Let's write a Debugger!

Levente Kurusa <lkurusa@linux.com>

Imperial College London

`linux.conf.au` 2018, Sydney, Australia January 25, 2018

Who am I?

- Final year undergraduate at Imperial College London
- Previously at Apple and Red Hat
- Now researching different ways of operating system construction
- Low-level hacker

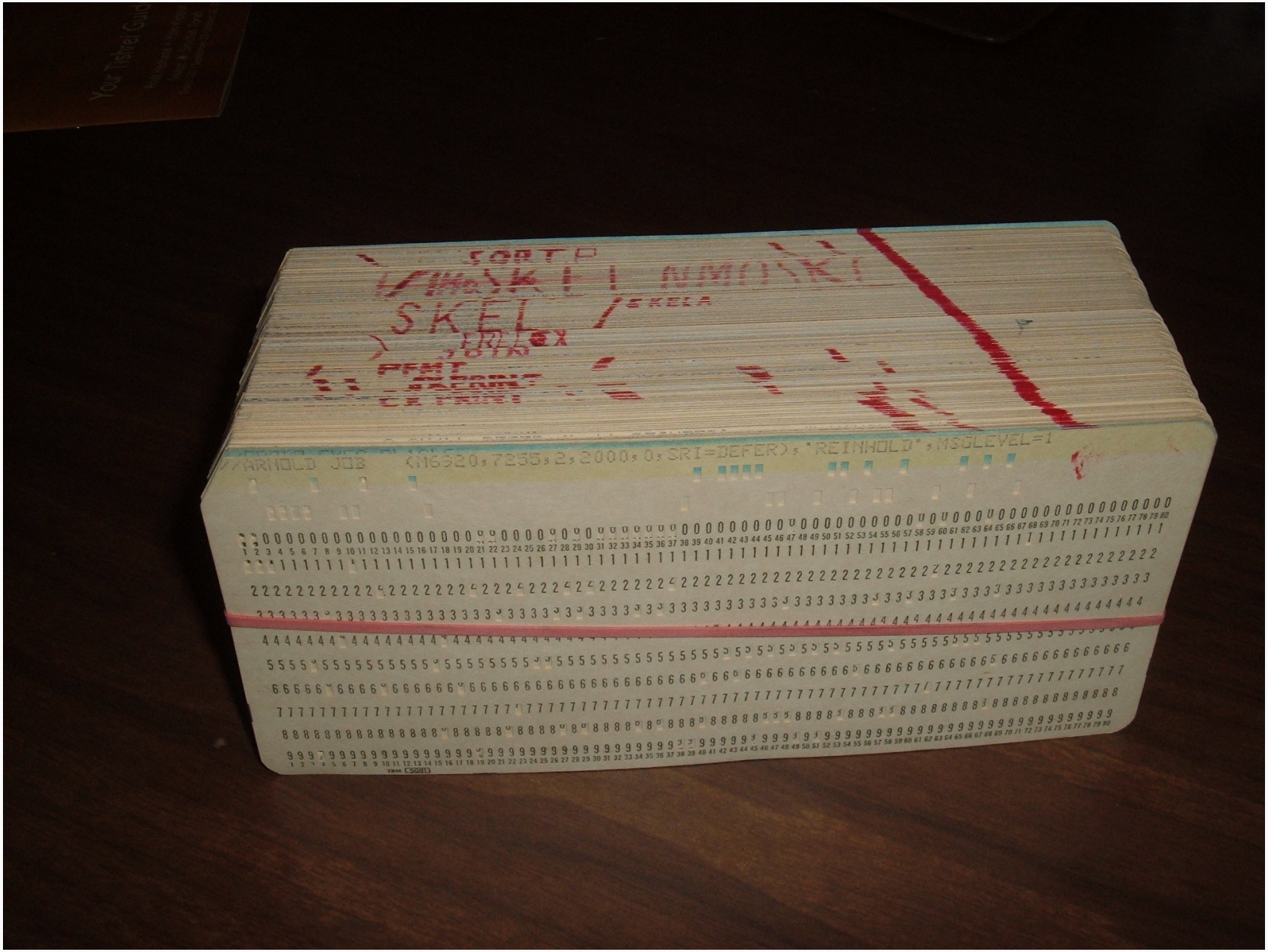
History of debuggers

Single user machines

- One of the first computers in the world
- Small application was loaded at the top of the memory
  - single step
  - examine registers
  - read/write memory

TX-0 at MIT

Batch processing machines



Batch processing machines

Debugged by putting macro call in the punch card and generating:

- Snapshots *(register dump)*
- Core dumps *(contents of memory)*

printf

Then came CTSS *(Compatible Time-Sharing System)*, one of the first time-sharing operating systems!

Debugging suddenly became interactive.

printf-debugging

```
*ptr = 1337;
printf("Did we crash at line %d?\n", __LINE__);
*((int *) 0) = 1337;
printf("Did we crash at line %d?\n", __LINE__);
```

Unix-es

- The first version of Unix had a debugger called, `DB`
- GNU had `GDB` and `LLDB`
- For Plan 9, `ADB` was created

These debuggers should be familiar!

Tracing processes

ptrace

Most debuggers heavily rely on a system call known as `ptrace`.

The prototype of `ptrace(2)`

```
#include <sys/ptrace.h>

long ptrace(enum __ptrace_request request, pid_t pid,
                    void *addr, void *data);
```

Signals

Signals originate from CPU exceptions..

Implementation

- Enable tracing
- Run until system call
- Monitoring registers
- Single stepping

Implementation

- Enable tracing
- Run until system call
- Monitoring registers
- Single stepping

Implementation

- Enable tracing
- Run until system call
- Monitoring registers
- Single stepping

Implementation

- Enable tracing
- Run until system call
- Monitoring registers
- Single stepping

Implementation

- Enable tracing
- Run until system call
- Monitoring registers
- Single stepping

Architectural support

Interrupting a process

`PTRACE_SYSCALL`

`PTRACE_SINGLESTEP`

Undefined instructions, debug interrupt...

Debug registers

`DR0-DR7`

Thanks!

Thank you for your attention!

Twitter: @iLevex
Email: <lkurusa@linux.com>
GitHub: levex
Website: `http://osdev.me/`

The LaTeX theme is available at `github.com/matze/mtheme`