Title	Perspective of Verifiable and Evolvable e-Society
Author(s)	Katayama, Takuya
Citation	
Issue Date	2005-03-11
Type	Presentation
Text version	publisher
URL	http://hdl.handle.net/10119/8267
Rights	
Description	JAIST 21　CCE　　　　　2005　　　　= JAIST 21st Century CCE Symposium 2005 " Verifiable and Evolvable e-Society", 2005　3　10　　11　, 　　, Key note speech

Japan Advanced Institute of Science and Technology

Perspective of Verifiable and Evolvable e-Society

Takuya Katayama
Leader, COE Program
School of Information Science
Japan Advanced Institute of Science and Technology

COE Program
"Verifiable and Evolvable e-Society" (1/3)

- COE Program - Overview
  - Targeted Support for Creating World-level Research and Education Bases, Started FY 2002
  - National recognition of excellent group
- "Verifiable and Evolvable e-Society" Program
  - One of 12 computer science related programs so far granted
  - Granted in 2004 in "Revolutionary Area " (28 out of 330)
  - Only one program in software engineering and dependability area
- Establish research and education bases on the science and technology for Trustworthy e-Society from two standpoints:
  - Verification and Evolution of e-Society
    - Formal logic, software engineering and artificial intelligence
  - Infrastructures for Trustworthy e-Society
    - Algorithm , human interface, network and hardware
  - 5 year project

COE Program
"Verifiable and Evolvable e-Society " (2/3)

- Create a research base on Trustworthy e-Society
  - Formal description of e-Society
  - Trustworthy requirements and their verification methods
  - Modeling of e-Society
  - Verification and simulation mechanisms
  - Evolution of e-Society
  - Trustworthy infrastructures for e-Society

COE Program
## "Verifiable and Evolvable e-Society " (3/3)

- Create an education base in Trustworthy e-Society area
  - Train Ph.D level researchers and engineers in the design, verification and implementation of e-Society / e-Government
  - Establish curriculum
    - 15 courses that we have on trustworthy information systems
      - Logic, formal systems, verification, software design, security, networks, hardware ...
    - New courses in e-Government / e-society (NTT Data Corp.)
      - Large scale information system
      - Social information systems
  - 30 Ph.D students in 5 years

Collaborations

- National collaborators
  - NTT Data Corporation
    - Research on verification of enterprise information systems
    - Collaborated Unit on "e-Society Systems" in School of Information Science
  - INTEC Corporation and Toyama Prefecture
    - Study on the legal reasoning in the administration of Toyama prefecture
  - Hokuriku NES Corporation
    - Formal methods for security protocol verification
- International collaborators
  - AT&T Labs-Research, EPFL, Politecnico di Milano,
  - NICTA (to be considered)

---

e-Society

- e-Society is a part of social system which is realized by information system
  - Supports fundamental part of our social activities
  - Politics, administration, business, judicature, education, ...
  - Infrastructure of our society
- e-Society should be trustworthy.

Our Society

Social Infrastructure Information System
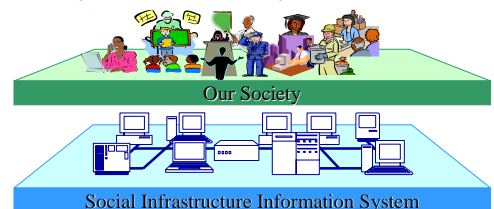
Requirements for Trustworthy e-Society

1. **Correctness**
   Are the functions correct?   "Is my tax amount correctly calculated?"
2. **Accountability**
   Can questions about the information system answer be answered?
3. **Security**
   No illegal data access, Privacy protected…
4. **Fault Tolerance**
   Can tolerate failures and accidents?
5. **Evolvability**
   Can e-society system be changed according to the change of society?
6. **Trustworthy infrastructures**
   Supported by reliable network and hardware systems

Correctness

- Requires that e-Society information system correctly implements our real society.
  - Structures and functions of e-Society have to be consistent with the laws and systems of our society.
  - Is the tax amount correctly calculated ?
- The most important requirement to e-Society

Correctly implemented ?
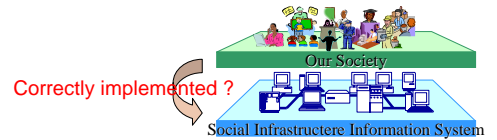
Accountability

- Requires that it is possible to answer questions or explain about e-Society
  - Why is my tax amount correct?
  - You or the information system itself has to answer.
- As details of e-Society is hidden inside its complex information system, there must be some mechanism to answer.

Why ?

Security

- Requires that information security is observed according to what are explicitly or implicitly defined in our security-related social systems and laws.
  - Is your private data illegally accessed or altered?
  - Is it possible for enterprise data to be stolen?

Fault Tolerance

- Requires that e-Society continues to operate its fundamental functions and services despite failures and accidental events of individuals, organizations and underlying network and hardware systems.


Evolvability

- Requires that e-Society information system could be changed according to the change of our society.
  - Lack of evolvability will make e-Society obsolete, and prevents the progress of our society.
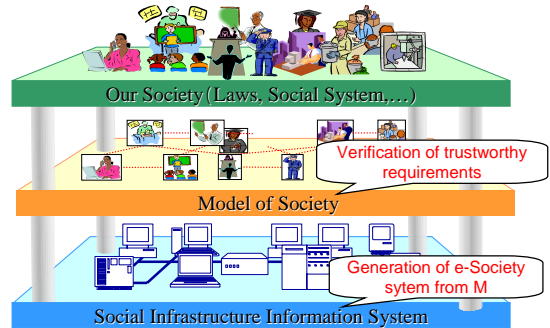
Trustworthy e-Society Through Advanced Computer Science

- A large body of computer science has been formed and used to construct complex social infrastructure information systems.
  - Software, network, hardware, AI, algorithms, logic,....
  - The information systems have supported and continue to support fundamental part of our lives.
- Still,...
  - They are not trustworthy enough to leave our lives in the coming e-Society age.
  - More computer science has to be put into the development of information system,

  At the same time
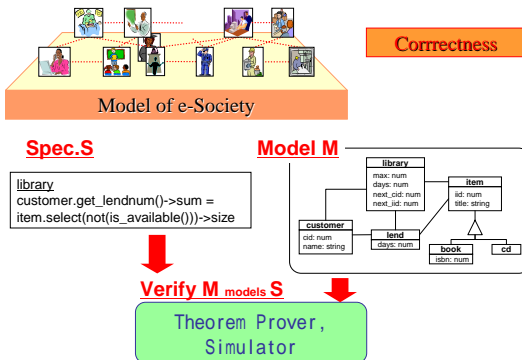 - More social structures have to be explicitly considered in the design of e-Society systems.
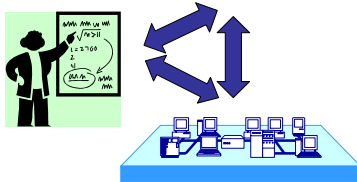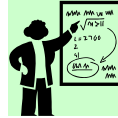
Build trustworthy e-Society on advanced computer science and sociological considerations.

Model Driven Approach to Trustworthy e-Society

Our Society Laws, Social System,…)

Verification of trustworthy requirements

Model of Society

Generation of e-Society sytem from M

Social Infrastructure Information System

Verification of e-Society, An Example

Correctness

Model of e-Society

Spec.S

```
library
customer.get_lendnum()->sum =
item.select(not(is_available()))->size
```

Model M

library
max: num
days: num
next_cid: num
next_iid: num

item
iid: num
title: string

customer
cid: num
name: string

lend
days: num

book
isbn: num

cd

Verify M models S

Theorem Prover, Simulator

Some Challenges

Formal Description of e-Society

Laws, Social System L — determines → Our Society S
formalized by
Formal Spec. P of e-Society — specifies → Model M of e-Society for S
modeled by
expressed in
Formal Logic F, Reasoning System

- Logics for e-Society, allowing to describe and infer about individuals, organizations, their obligations/rights and other relations in e-Society
- Reasoning system for the logics
- Algorithms for efficient reasoning
- Mathematical structures of the logics

Legal Reasoning and Related Language Processing

Laws, Social System L — determines → Our Society S
formalized by
Formal Spec. P of e-Society — specifies → Model M of e-Society for S
modeled by

- How formal specification P could be obtained from legal documents L?
  Natural language processing + Manual work
- Check if P consistent? If not, how to remove inconsistency?
  Use of theorem proving/inference engine
- How a question Q about P be answered?
  Conduct inference P|-Q .
  Generate explanation about the results in natural language?

Modeling e-Society

Laws, Social System L — determines → Our Society S
formalized by
Formal Spec. P of e-Society — specifies → Model M of e-Society
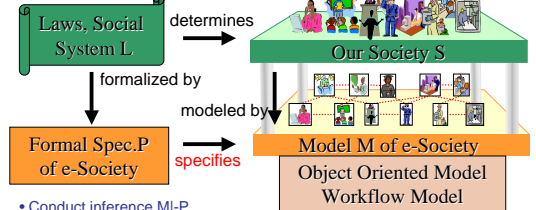modeled by

Object Oriented Model
Workflow Model

- Methods for obtaining M from S
  - Modeling should reflect social structures
  - Object-Oriented / Workflow
- Robust modeling again evolution
- Preparation for accountability
- Representation of rules and policies in real word S

Verification of Correctness of M against P

Laws, Social System L — determines → Our Society S
formalized by
Formal Spec. P of e-Society — specifies → Model M of e-Society
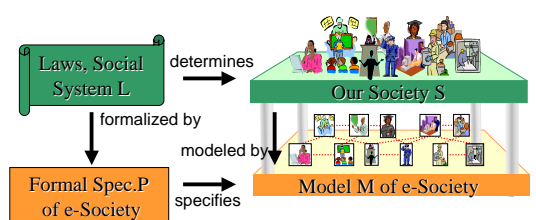modeled by

Object Oriented Model
Workflow Model

- Conduct inference M|-P
  Apply conventional program/software verification techniques
  e-Society specific verification methods have to be developed.
- Model checking M for correct workflows
- Verification may be easier than for programs ?
  Yes: Level of abstraction of M is much higher than programs and
  its size will be smaller.
  No: It has to handle social concepts which may be hard to formalize.

Accountability
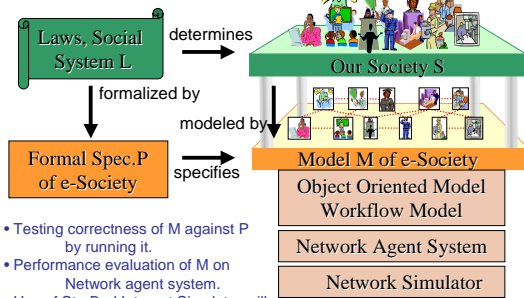
D {
Our Society S
modeled by
Model M of e-Society
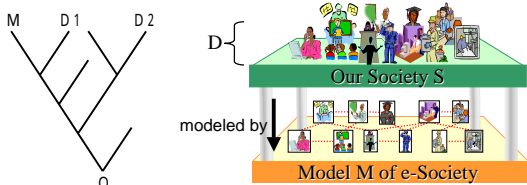
- Answering a question Q about e-Society model M
  Why is my tax so calculated ?
- Very important as everything is hidden inside information system in e-Society.
- May be formulated as an inference
  M, D|-Q, where D is relevant knowledge about real S
  Generate explanation from the proof
- It may require a very long inference and not be easy to be done mechanically.
  M has to be prepared to make accountability easier.
  Object with accountability mechanism

Security

Laws, Social System L — determines → Our Society S
formalized by
Formal Spec. P of e-Society — specifies → Model M of e-Society
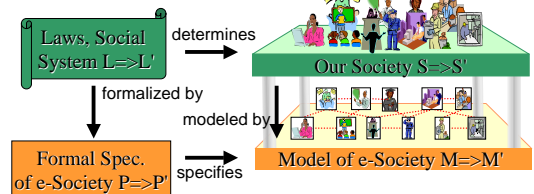modeled by

- Need to show information leak or illegal data access could not happen in M.
- Cryptography, secure protocols, wiretapping protection, ...
- Mechanical verification of legal information access
  Given the structure or description of e-Society model M,
  express the security requirements R given by security related
  laws or rules by a formal logic,
  prove M |- R using verification techniques.

e-Society Simulator

Laws, Social System L → (determines) → Our Society S

Laws, Social System L → (formalized by) → Formal Spec. P of e-Society

Formal Spec. P of e-Society → (specifies) → Model M of e-Society

Our Society S → (modeled by) → Model M of e-Society

Model M of e-Society:
- Object Oriented Model Workflow Model
- Network Agent System
- Network Simulator

- Testing correctness of M against P by running it.
- Performance evaluation of M on Network agent system.
- Use of StarBed Internet Simulator will help more realistic evaluation.

Evolution of e-Society

Laws, Social System L=>L' → (determines) → Our Society S=>S'

Laws, Social System L=>L' → (formalized by) → Formal Spec. of e-Society P=>P'

Formal Spec. of e-Society P=>P' → (specifies) → Model of e-Society M=>M'

Our Society S=>S' → (modeled by) → Model of e-Society M=>M'

- In the change P=>P' of social specification, how to find and remove inconsistency in P' ?
- How should model evolution M=>M' be done according to P=>P' ?
  Aspects, Ontology, Versioning, Components, ...
  Need to investigate how P and M are related.
        How individuals, organization and their relations are modeled in M ?

Dependability

- M needs to continue its functions despite failures and accidents occurred to individuals and organizations in M.
  - Apply FT technologies for distributed systems
    Group membership, Consensus, atomic broadcast,...
  - What are e-Society specific problems, which are not found in the computer/network systems ?
- What is the implication of the e-Society dependability requirements to infrastructure networks and computer systems supporting it.

Our Society S

Model of e-Society M
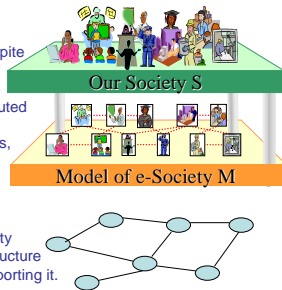
Infrastructures for Trustworthy e-Society

- Mathematical infrastructure
  - Algorithmic study for efficient reasoning systems
- Advanced human interface infrastructure
  - Secure exchange of information between people and the e-Society, multimedia-based interactive access system, human interface for disabled people, shared intelligent spaces that make use of robots
- High-reliability network infrastructure
  - Reliability and security technologies for constructing and operating heterogeneous internet and ubiquitous network infrastructures for e-Society
- High-reliability hardware infrastructure
  - Processor design through fully automated synthesis, based on a specification description; fault tolerant architecture; and a highly reliable real-time operating system

Summary

- COE programs in general
- COE program "Verifiable and Evolvable e-Society"
  - Trustworthy requirements
    - Correctness, Accountability, Security, Evolvability, Fault-tolerance
  - Model driven approach + Formal approach + Sociological approach
- Some challenges