

Individual

Bob: Coach

Many Members

Changeable

Increase Privacy Risks

Difficulties

An Adaptive Framework for Individual Privacy

Available Services	Alice Choice
(Guidance) Provide Exercise Guidance	✔
(Motivation) Keep up Motivation of Exercise	✔

Privacy Preference (Impact)

Private Info.	Coach	Friend	Other
BMI	Moderate	Moderate	No
Age	High	Moderate	Moderate

Impact on sharing age with Coach

Risk based Service Levels + **Likelihood** of Privacy Breaches

Privacy Requirements for Alice

To satisfy

An Adaptive Framework

Example: Specification of Service Options

Available Services	Options and the details	Requirements of Private Information
(Guidance) Provide Exercise Guidance	**Coach** recommends an exercise program and the goals of BMI	K_{Coach}(nickname, Age, BMI)
(Motivation) Keep up Motivation of Exercise	Option (SF) Share status of reducing BMI with **Friends**	K_{Friend}(nickname, BMI)
	Option (SO) Share status of reducing BMI with Other members	K_{Other} (nickname, BMI)

Other members will know BMI of nickname by this service

How to assess Privacy Risk for a user?

Available Services	Options and the details	Requirements of Private Information
(Guidance) Provide Exercise Guidance	**Coach** recommends an exercise program and the goals of BMI	K_{Coach}(nickname, Age, BMI)
(Motivation) Keep up Motivation of Exercise	Option (SF) Share status of reducing BMI with **Friends**	K_{Friend}(nickname, BMI)
	Option (SO) Share status of reducing BMI with **Other** members	K_{Other} (nickname, BMI)

Alice needs to assess her privacy risk of private information leakage for each service

What's Privacy Risk via service?

Risk of Leakage of Private Information

Subjective damage when private information is known by someone

Possibility for someone to know private information via service

Privacy Risk = Impact × Likelihood

Privacy Preference

Depends on a service, e.g. communication frequency

Specification

(SF)

:Friend

Depends on a context, e.g. number of Friends

Privacy Preference

Subjective Privacy Impact Level of Alice

Private Info. \ Role	Coach	Friend	Other
BMI	Moderate	Moderate	No
Age	High	Moderate	Moderate

A impact level when a role knows private information via service

Impact Level ≒ Negative Feeling =
{Terrible, High (Very Bad), Moderate (I don't Know), No (No Problem)}

Likelihood with Privacy Context

Ex) Likelihood Specification of Option (SF)

Frequency of Communication

BMI

Depends on the number of Friends

Privacy Likelihood Specification of BMI

Likelihood Level	Privacy Context
Very Low	Number(Friend) < 10
Low	10 <= Number(Friend) < 20
Moderate	20 <= Number(Friend) < 30
High	30 <= Number(Friend) < 40
Very High	Number(Friend) >= 40

Privacy Risk = Expected Negative Damage

Privacy Risk of BMI via (SF) for Alice

Alice Impact

Info.	Friends
BMI	Moderate
Age	Moderate

Likelihood / Impact	Very Low (0.1)	Low (0.25)	Moderate (0.5)	High (0.75)	Very High (1)
No	No Risk	No Risk	No Risk	No Risk	No Risk
Moderate (3)	VL(0.3)	VL(0.75)	L(1.5)	M(2.25)	H(3)
High (5)	VL(0.5)	L(1.25)	M(2.5)	H(3.75)	VL(5)

possibility

damage

Likelihood of SF	Privacy Context
Very Low	Number(Friend) < 10
Low	10 <= Number(Friend) < 20
Moderate	20 <= Number(Friend) < 30
High	30 <= Number(Friend) < 40
Very High	Number(Friend) >= 40

Privacy Risk	Privacy Context
Very Low (VL)	Number(Friend) < 20
Low (L)	20 <= Number(Friend) < 40
Moderate (M)	40 <= Number(Friend)
High (H)	N/A
Very High (VH)	N/A

Current Risk

Current Number(Friend) = 20

Current Risk of BMI via (SF) is Low

Risk on Exercise Guidance by Coach

Likelihood / Impact	No (0)	Very Low (0.1)	Low (0.25)	Moderate (0.5)	High (0.75)	Very High (1)
No (0)	No Risk	No Risk	No Risk	No Risk	No Risk	No Risk
Moderate (3)	No Risk	VL(0.3)	VL(0.75)	L(1.5)	M(2.25)	H(3)
High (5)	No Risk	VL(0.5)	L(1.25)	M(2.5)	H(3.75)	VL(5)

Alice Impact

Private Information	Coach
BMI	Moderate
Age	High

	Likelihood
BMI	High
Age	High

Private Information	Risk
BMI	Moderate
Age	High

Risk of Age shared with Coach is high

Not So Privacy-Friendly!

(Guidance)
Provide Exercise Guidance

(G: Level 3)
K_{Coach}(nickname, Age, BMI)

Coach recommends an exercise program and the goals of BMI

Risk is high

Accept? or Nothing?

Service Levels for Risk Mitigation

(Guidance)
Provide Exercise Guidance

(G: Level 3)
K_{Coach}(nickname, Age, BMI)

Coach recommends an exercise program and the goals of BMI

Risk is high

High Value

> Age

(G: Level 2)
K_{Coach}(nickname, abst(Age), BMI)

Coach recommends an exercise

> {Age, BMI}

Service level for Risk mitigation of age and BMI

Less functionality with abstracted information

> Age,BMI

Automatic guidance without coach

(G: Level 1)
$K_{coach}\{\}$

Show a general recommendation with respect to BMI

Low Risk

Abstraction of Privacy Related Information

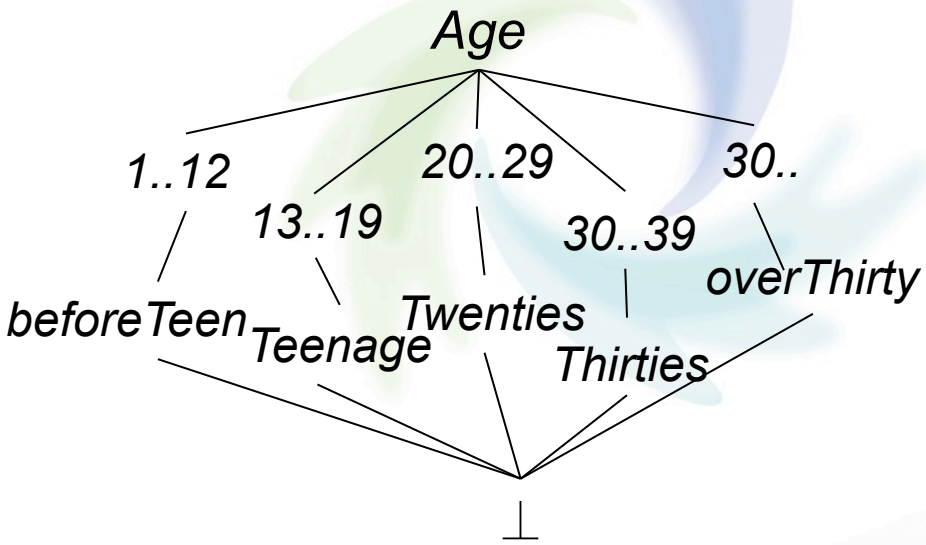
K_r(u: Identifiable Information, p: Private Information)

u … e.g. full name

pseudonym(u)
… e.g. nickname

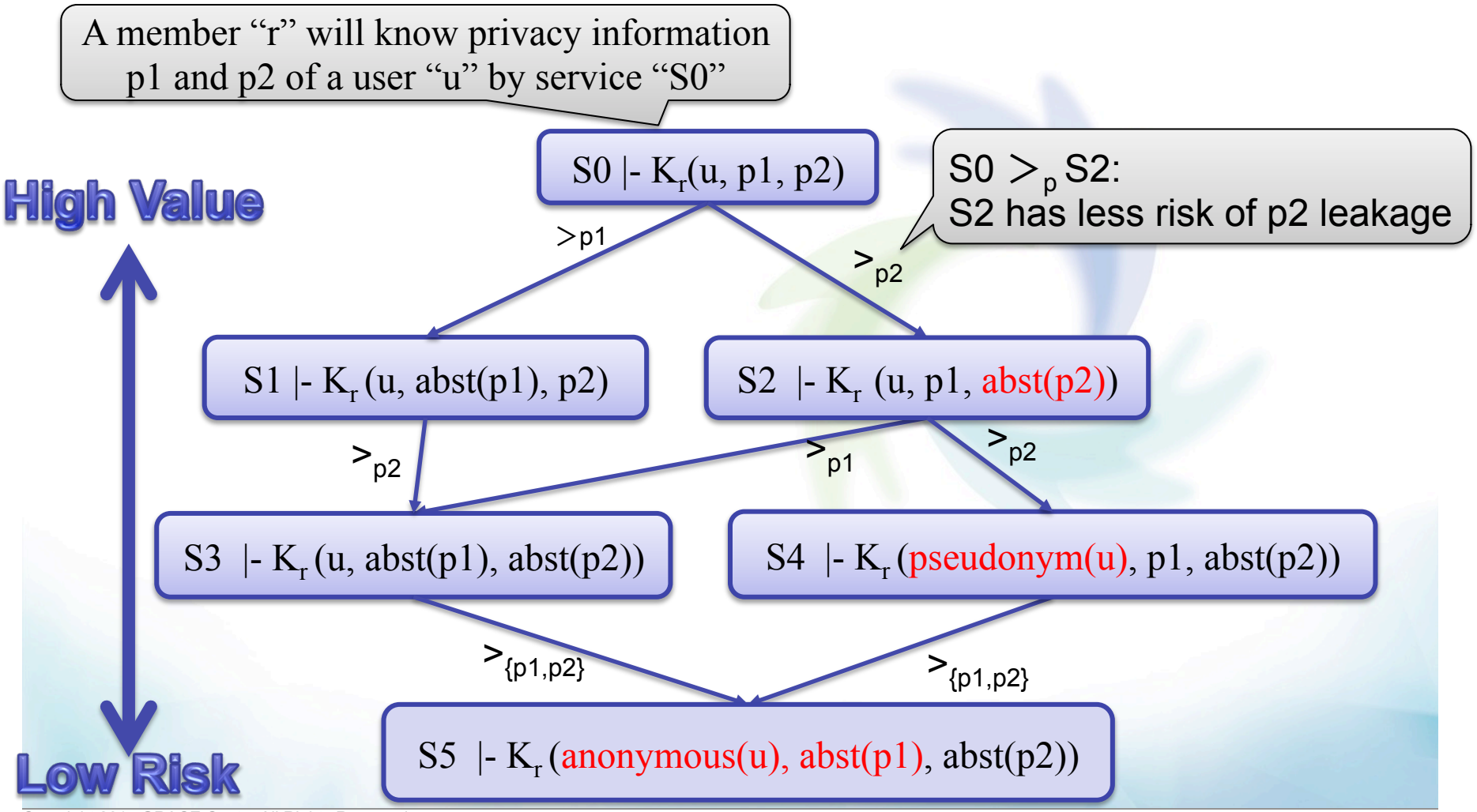
anonymous(u)
… e.g., hiding of u

An example of abstraction



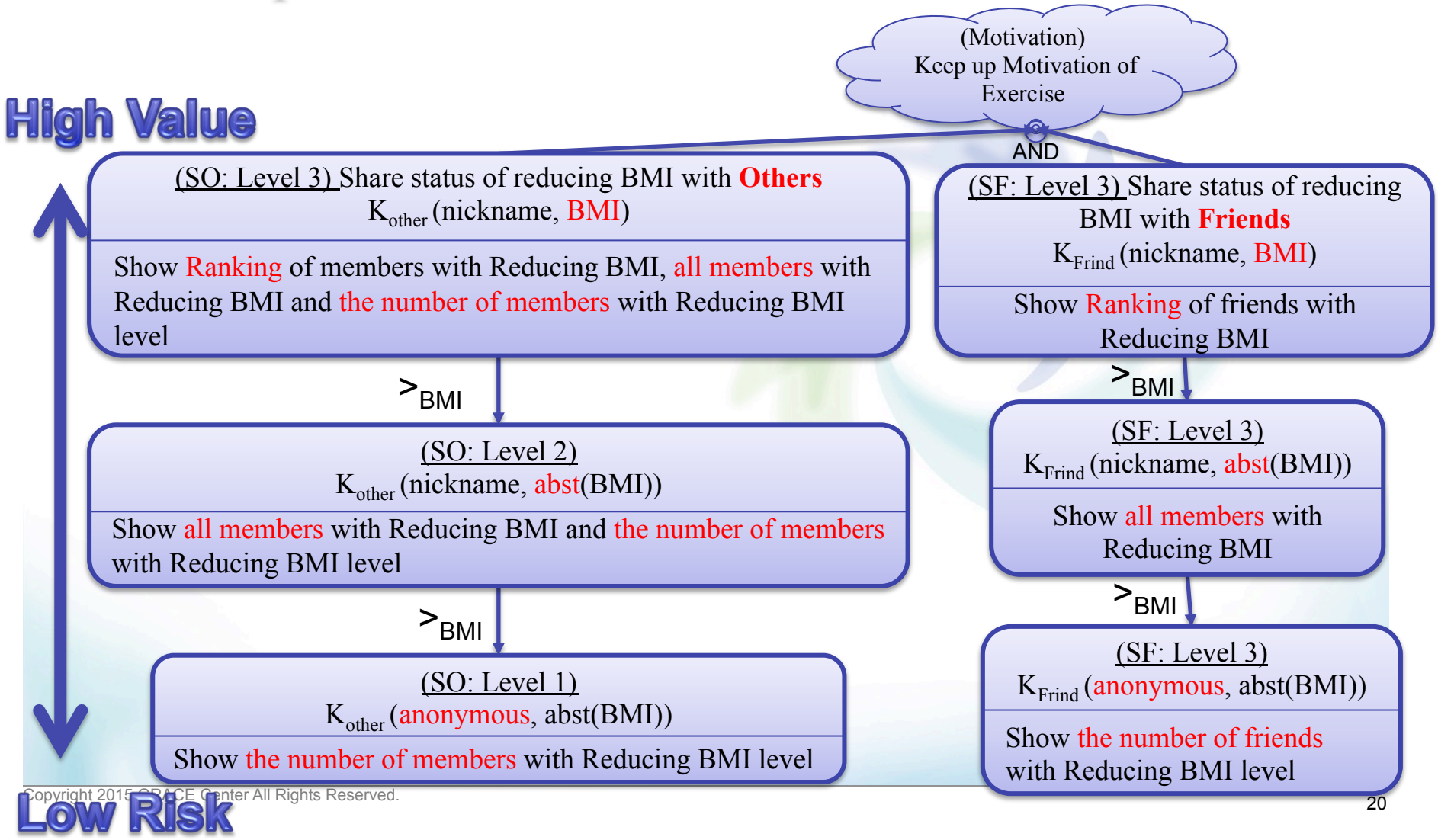
Abst(20:Age) = `Twenties'

Various Service Levels for risk mitigation



Available Services and the Levels:

Service Specifications on Motivation



Risk Assessment of Alice

Available Services	Requirements of Private Information	Current Risk	Recommended Service Level	Alternative Level
(Guidance) Provide Exercise Guidance	K_{Coach}(nickname, Age, BMI)	BMI: Moderate Age: High	(G: Level 2) K_{Coach}(nickname, abst(Age), BMI)	(G: Level 1) $K_{coach}\{\}$
(Motivation) Keep up Motivation of Exercise	Option (SF) K_{Friend}(nickname, BMI)	BMI: Low Age: No Risk (Number(Friends) = 20)	(SF: Level 2) K_{Friend}(nickname, abst(BMI) when Moderate Risk (40 <= Number(Friend))	N/A
	Option (SO) K_{Other} (nickname, BMI)	BMI: No risk Age: No risk	(SO: Level 2) K_{Others}(nickname, abst(BMI)) when Moderate Risk (Number(Member) <= 3)	N/A

Risk on SF	Privacy Context
Very Low	Number(Friend) < 20
Low	20 <= Number(Friend) < 40
Moderate	40 <= Number(Friend)

Decision of Service Level

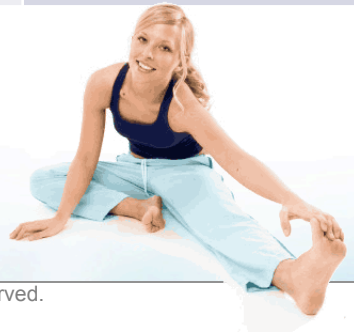
disadvantage:
No specific goal is recommended

Available Services	Requirements of Private Information	Current Risk	Recommended Service	Alternative Level
(Guidance) Provide Exercise Guidance	K_{Coach}(nickname, Age, BMI)	BMI: Moderate Age: High	(G: Level 2) K_{Coach}(nickname, abst(Age), BMI)	(G: Level 1) $K_{coach}\{\}$
(Motivation) Keep up Motivation of Exercise	Option (SF) K_{Friend}(nickname, BMI)	BMI: Low Age: No Risk (Number(Friends) = 20)	(SF: Level 2) K_{Friend}(nickname, abst(BMI) when Moderate Risk (40 <= Number(Friend))	N/A
	Option (SO) K_{Other} (nickname, BMI)	BMI: No risk Age: No risk	(SO: Level 2) K_{Others}(nickname, abst(BMI)) when Moderate Risk (Number(Member) <= 3)	N/A

Choose risk mitigation

Privacy Requirements for Alice

Services	Privacy Requirements	Risk Aware Privacy Requirements
(Guidance) Provide Exercise Guidance	(G: Level 2) K_{Coach}(nickname, abst(Age), BMI)	
(Motivation) Keep up Motivation of Exercise	Option (SF: Level 3) K_{Friend}(nickname, BMI)	(SF: Level 2) K_{Friend}(nickname, abst(BMI)) when Moderate Risk (40 <= Number(Friend))
	Option (SO: Level 3) K_{Other} (nickname, BMI)	(SO: Level 2) K_{Others}(nickname, abst(BMI)) when Moderate Risk (Number(Member) <= 3)



An Adaptive Framework for Individual Privacy

Available Services	Alice Choice
(Guidance) Provide Exercise Guidance	✔
(Motivation) Keep up Motivation of Exercise	✔

Privacy Preference (Impact)

Private Info.	Coach	Friend	Other
BMI	Moderate	Moderate	No
Age	High	Moderate	Moderate

Impact on sharing age with Coach

Risk based Service Levels + **Likelihood** of Privacy Breaches

Privacy Requirements for Alice

To satisfy

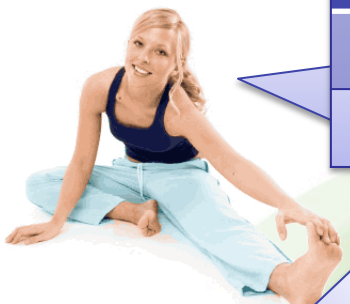
An Adaptive Framework

An Adaptive Framework for Individual Privacy

Available Services	Alice Choice
(Guidance) Provide Exercise Guidance	✔
(Motivation) Keep up Motivation of Exercise	✔

Privacy Preference (Impact)

Private Info.	Coach	Friend	Other
BMI	Moderate	Moderate	No
Age	High	Moderate	Moderate



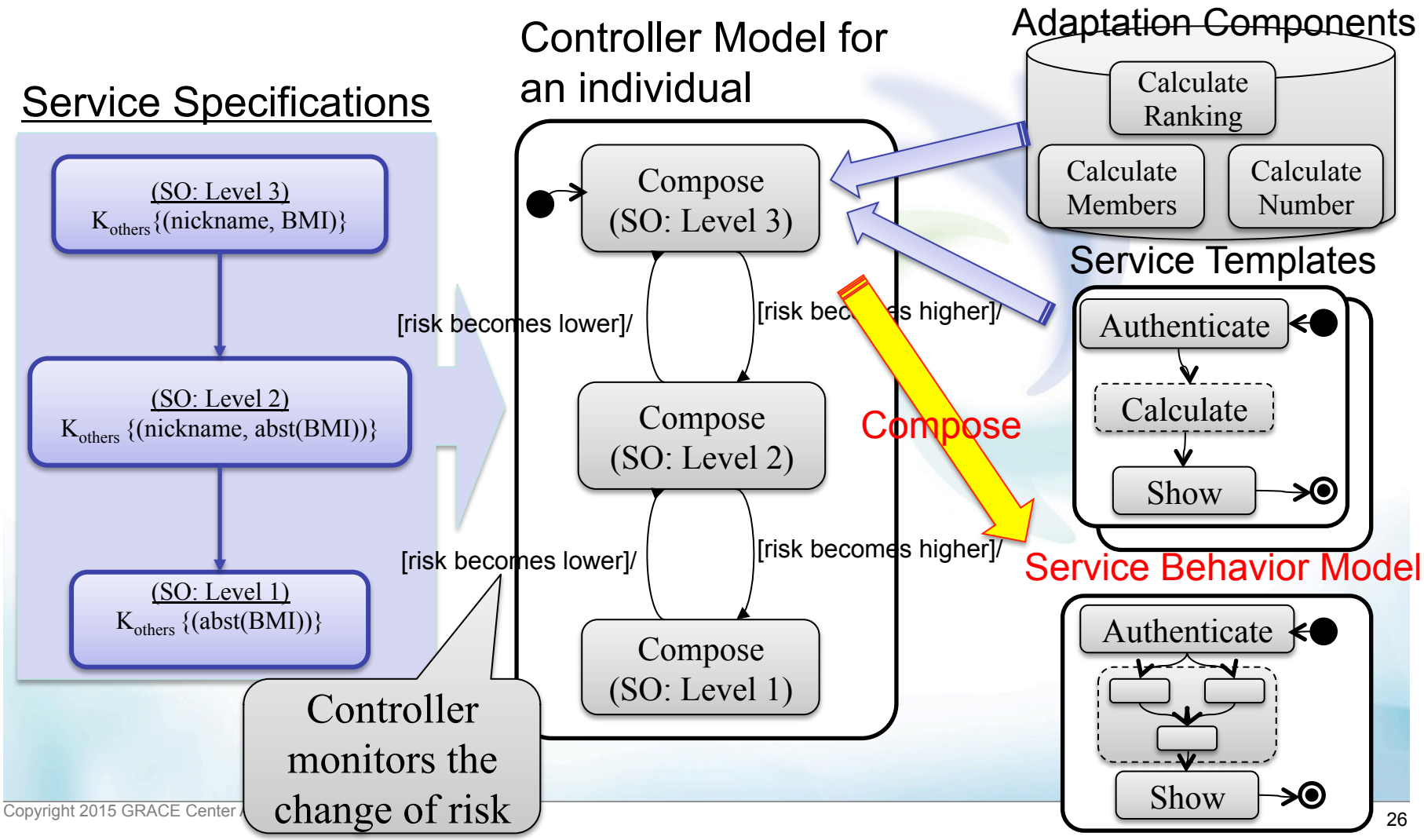
Risk based Service Levels
+ **Likelihood** of Privacy Breaches

Privacy Requirements for Alice

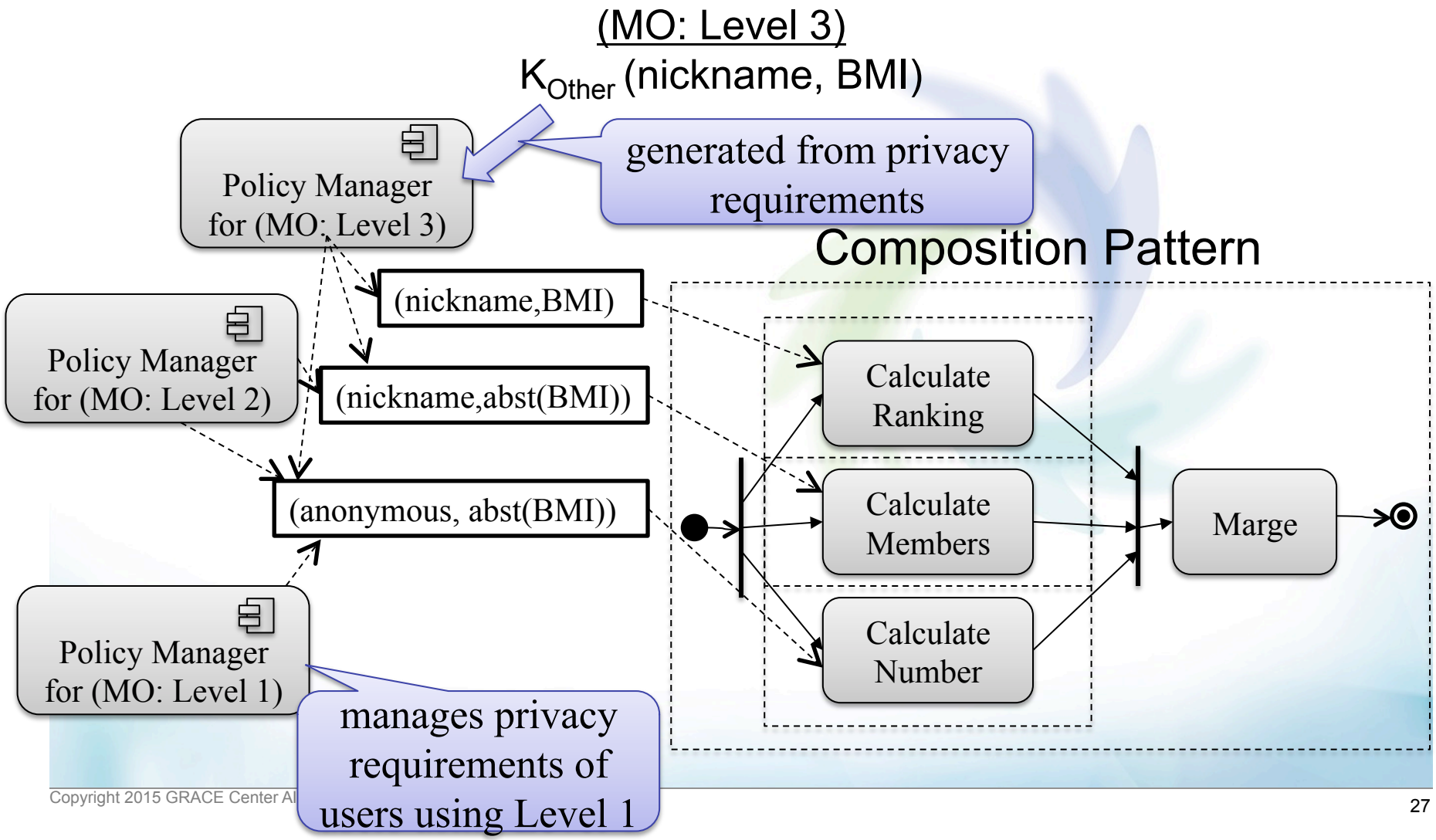
To satisfy

An Adaptive Framework

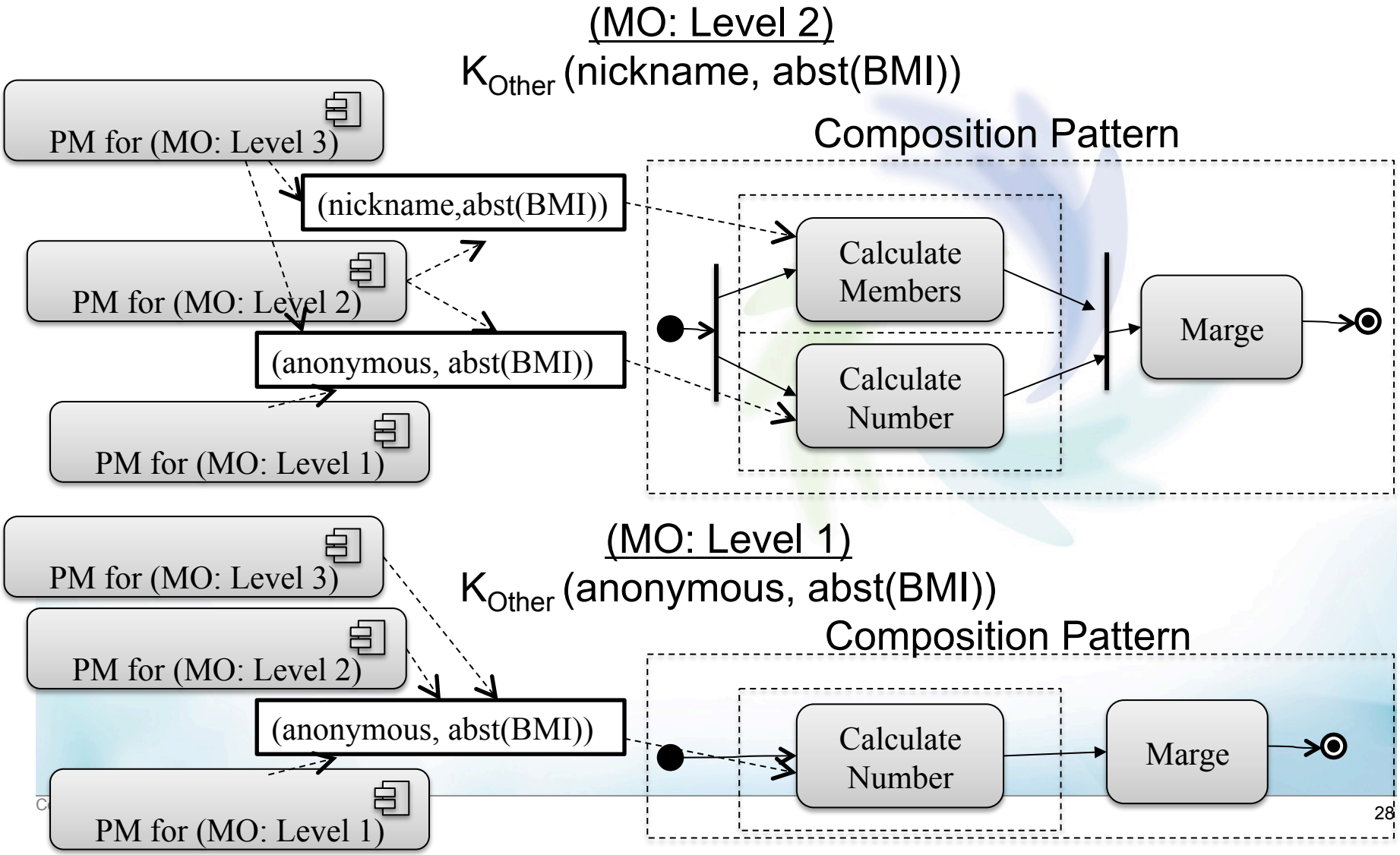
Controller of Service Behavior Model



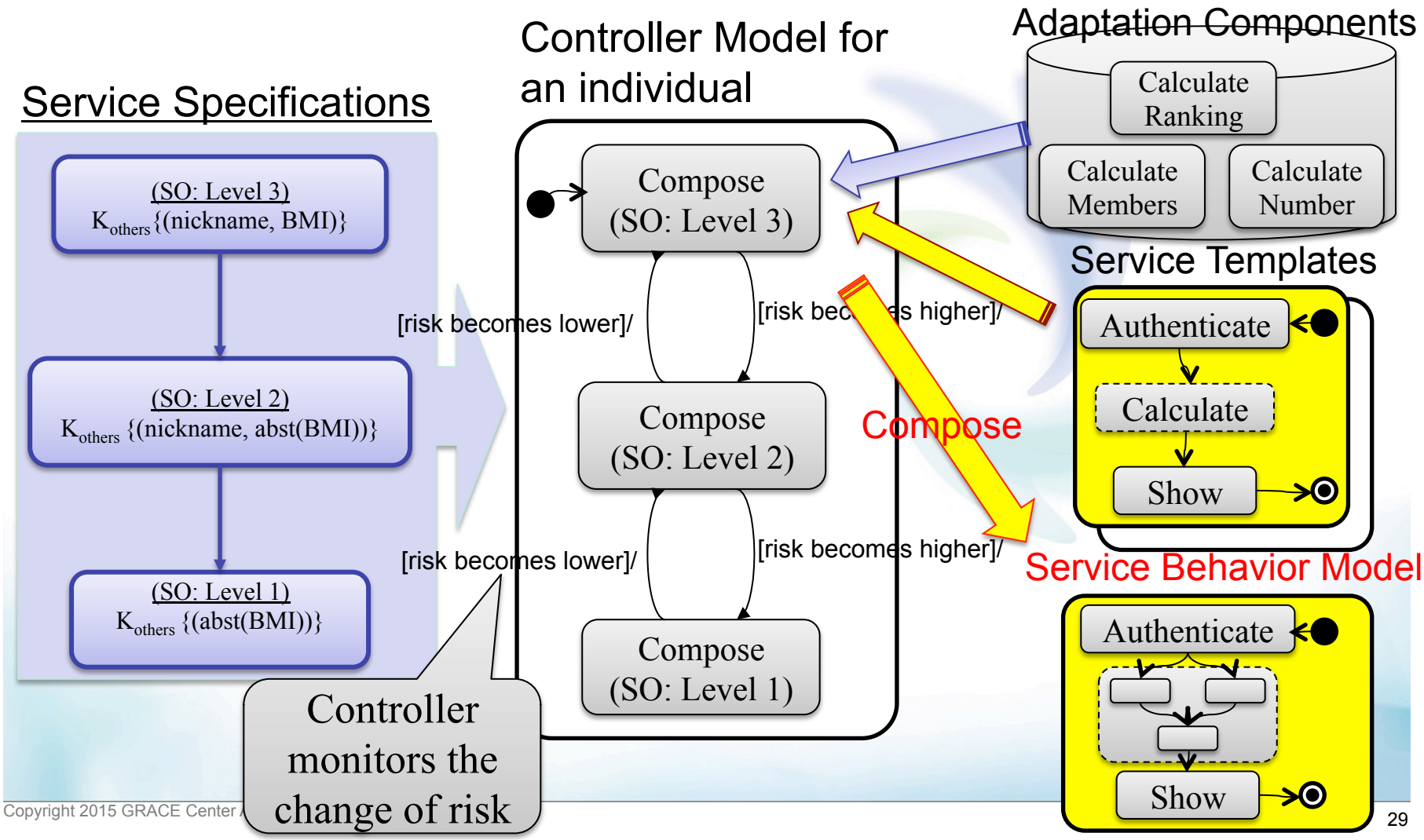
Service Specification for (MO: Level 3)



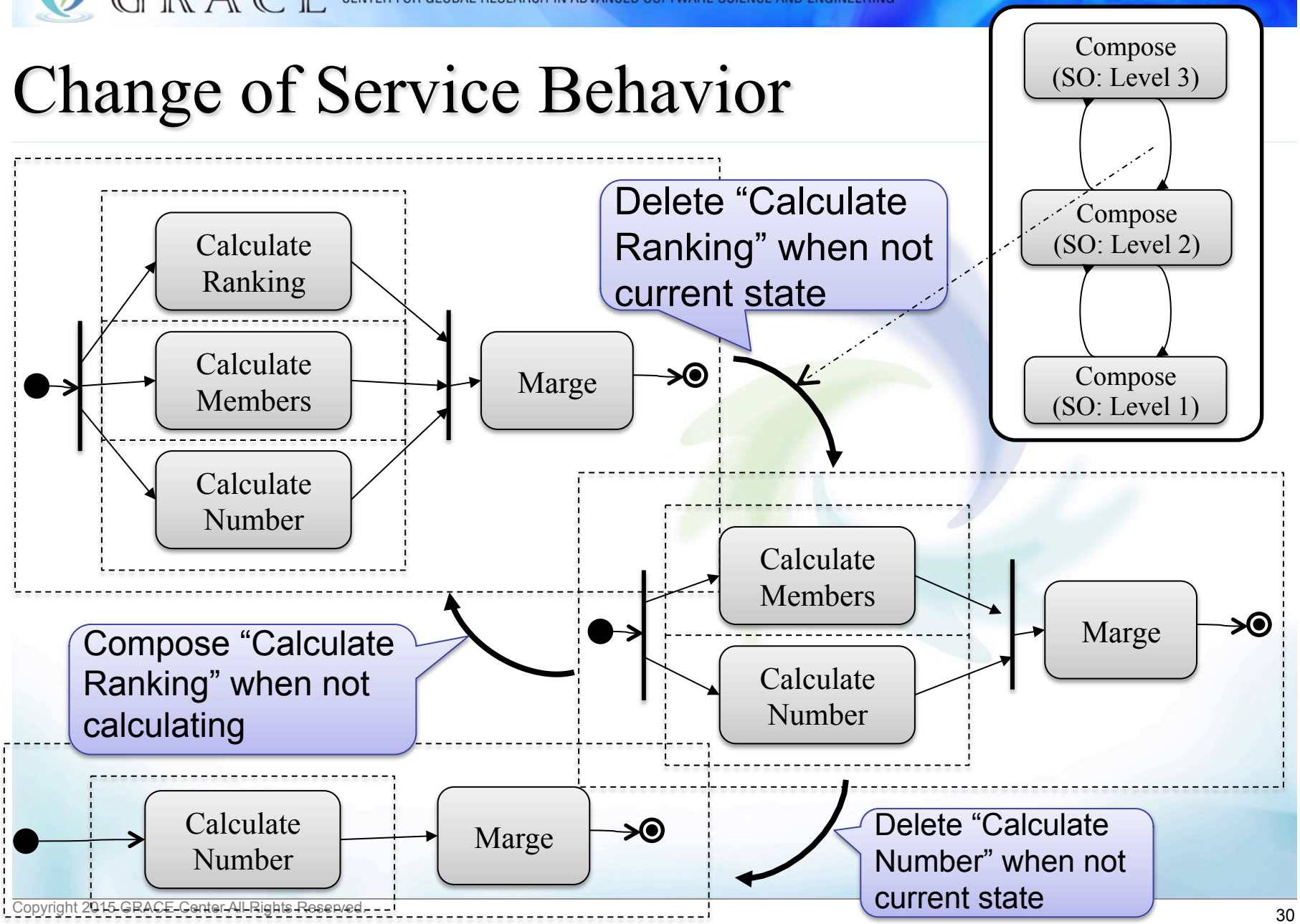
Service Specification for Level 2 and 1



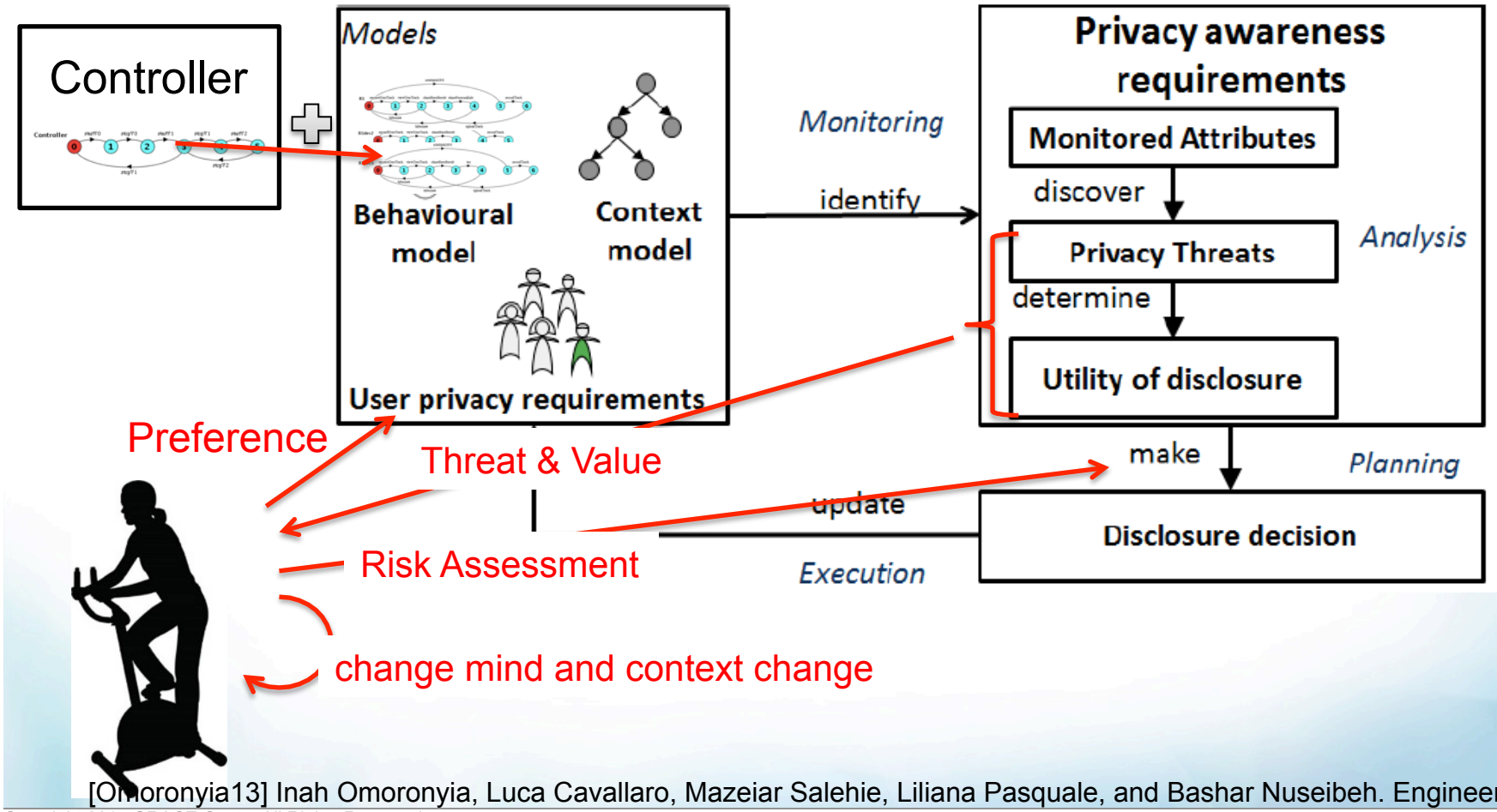
Controller of Service Behavior Model



Change of Service Behavior



Adaptive Privacy Framework [Omoronyia13]



[Omoronyia13] Inah Omoronyia, Luca Cavallaro, Mazeiar Salehie, Liliana Pasquale, and Bashar Nuseibeh. Engineering adaptive privacy: on the role of privacy awareness requirements. ICSE '13, pp. 632-641.

Conclusion

- **We are going to propose**
  1. **A notation of privacy requirements and user preferences for privacy,**
  2. **Guidelines to specify privacy options, and**
  3. **An adaptation framework to generate behavior with privacy options automatically.**

⇨ We can provide privacy options efficiently