IFIP WG10.4

Evidence-based Computing for Dependability (Demo)

Kimio Kuramitsu
Yokohama National University
Today’s Talks

• First prototype of our open system framework
  – Target: Embedded Linux
  – Demo in Embedded Technology 2009
  – Scenario: networked video surveillance system
    • Today’s demo are ported on VMWare

• Experience
  – toward “open systems”
  – Future direction
Classic View: Dependable OS

- Dependable OS never crashes
- Applications must handle with external errors (such as I/O errors) by itself
Our View: D-Framework

• Dependable OS must be dependable
Our View: D-Framework

- Dependable OS must be dependable
- Evidences will be a common basis
Why We Focus on Evidence?

• **Evidence:**
  – digital records of facts: source code, logs
  – “correct” enough to take logical actions

• **Evidences are a key to:**
  – account facts
  – reestablish agreements
  – correct situations
Today’ Demo
developed with
Masahiro Kato, Youtaro Hiraoka, Masaki Goshima
Ken Igarashi, Masahiro Ide, Shinpei Nakata and Me

Goal Structuring Notation, View of monitored evidences

Monitoring Injection (Work Up)  Help!!

Operating System

Evidence Infrastructure

Framework
This story is based on a true event at Embedded Technology 2009, Japan
ET2009 Day 1

Yutaka Matsuno, 10:01 am
いまこんな感じです

Yasuhiko Yokote, 10:03 am
さすがに１０：０１だとお客さん
はいない？？？

Yutaka Matsuno, 10:01 am
一人きりました
デモが動いていないです

Yosuhiko Yokote, 11:44am
ぴーんち！昨日は動いていたの
に・・・

Yutaka Matsuno, 11:45 am
横国の学生さんがいま会場にいっ
ているそうです
MT2009 Day 2

Me,
何だったの？

My Student N
Web Server の起動がうまくいかなくて通信ができなかったようですね

Me,
それだけである大騒ぎなの？

My Student N
DEOSって何がしたいんだったのでしょうか？
It was a typically student bug

- My student forgot exception handling. He didn’t know what if the server is down.

```java
try {
    in = new InputStream($dcase.server);
    ....
}
catch(IOExeption e) {

}
```

- No blame on him
  - “Less experience” could be a good analogy to “unexpected faults” in open systems
Towards Open Systems

• **Failures will happen**
  – Everything is not predictable
  – Vulnerable to unexpected happenings.

• **Accountability is important**
  – Everybody feels anxious, insecure and angry

• **Human experts are needed to recover**
“Open Systems” Management

- Seamless integration of
  - Expert intervention for unexpected faults
  - Automated management for expected faults
Research Directions

• Evidence technology
  – collection mechanism and storage
  – standardization

• Models for evidence
  – dependability cases
  – policy and fault analysis

• Language
  – Describe dependability practices to share and automate
Future Direction

- All of tools have been implemented in Konoha, our dependable scripting language.
Question?

Kimio Kuramitsu
Yokohama National University
kimio@ynu.ac.jp