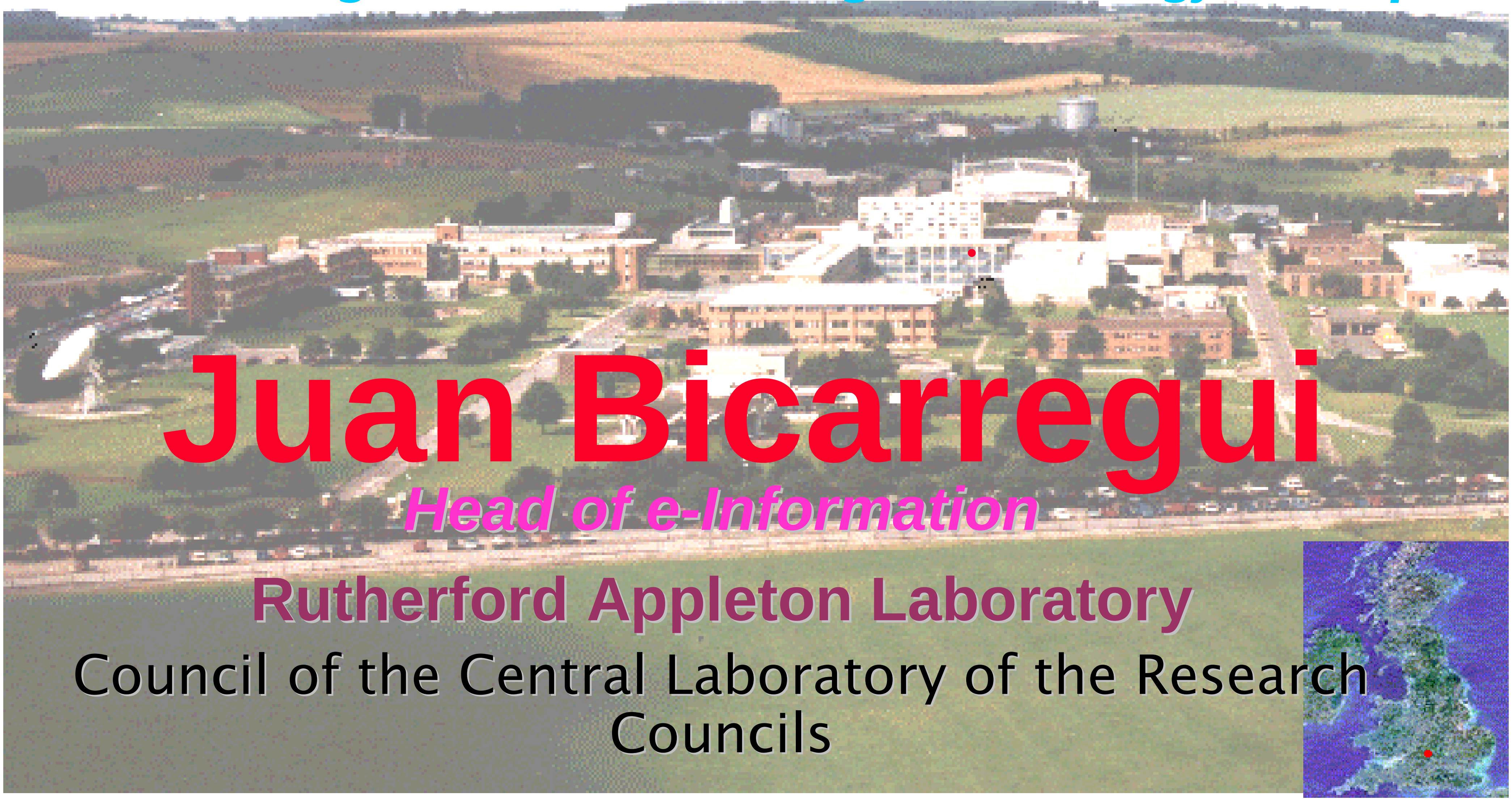
Information Systems Research and Development at CCLRC

Accelerating Innovation Through Technology Transfer



Juan Bicarregui

Head of e-Information

Rutherford Appleton Laboratory

Council of the Central Laboratory of the Research Councils

Who we are: CCLRC

Facilities include:

- Neutron and Muon Source
- Synchrotron Radiation Source
- Lasers
- Microstructures
- Space Science
- Satellite Technology
- Solar Terrestrial Physics
- Molecular Spectroscopy
- High Performance Computing
- Wind Energy Research
- Information Technology
- Nuclear Physics
- Particle Physics
- Radio Communications
- Surfaces Transforms and Interfaces

Also Spin-in/out Companies:

- Exitech (1984)
  - laser processing (50 Staff)
- Bookham Technology(1989)
  - optoelectronic (400, £3bn)
- UKERNA (1994)
  - Networking (60)
- Ceravision
  - displays (£30M)
- Neos Interactive
  - multimedia internet (£20M, 20)
- Petrra(2000)
  - Medical Diagnostic (2)

Who we are: e-Information

Information Systems and Services

- ***Information Science and Engineering Group***
  - *IS Research and Development*
    - *EU & UK Research, In-house projects R&D, Private Sector R&D*
- ***Information Services Group***
  - *In house and commercial services*
    - *Library, ERMS, Legal (Freedom of Information and data Protection Acts)*
- ***W3 Group***
  - *UK& Ireland W3C office, ERCIM, etc.*

Information Systems and Services
Research Challenges

- *e-Science*

  ...
- *e-Government*

  ...
- *Semantic Web*

  ...
- *Trusted e-Services*

  ...
- **Ambient Computing**

  ...

European Research Consortium for Informatics and Mathematics
ERCIM

W3C WORLD WIDE WEB consortium
United Kingdom Office

Information Systems and Services
Research Themes

- ***Information Modelling and Analysis***
  - ....
- ***Security and Trust management***
  - ....
- ***Weband Grid Technology***
  - ....

Contents

- The advert
- Two areas of research
  - Modeling Trust in e-Services
  - Semantics of information hiding
- Future work

Trust in e-Services

(Theo Dimitrakos)

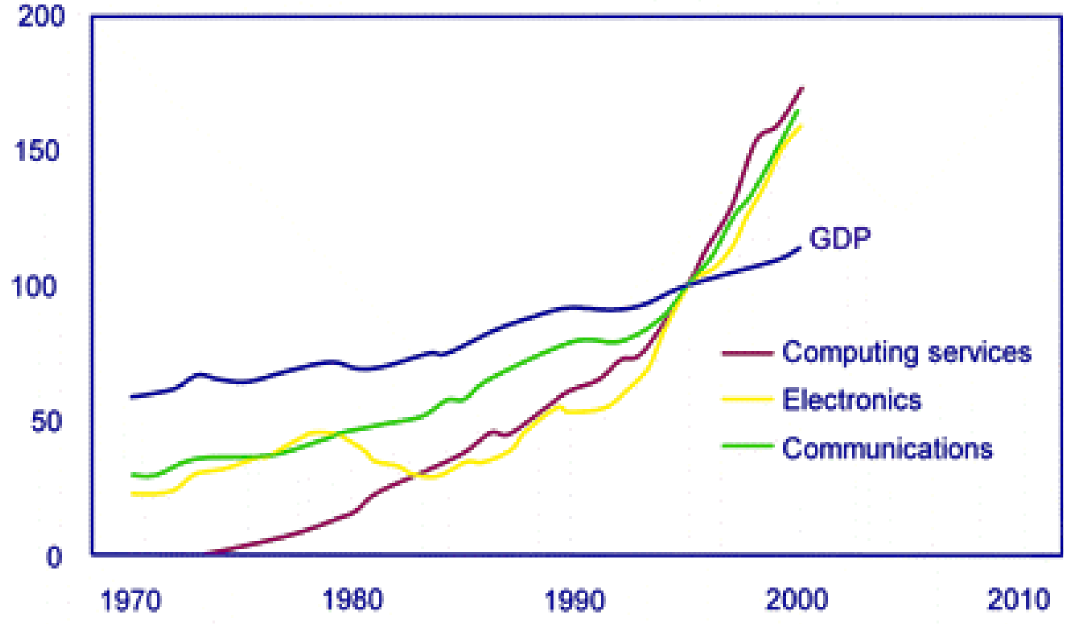
- motivation for modelling trust
- some properties of trust in e-services
- aims for trust management

Building Trust into e-Services Why?

"The UK is the largest e-commerce market in Europe ... Value added in ITEC sectors accounts for nearly a third of GDP growth"

[UK On-line annual report 2000]

Value added in ICT sectors and the whole economy (1995 = 100)



Building Trust into e-Services Why?

BUT ... major concern about the trustworthiness of *e*-Services

"While internet penetration is growing rapidly, all the evidence shows that consumer confidence in the e-commerce medium itself and in cross-border transactions remains low.

E-commerce, therefore, is an insignificant part of final consumption within the European Union – significantly below 1% of total retail sales."

[David Byrne, European Commissioner for Health and Consumer Protection]

Building Trust into e-Services Why?

"Despite the presence of effective base technologies, there remains a need for further innovation before trust can be managed efficiently at the service level."

"For e-services to achieve the same levels of acceptance as their conventional counterpart trust management has to become an intrinsic part of e-service provision."

Patricia Hewitt - UK minister for e-commerce

Trust in e-Services

- ☑ motivation for modelling trust
- ❑ **a model of trust in e-services**
- ❑ aims for trust management

A Model of Trust

Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context

Trust is **relative** to a specific service. Different trust relationships appear in different business contexts

The measurement may be **absolute** (e.g. probability) or **relative** (e.g. dense order)

This period may be in the **past** (history), the **duration of the service** (from now and until end of service), **future** (a scheduled or forecasted critical time slot), or always

Dependability is deliberately understood broadly to include
security, safety, reliability, timeliness, maintainability
(following Newcastle the interpretation **www.dirc.org.uk**)

A model of Trust

Subjective beliefs as *opinions*

(Dempster-Shafer, *Theory of evidence*)

(Jøsang, Subjective Logic)

- **Opinions $w^A(p)$ = (b,d,u,a)**

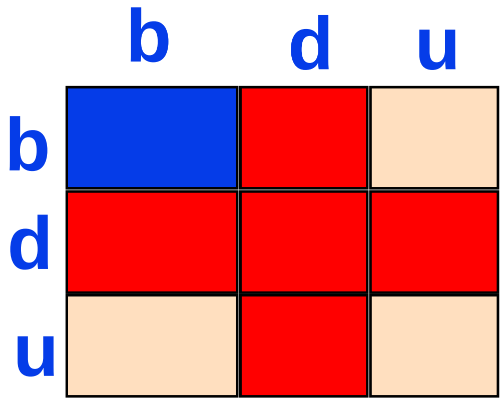
(belief,disbelief,uncertainty,atomicity)

$$b+d+u=1$$

A model of Trust

- **Conjunction**

  $$b(p\&q) = b(p).b(q)$$
  $$d(p\&q) = d(p) + d(q) - d(p).d(q)$$
  $$u(p\&q) = b(p).u(q) + u(p).b(q) + u(p).u(q)$$



A model of Trust

- ***Recommendation:***

$$w^{A,B}(p) = w^{A}(i_B) \otimes w^{B}(p) =$$

$$= (b(i_B).b(p)\ ,\ b(i_B).d(p)\ ,\ \ldots)$$

i_B = *"B reliably tells the truth"*

- ***Consensus***

$$w^{A}(p) \oplus w^{B}(p) = \left(\frac{b_1(p).u_2(p)+u_1(p).b_2(p)}{u_1(p)+u_2(p)-u_1(p).u_2(p)}\ ,\ \ldots \right.$$

Independent evidence (there are alternatives)

Trust in e-Services

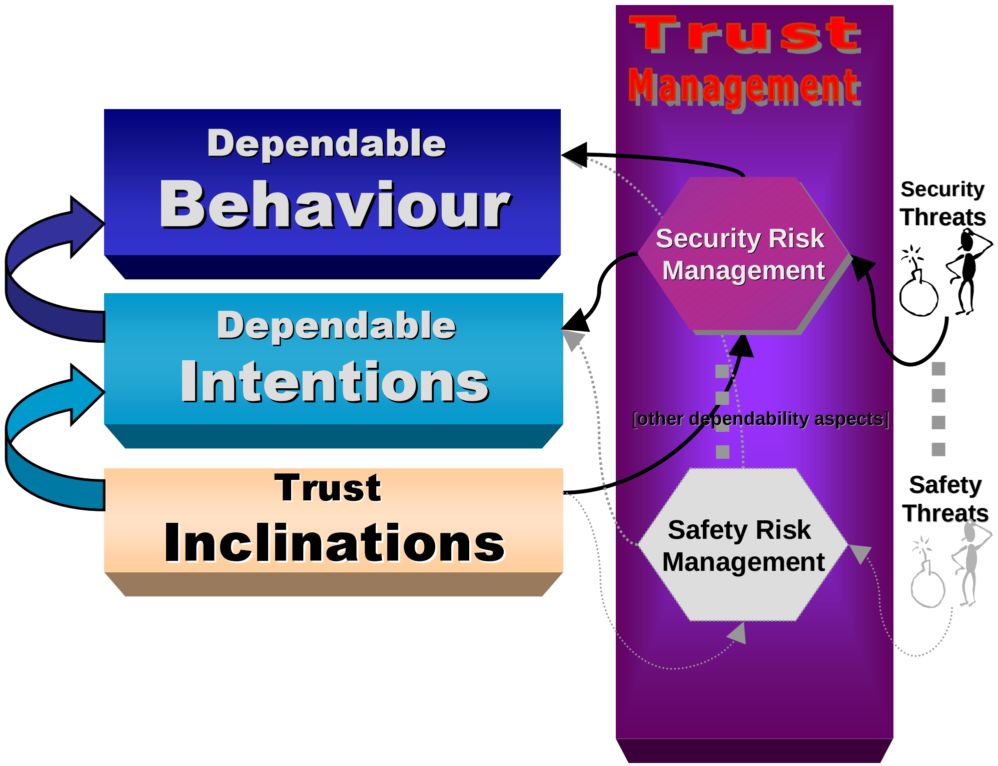
- ☑ motivation for modelling trust
- ☑ a model of trust in e-services
- ☐ **aims for trust management**

Trust Management

Trust Management aims to maximise trust while minimising risk.

The total process of identifying, controlling and minimising the impact of deception and failure in trust.

Analyses threats and trust inclinations while supporting the formation of dependable intentions and controlling dependable behaviour.



Trust management subsumes and relies on risk analysis and risk management.

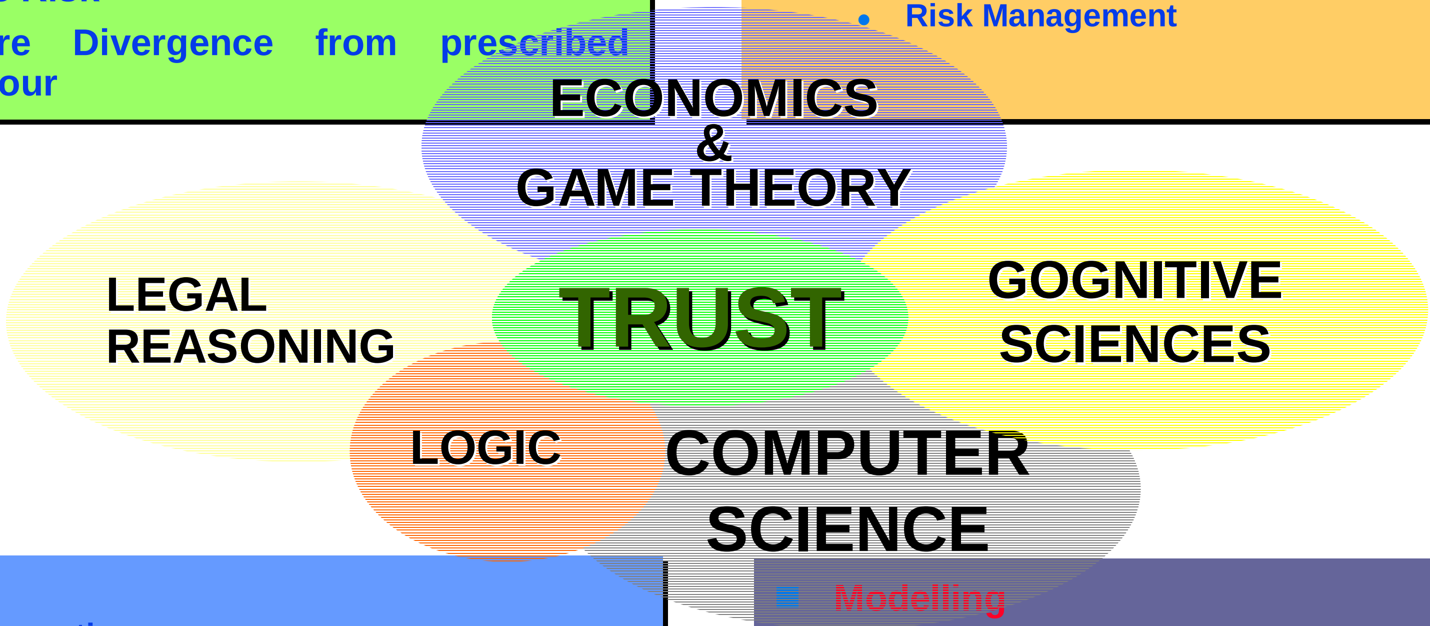
"a unified approach to specifying and interpreting security policies, credentials, relationships [which] allows direct authorization of security-critical actions"

-- **Blaze, Feigenbaum & Lacy 1998 [AT&T POLICYMAKER]**

Trust
Future Work

- **Analysis**
  - Assess Dependability
  - Assess Risk
  - Measure Divergence from prescribed behaviour

- **Management**
  - Policy Oriented Management
  - Contract Management
  - Risk Management



- **Logic**
  - Belief Formation
  - Subjective Reasoning
  - Legal & Deontic Reasoning
  - Conflict Resolution

- **Modelling**
  - Intentional modelling
  - Policy specification
  - Business Process Modelling
  - System Modelling

On the Semantics of Information Hiding

- Do not read this
- Exploring the role of frames in refinement
- Non-interference : Component A does not depend on component B

On the Semantics of Information Hiding

Motivation

Simple examples of the usefulness of information hiding

Informal Treatment

Three interpretations of “Do not read this”

Formal Semantics

Substitutions with read and write frames

Refinement

“Refinement does not preserve information hiding”

Reflections

Examples revisited, Conclusions, Future work

Motivation

Examples

Is x:=x the same as skip ?

- wp(x:=x)P = wp(skip)P
- Dunne ZB2002>... but x:=x+1||skip not same as x:=x+1||x:=x

→ semantics with explicit write frame

Is x:=y-y the same as x:=0 ?

- wp(x:=y-y)P = wp(x:=0)P
- but x:=y-y may not be well formed if y should not be read

→ semantics which interprets read frames also

More Examples

- **Read frames and Non-interference**
  - When is S||T refined by S;T ?
- **Read frames and Initialisation**
  - Is x := x a valid initialisation ? (or x := x-x ?)
- **Read frames and Encapsulation**
  - When does x := y for y : {1,2} refine x :∈ {1,2} ?
- **Read frames and Underspecification**
  - What refines x:=c for some underspecified constant c:{0,1} ?
- **Read frames and Refinement**
  - When is $S \sqsubseteq P \Longrightarrow S$?

Examples

Read frames and Non-interference

- When is S||T refined by S;T ?
- Sufficient: If T *does not read* any variables written by S
  - eg   x:=3 ; y:=4   but not   x:=3 ; y:=x
  - Not necessary: e.g. x:=3 || y := x-x   or   x:=y-y || y:=x
- Sematically: If T *does not depend on* any variables *changed* by S
- How is this justified formally ?
  - If   ????   then $S \| T \sqsubseteq S;T$ ---- to be done

Informal Treatment

An operation in 4 parts

(F,R,W,S)

- F - the frame of all variables in scope
- R - the subset of F which can be read
- W - the subset of F which can be written
- S - the body of the substitution
  - Do we require $R \supseteq W$?

4 Semantic models

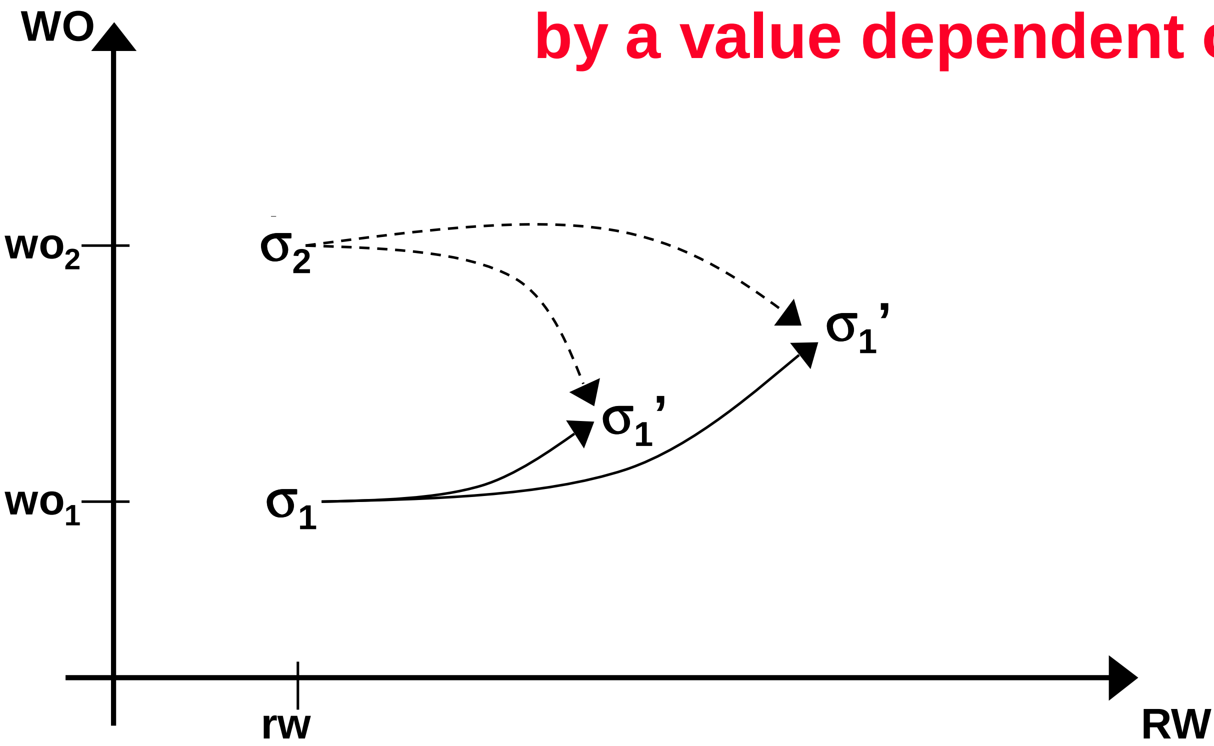
Will give 4 relational semantics models

- M_0 M_R M_W M_{RW}
  - M_0 the usual semantics – no frames
    - $M_0 = \{(\sigma_1, \sigma_2):\Sigma x\Sigma \mid \neg[S]\neg(\sigma_1=\sigma_2)\}$
  - M_W writes only W, reads all – simple
    - $M_W = M_0 \cap \Xi_{F\text{-}W}$
  - M_R reads only R, writes all – to be defined
- $M_{RW} = M_R \cap M_W$ - separation of concerns
  - M_R introduces "*write-only*" variables (F = RW x WO)
  - perhaps WO vars are useful as "partial" substitutions , cf miracles
  - ... but what do they mean ?

write-only (1 of 3) Must-write Semantics

Write only variables *must* be written

by a value dependent only on reads



$$\forall \sigma_1, \sigma_2, \sigma_1' \bullet \sigma_1 \Xi_R \sigma_2 \wedge \sigma_1 M_R \sigma_1' \Rightarrow \sigma_2 M_R \sigma_1'$$

Initialisation of variables: $x := E$ where $x = W$ and vars $E \subseteq R$

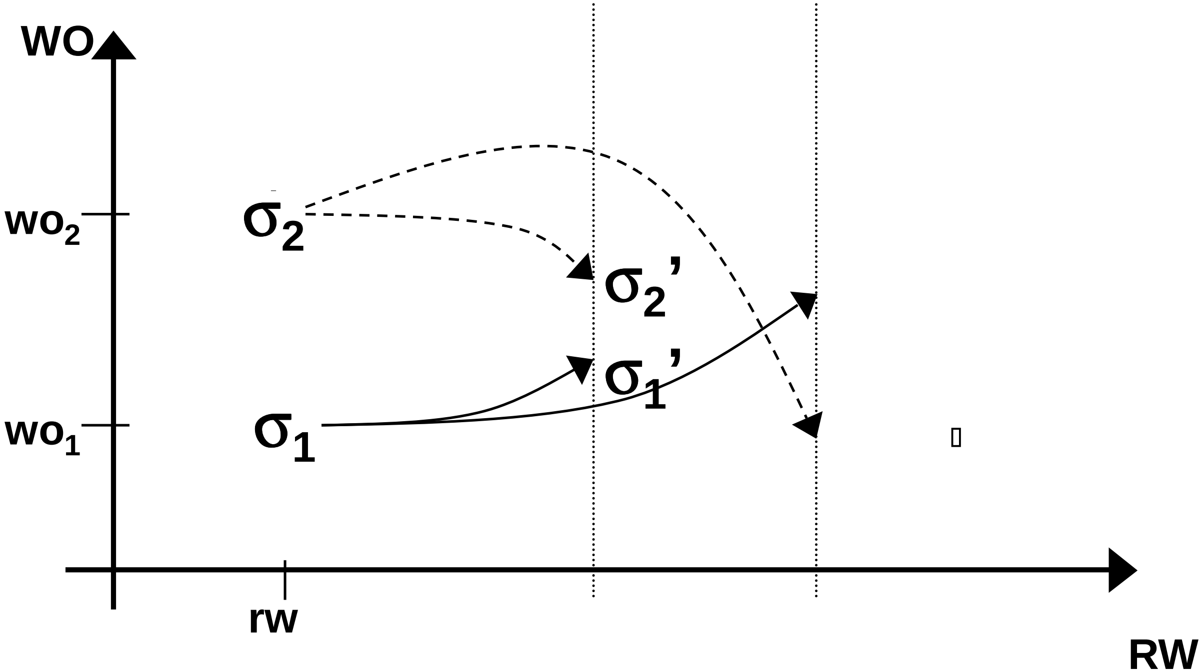
... but does not combine with M_W

write-only (2 of 3) May-write Semantics

- **Must-write disallows skip**
  - **as skip allows old value to persist**
- **May-write reintroduces skip**
  - **"writes x or skip$_x$"**
  - **outcome depends on x only if x unchanged**

- **Not elegant and not what we want.**

write-only (3 of 3) non-interference Semantics



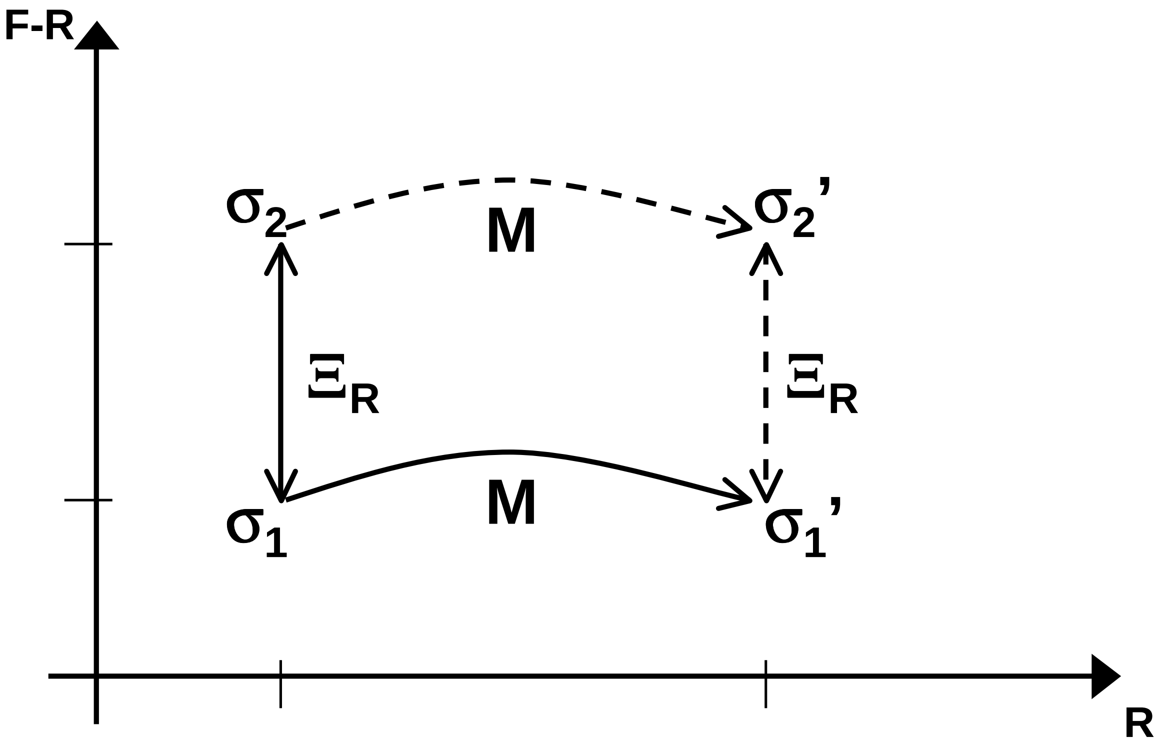
$$\forall \sigma_1, \sigma_2, \sigma_1' \bullet \sigma_1 \Xi_R \sigma_2 \wedge \sigma_1 M \sigma_2 \Rightarrow \exists \sigma_2' \bullet \sigma_1' \Xi_R \sigma_2' \wedge \sigma_1' M \sigma_2'$$

Allows skip and others which do not depend on un-read vars

- **final values of read variables depend only on read variables**
- **no info flow from unread to read**

Adding no-change of un-write vars gives non-int result

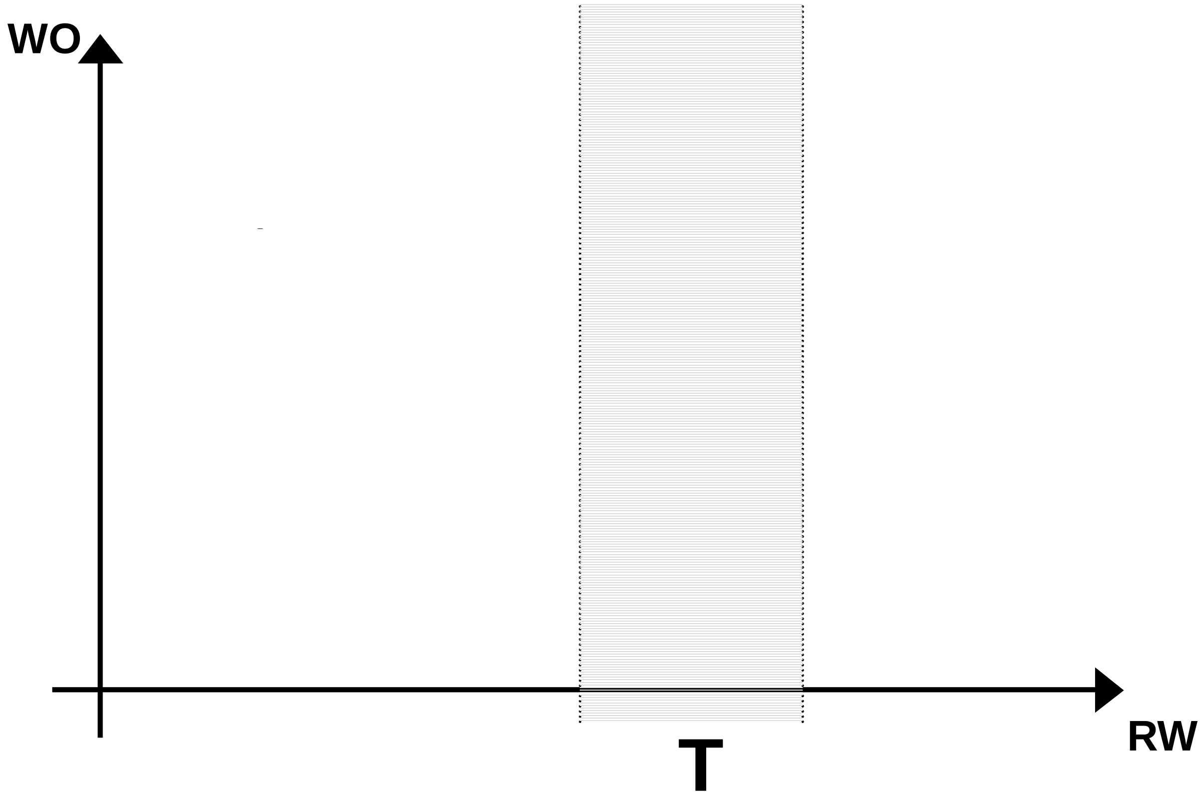
write-only non-interference Semantics (cont)



$$\Xi_R \; ; \; M \subseteq M \; ; \; \Xi_R$$

M_R is largest subrelation of M_0 st Ξ_R is a bisimulation on M_R

Termination Semantics



- **T is a cylinder in state space**
- $\Xi_R(|T|) \subseteq T$

Formal Semantics

Concrete Syntax

	subst	reads	writes
skip	skip	{ }	{ }
assign	x:=E	vars E	{x}
precond	P | S	vars S U reads S	writes S
guarded	G ==> S	vars G U reads S	writes S
sequential	S ; T	reads S U reads T	writes S U writes T
bdd choice	S [] T	reads S U reads T	writes S U writes T
parallel	S||T	reads S U reads T	reads S U reads T
set_reads	^{R}S	R	writes W
set_writes	S^{W}	reads S	W
•••			

- **set_reads (writes) overwrites frame; expands or contracts**
- **Do we require R ⊇ W ?**

Abstract Syntax

(F,R,W,S)

- F - declares and binds all variables in scope
- R $\subseteq$ F – the variables which can be read by an implementation
- W $\subseteq$ F – the variables which can be written by an implementation
- S - the substitution

Semantics

Define three predicates on (T,M) pairs:

$\mathbf{subst}_{(F,R,W,S)}(T,M) \;=\; T \supseteq [S]true \;\wedge\; M \subseteq \neg[S]\neg(\sigma=\sigma')$ No mention R,W

$\mathbf{writes}_{(F,R,W,S)}(T,M) = M \subseteq \Xi_{F\text{-}W}$ No mention R

$\mathbf{reads}_{(F,R,W,S)}(T,M) \;=\; \Xi_R(|T|) \subseteq T \;\wedge\; \Xi_R;M \subseteq M;\Xi_R$ No mention W

Take all (T,M) pairs which satisfy them:

$$\mathbf{S} = \{ \; (T,M) \;\mid\; \mathbf{subst}_{(F,R,W,S)}(T,M) \wedge \mathbf{reads}_{(F,R,W,S)}(T,M) \wedge \mathbf{writes}_{(F,R,W,S)}(T,M) \; \}$$

Take the unique least refined of these:

$$[[(F,R,W,S)]]_0 \;=\; \iota\,(T,M) \in \mathbf{S} \bullet \forall (T_i,M_i) \in \mathbf{S} \bullet \; T \subseteq T_i \;\wedge\; M \supseteq M_i$$

Theorem: Non-interference 1

$$\frac{R_1 \supseteq W_1 \wedge R_2 \supseteq W_2 \qquad R_1 \cap W_2 = \{\} = R_2 \cap W_1}{[[S_1 \parallel S_2]]_0 = [[S_1 ; S_2]]_0 = [[S_2 ; S_1]]_0}$$

Proof – subsumed by later result

... but why require R $\supseteq$ W ?

... and what about refinement ?


Refinement

Refinement Semantics

- Take set of all *frame-respecting* refinements as semantics:
  - $[[(F,R,W,S)]]_1 = S$
- Refinement becomes subset:
  - $(F_1,R_1,W_1,S_1) \sqsubseteq_1 (F_2,R_2,W_2,S_2) \quad = \quad S_1 \supseteq S_2$
- Retrieve $[[\ ]]_0$ by $\cap$ and $\cup$ on S
  - $[[(F,R,W,S)]]_0 = (\bigcap_{(T,M) \in S} T \ , \ \bigcup_{(T,M) \in S} M)$
- New definition admits fewer refinements
- Non-read respecting refinements are pre-filtered out
  - ditto writes
- Refinement *with frames* "encoded" into op's semantics

Theorem: Non-interference 2

For $S_i = (F, R_i, W_i, s_i)$

$$\frac{R_i \supseteq W_i \qquad R_1 \cap W_2 = \{\} = R_2 \cap W_1 \qquad S_i \sqsubseteq_1 T_i}{T_1 ; T_2 = T_1 \| T_2 = T_2 ; T_1}$$

Proof requires:

- 4 frame properties reads(R_i,M_i) and writes(W_i, M_i)
- non-interference conditions F- $W_2 \supseteq R_1$ and F- $W_1 \supseteq R_2$
- read respecting refinement
- and $R_i \supseteq W_i$ (again)


Reflections

Examples revisited

- **Read frames and Non-interference**
  - see last result
- **Read frames and Initialisation**
  - eg inv $x=y$ init $(\{x,y\}, \{\ \}, \{x,y\}, x:=y)$
- **Read frames and Encapsulation**
  - Can we underpin the hiding conditions?
- **Read frames and Underspecification**
  - $(\{x\}, \{\ \}, \{x\}, x :\in \{1,2\})$
- **Read frames and Refinement**
  - new hypotheses in proof rules for refinement ...

Examples revisited

Read frames and Refinement

- strengthen reads and strengthen writes

$$\frac{R_1 \supseteq R_2 \supseteq W}{(F, R_1, W, S) \sqsubseteq (F, R_2, W, S)} \qquad \frac{W_1 \supseteq W_2}{(F, R, W_1, S) \sqsubseteq (F, R, W_2, S)}$$

reads proof requires: $M \subseteq \Xi_{F-W} \subseteq \Xi_{R1-R2}$ requires $R_i \supseteq W$

- Strengthen substitution

$$\frac{\Xi_R\,(\!|\, G \,|\!) \subseteq G}{(F, R, W, S) \sqsubseteq (F, R, W, G ==> S)}$$

proof requires G respects read frame

So what about $R \supseteq W$ ....

Why needed $R \supseteq W$ for the proofs?

- elsewhere reads, writes, and subst orthogonal

Strengthen reads predicate to

- $\text{reads'}_{(F,R,W,S)}(R,M) = \forall S \supseteq R \bullet \text{reads}(S,M)$
  - no info flow between unreads

Gives more general form of non-int result....

Theorem: non-interference 3

$$\frac{\begin{array}{c}\text{reads}'(R_i, M_i) \wedge \text{writes}(W_i, M_i) \\ W_1 \cap (R_2 \cup W_2) = \{\} = W_2 \cap (R_1 \cup W_1)\end{array}}{M_1; M_2 = M_2; M_1}$$

Proof is "satisfyingly precise"

Details in FME'02 paper


¬ The End