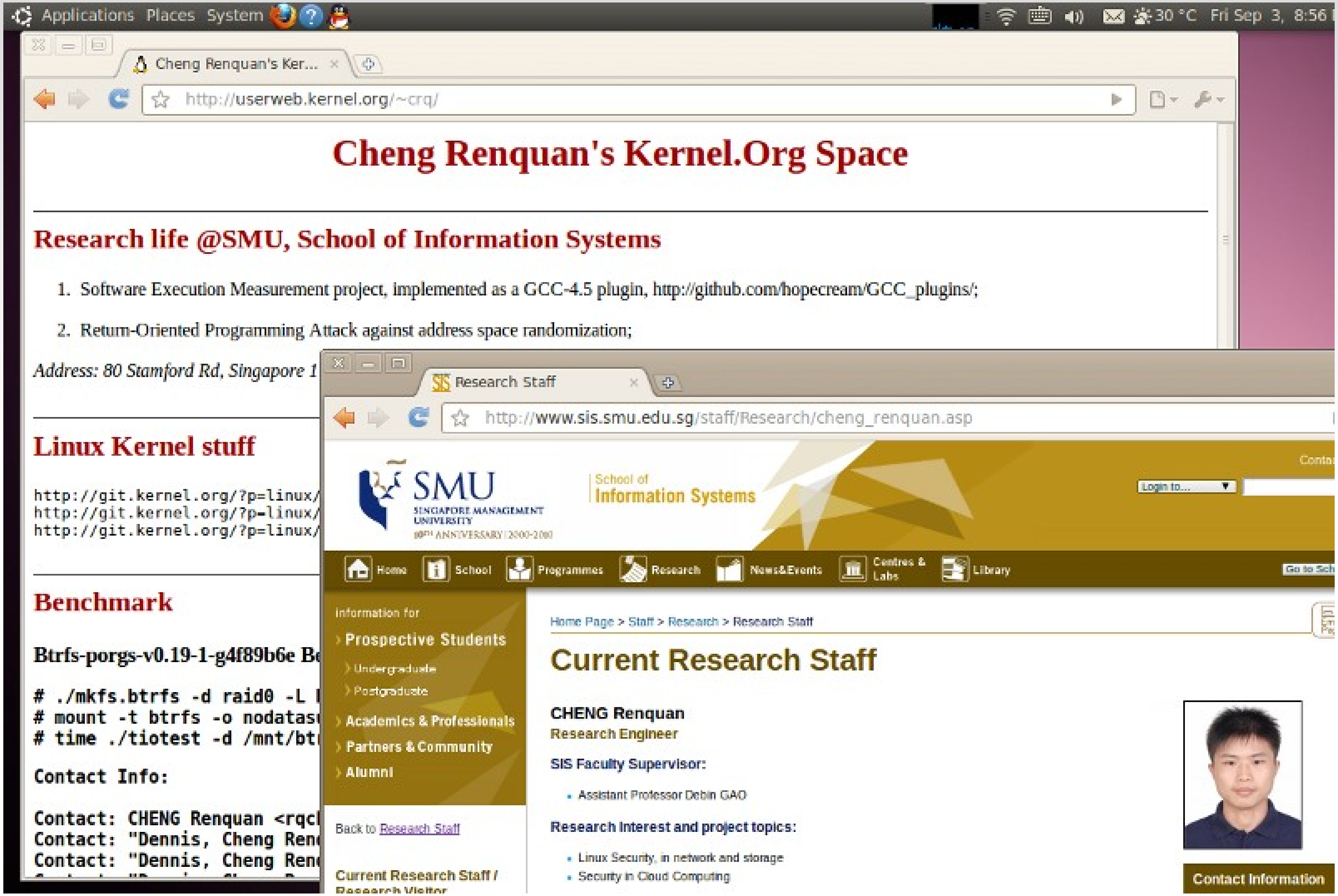
GCC compiler programming / hacking tutorial

SMU
SINGAPORE MANAGEMENT UNIVERSITY
10TH ANNIVERSARY | 2000-2010

School of
Information Systems

About me


Applications Places System
30 °C Fri Sep 3, 8:56
Cheng Renquan's Ker...
http://userweb.kernel.org/~crq/
Research Staff
http://www.sis.smu.edu.sg/staff/Research/cheng_renquan.asp
SMU SINGAPORE MANAGEMENT UNIVERSITY 10TH ANNIVERSARY 2000-2010
School of Information Systems
Login to...
Home
School
Programmes
Research
News&Events
Centres & Labs
Library
Go to Sch
Information for
Prospective Students
Undergraduate
Postgraduate
Academics & Professionals
Partners & Community
Alumni
Back to Research Staff
Current Research Staff / Research Visitor
Home Page > Staff > Research > Research Staff
Contact Information

Cheng Renquan's Kernel.Org Space

Research life @SMU, School of Information Systems

1. Software Execution Measurement project, implemented as a GCC-4.5 plugin, http://github.com/hopecream/GCC_plugins/;
2. Return-Oriented Programming Attack against address space randomization;

Address: 80 Stamford Rd, Singapore 1

Linux Kernel stuff

```
http://git.kernel.org/?p=linux/
http://git.kernel.org/?p=linux/
http://git.kernel.org/?p=linux/
```

Benchmark

Btrfs-porgs-v0.19-1-g4f89b6e Be

```
# ./mkfs.btrfs -d raid0 -L 
# mount -t btrfs -o nodatasu
# time ./tiotest -d /mnt/bt

Contact Info:

Contact: CHENG Renquan <rqc
Contact: "Dennis, Cheng Ren
Contact: "Dennis, Cheng Ren
```

Current Research Staff

CHENG Renquan
Research Engineer

SIS Faculty Supervisor:

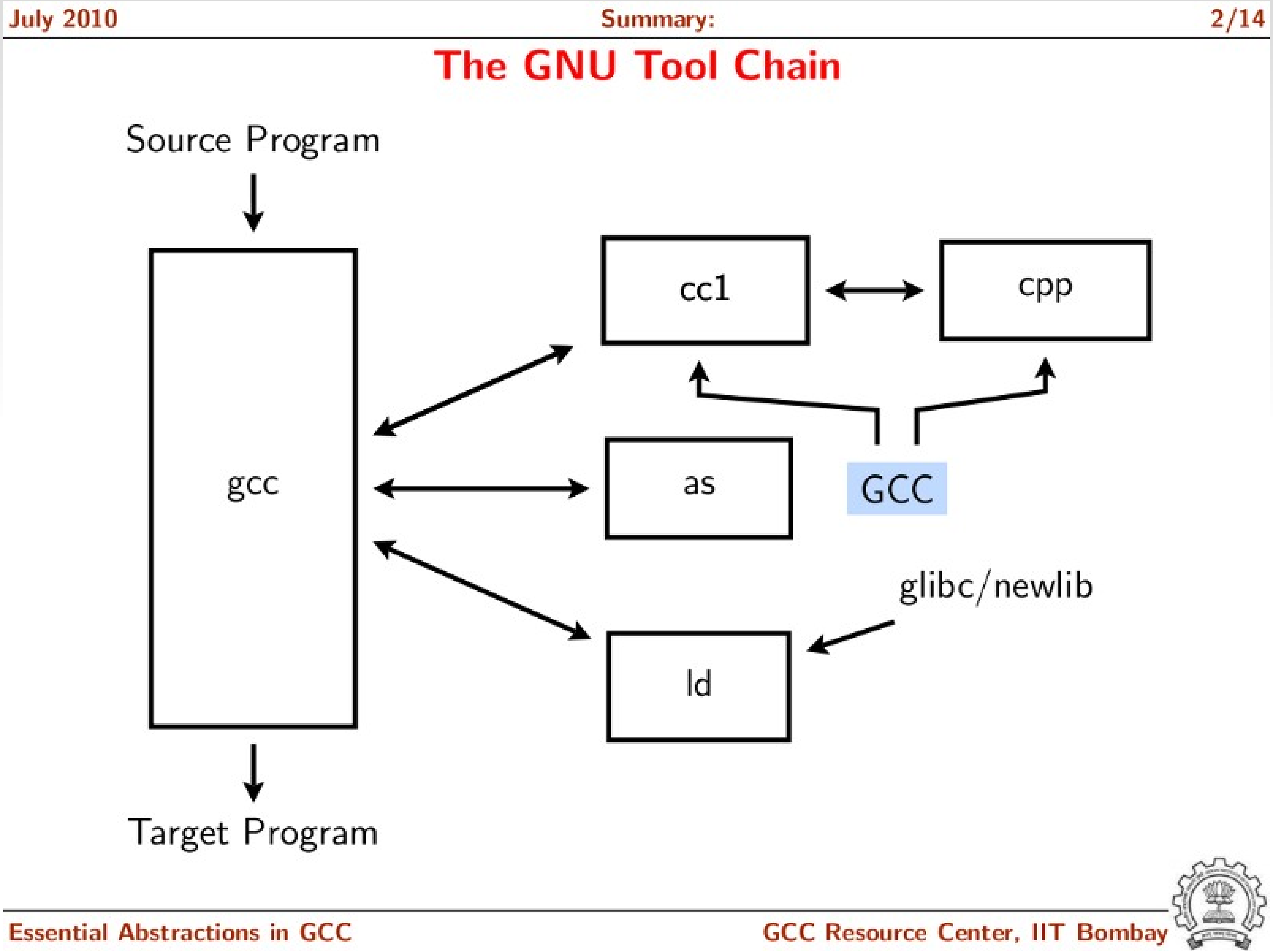
- Assistant Professor Debin GAO

Research Interest and project topics:

- Linux Security, in network and storage
- Security in Cloud Computing

SMU SINGAPORE MANAGEMENT UNIVERSITY
10TH ANNIVERSARY 2000-2010
School of Information Systems

Gcc Architecture



July 2010 Summary: 2/14

The GNU Tool Chain

Source Program

gcc

cc1

cpp

as

GCC

glibc/newlib

ld

Target Program

Essential Abstractions in GCC

GCC Resource Center, IIT Bombay

Compile GCC

```
 $ { time { enable_bootstrap=no ../gcc-
4.5-20100902/configure --prefix=/usr
--disable-nls --with-system-zlib &&
with_arch=core2 with_pkgversion='GCC
compiled by <crq at gcc.gnu.org> 0.1' make
--debug=b -j1 DESTDIR=$PWD/dest; } ; } |&
tee -a build-log
 $ time make --debug=b -j1 install
DESTDIR=~/opt/gcc-0902/ |& tee -a install-
log
```

Plugin Structure

- available since Gcc-4.5, April 2010

Simple Plugin Tutorials

- hello.c
- tut1 by register_callback
- tut2 by register passes
- plugin arguments

Pass Manager

- use GIMPLE passes
- use IPA passes
- use RTL passes

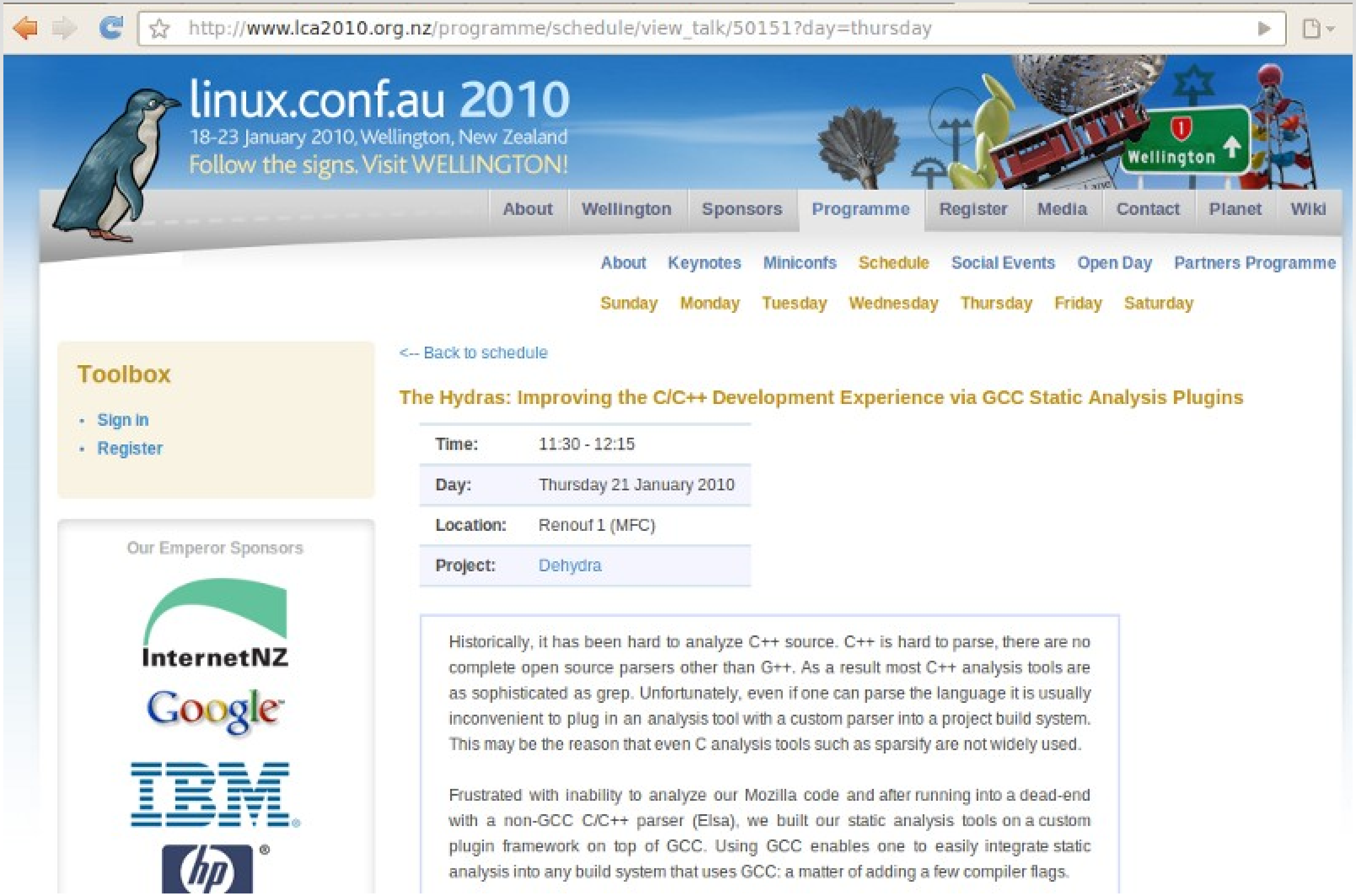
What interesting things could be done through a gcc plugin?

I. Read-only Analysis

II. Modifying during compiling

And, some further materials, ...

The Hydras: Improving the C/C++ Development Experience via GCC Static Analysis Plugins



<-- Back to schedule

The Hydras: Improving the C/C++ Development Experience via GCC Static Analysis Plugins

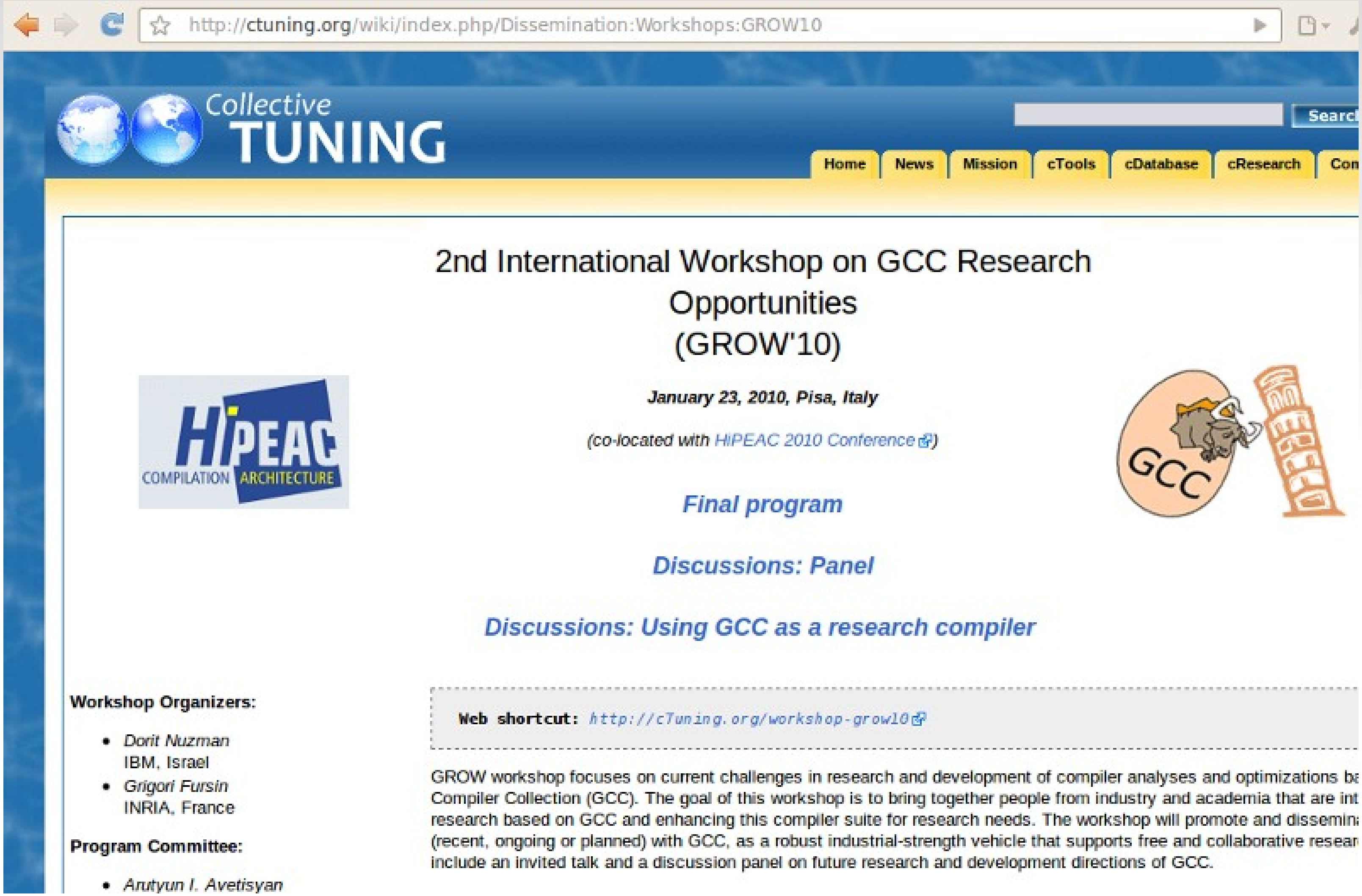
Time:	11:30 - 12:15
Day:	Thursday 21 January 2010
Location:	Renouf 1 (MFC)
Project:	Dehydra

Historically, it has been hard to analyze C++ source. C++ is hard to parse, there are no complete open source parsers other than G++. As a result most C++ analysis tools are as sophisticated as grep. Unfortunately, even if one can parse the language it is usually inconvenient to plug in an analysis tool with a custom parser into a project build system. This may be the reason that even C analysis tools such as sparsify are not widely used.

Frustrated with inability to analyze our Mozilla code and after running into a dead-end with a non-GCC C/C++ parser (Elsa), we built our static analysis tools on a custom plugin framework on top of GCC. Using GCC enables one to easily integrate static analysis into any build system that uses GCC: a matter of adding a few compiler flags.

SMU
SINGAPORE MANAGEMENT UNIVERSITY
10TH ANNIVERSARY | 2000-2010
School of Information Systems

Workshop on GCC Research Opportunities (GROW'10)


http://ctuning.org/wiki/index.php/Dissemination:Workshops:GROW10
Collective TUNING
Searc
Home
News
Mission
cTools
cDatabase
cResearch
Con
HiPEAC COMPILATION ARCHITECTURE
GCC

2nd International Workshop on GCC Research Opportunities
(GROW'10)

January 23, 2010, Pisa, Italy

(co-located with HiPEAC 2010 Conference)

Final program

Discussions: Panel

Discussions: Using GCC as a research compiler

Workshop Organizers:

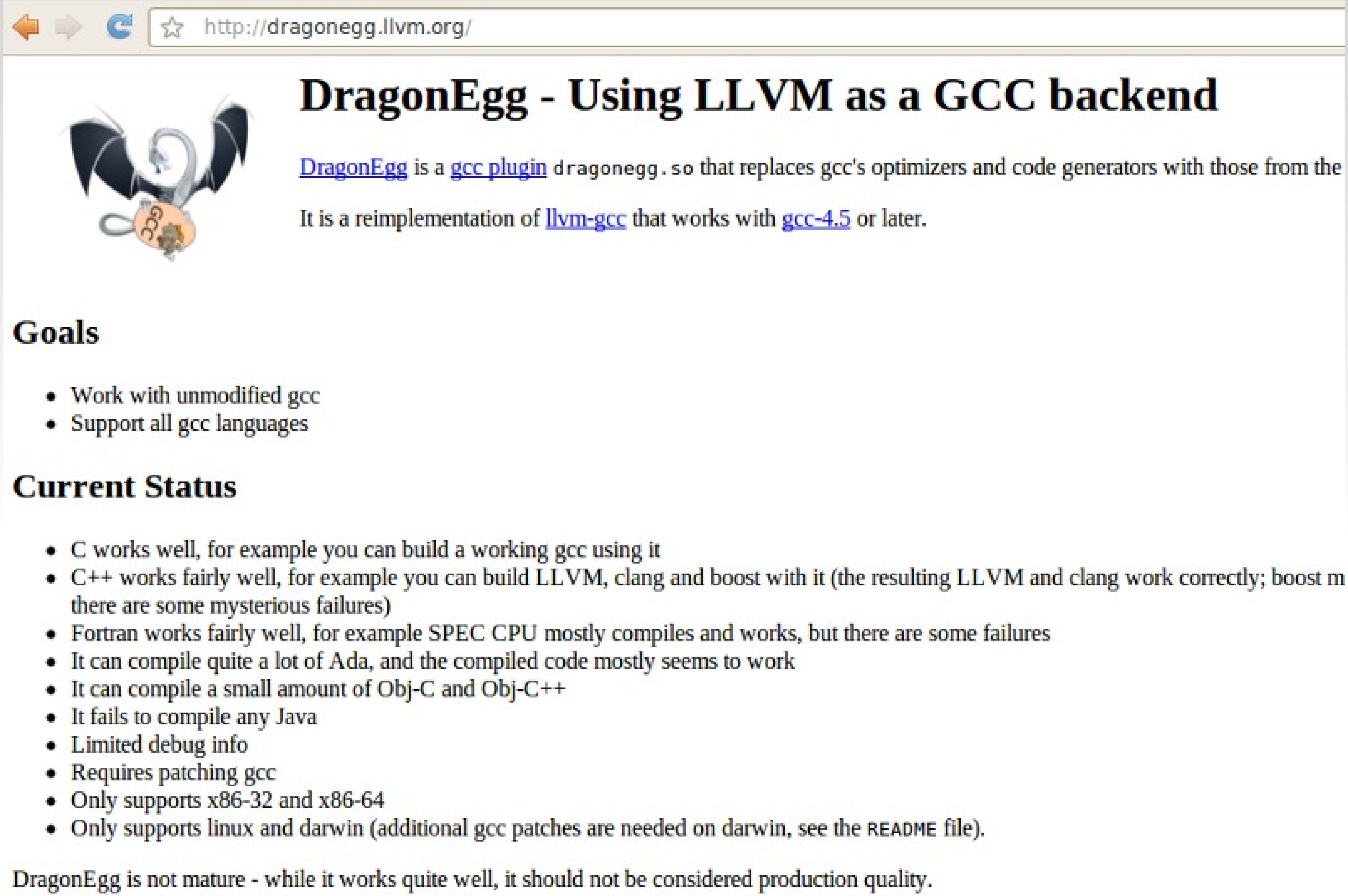
- *Dorit Nuzman*
  IBM, Israel
- *Grigori Fursin*
  INRIA, France

Program Committee:

- *Arutyun I. Avetisyan*

Web shortcut: *http://cTuning.org/workshop-grow10*

GROW workshop focuses on current challenges in research and development of compiler analyses and optimizations ba Compiler Collection (GCC). The goal of this workshop is to bring together people from industry and academia that are int research based on GCC and enhancing this compiler suite for research needs. The workshop will promote and dissemina (recent, ongoing or planned) with GCC, as a robust industrial-strength vehicle that supports free and collaborative resear include an invited talk and a discussion panel on future research and development directions of GCC.



http://dragonegg.llvm.org/

DragonEgg - Using LLVM as a GCC backend

DragonEgg is a gcc plugin `dragonegg.so` that replaces gcc's optimizers and code generators with those from the

It is a reimplementation of llvm-gcc that works with gcc-4.5 or later.

Goals

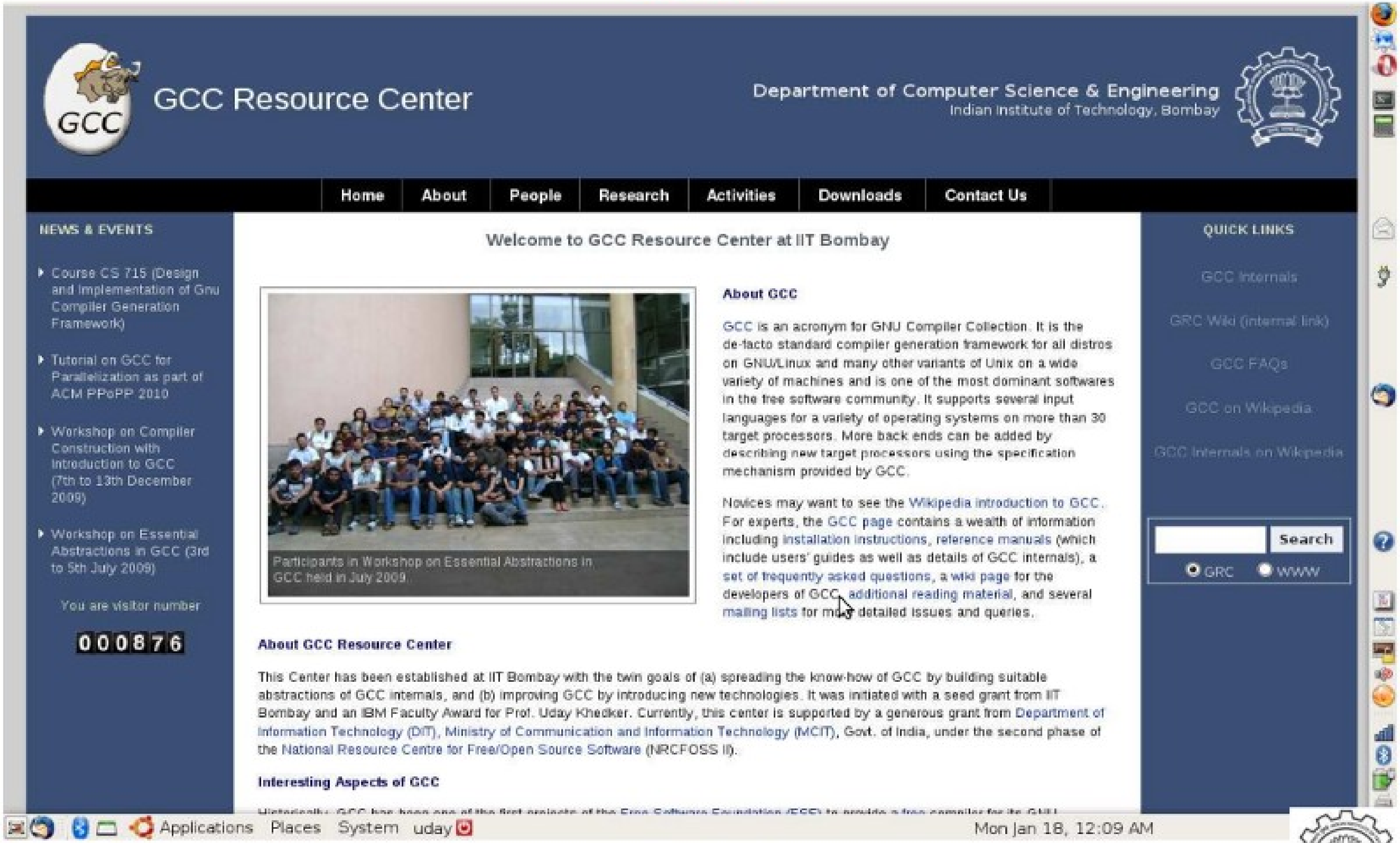
- Work with unmodified gcc
- Support all gcc languages

Current Status

- C works well, for example you can build a working gcc using it
- C++ works fairly well, for example you can build LLVM, clang and boost with it (the resulting LLVM and clang work correctly; boost m there are some mysterious failures)
- Fortran works fairly well, for example SPEC CPU mostly compiles and works, but there are some failures
- It can compile quite a lot of Ada, and the compiled code mostly seems to work
- It can compile a small amount of Obj-C and Obj-C++
- It fails to compile any Java
- Limited debug info
- Requires patching gcc
- Only supports x86-32 and x86-64
- Only supports linux and darwin (additional gcc patches are needed on darwin, see the `README` file).

DragonEgg is not mature - while it works quite well, it should not be considered production quality.

2009. . .



GCC
GCC Resource Center
Department of Computer Science & Engineering
Indian Institute of Technology, Bombay
Home
About
People
Research
Activities
Downloads
Contact Us

NEWS & EVENTS

- Course CS 715 (Design and Implementation of Gnu Compiler Generation Framework)
- Tutorial on GCC for Parallelization as part of ACM PPoPP 2010
- Workshop on Compiler Construction with Introduction to GCC (7th to 13th December 2009)
- Workshop on Essential Abstractions in GCC (3rd to 5th July 2009)

You are visitor number

000876

Welcome to GCC Resource Center at IIT Bombay

Participants in Workshop on Essential Abstractions in GCC held in July 2009

About GCC

GCC is an acronym for GNU Compiler Collection. It is the de-facto standard compiler generation framework for all distros on GNU/Linux and many other variants of Unix on a wide variety of machines and is one of the most dominant softwares in the free software community. It supports several input languages for a variety of operating systems on more than 30 target processors. More back ends can be added by describing new target processors using the specification mechanism provided by GCC.

Novices may want to see the Wikipedia introduction to GCC. For experts, the GCC page contains a wealth of information including installation instructions, reference manuals (which include users' guides as well as details of GCC internals), a set of frequently asked questions, a wiki page for the developers of GCC, additional reading material, and several mailing lists for more detailed issues and queries.

About GCC Resource Center

This Center has been established at IIT Bombay with the twin goals of (a) spreading the know-how of GCC by building suitable abstractions of GCC internals, and (b) improving GCC by introducing new technologies. It was initiated with a seed grant from IIT Bombay and an IBM Faculty Award for Prof. Uday Khedker. Currently, this center is supported by a generous grant from Department of Information Technology (DIT), Ministry of Communication and Information Technology (MCIT), Govt. of India, under the second phase of the National Resource Centre for Free/Open Source Software (NRCFOSS II).

Interesting Aspects of GCC

Historically, GCC has been one of the first projects of the Free Software Foundation (FSF) to provide a free compiler for its GNU

QUICK LINKS

GCC Internals

GRC Wiki (internal link)

GCC FAQs

GCC on Wikipedia

GCC Internals on Wikipedia