Thread Abstraction Layer — TAL

- implementation of \{fly, feather, light\} weight threads by three components:
  - thread yard .......................................................... 2
  - thread executive ..................................................... 9
  - thread interface extension ......................................... 29

- supplementing components take care of platform-specific features:
  - central processing unit ............................................. 16
    * register access functions ...................................... 19
    * state buffering .................................................. 24
  - application binary interface ................................. 14

- development of the class hierarchy and code fragments exemplary to C++

Thread Yard — thy

- at the physical level, a thread is represented by an untyped stack pointer
  - for being able to execute, at minimum a thread needs a stack as resource
  - when suspended, the thread’s stack stores the thread’s resumption address

- at the logical level, a thread is represented by a typed (aligned) stack pointer
  - an inactive thread’s stack pointer refers to a well-defined object
  - this object captures the resumption address of the thread
  - it is automatically created when a thread suspends execution

- a class ensemble takes care of mapping the logical to the physical view

\begin{verbatim}
Thread Yard

<table>
<thead>
<tr>
<th>thyThread</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpuElope* ra</td>
</tr>
<tr>
<td>label() : thyThread*</td>
</tr>
<tr>
<td>check() : thyThread*</td>
</tr>
<tr>
<td>setup()</td>
</tr>
<tr>
<td>badge()</td>
</tr>
<tr>
<td>split()</td>
</tr>
<tr>
<td>latch()</td>
</tr>
<tr>
<td>elope() : cpuElope*</td>
</tr>
<tr>
<td>elope(cpuElope*)</td>
</tr>
</tbody>
</table>
\end{verbatim}

\footnote{In the following, static member functions are indicated by a trailing caret (\textit{i.e.}, `\^`).}
Thread Yard

- support thread instantiation by a single method:
  - labeling of the current thread’s stack
  - splitting up the current thread of control
  - returning a thread handle ($0 \rightarrow$ dad, $\neq 0 \rightarrow$ son)

- a minimal extension to thyThread aiming at improved “user friendliness”
  - compared to thyThread, this may be at the expense of performance:
    * `$spawn()` exploits a C++ `?:`-clause to generate the return value
    * in turn, exploitation of $spawn()` is, typically, part of an if-clause
    - as a consequence, a nested conditional expression needs to be evaluated

- generation of a typed stack pointer:
  1. CPU-defined alignment
     - `top()`
  2. CPU-defined stack expansion
     - `top()`
  3. user-defined type conformance
     - `new()` resp. `new[]()`

- attempts of stack-pointer deallocation by exploitation of `delete()` are trapped

Thread Yard

- description of a thread’s runtime stack
  - a user-defined number of `thyEntity` slots
- represented as a parameterized data type
  - with the number of slots as actual parameter
- manifests a `thyThread` including stack space
Thread Executive — the

- implementations of a featherweight thread
  - attribute is the thread’s context pointer
  - identifies the “scope” of the thread
  - thread shifts update the context pointer

- thread construction means binding of a thread instance to a thread context
  - the context pointer (toc^2) makes up the thread’s initial stack pointer

- thread shifting updates the binding by pointing to the saved resumption address

Thread Executive — theObject

- implementation of a lightweight thread
  - depends on stack space for context saving

- threads save/restore their context on their own
  - before/after the thread-shifting procedure

- context saving distinguishes between the abstract and concrete processor
  - grant() is for the abstract processor “compiler”
  - yield() is for the concrete processor “CPU”
Thread Executive

- the initial thread resp. “objective main()”
  - distinguishes different invocation patterns:
    * with no parameters
    * with an argument vector
    * with an environment pointer
  - provides the default entry point(s)
- introduced to support pure object-orientation
- the “genius” is automatically created by main(), with the action() left open

Application Binary Interface — abi

- the interface between application and hardware as defined by the compiler
  - particularly, it assigns to selected CPU registers a specific function
    * e.g., to employ the x86 general-purpose register “ebp” as local base
  - it specifies which compiler feature is implemented by which CPU feature
- a major aspect that has influence on a thread model is register banking:
  - volatile register set i.e. the set of those CPU registers whose contents need not be maintained across procedure calls
  - non-volatile register set i.e. the set of those CPU registers whose contents must be maintained across procedure calls
- thread-context saving may take advantage out of this “artificial” distinction

Thread Executive

Class Hierarchy

Application Binary Interface

- context save and restore
  - stack-based
  - non-volatile register set
- platform dependencies:
  - GNU gcc compilers
  - Intel x86 processors
- minimization of context-saving overhead in the light of big (RISC) register sets

```
inline void abiStack::store () {
  asm ("pushl %ebp");
  asm ("pushl %esi");
  asm ("pushl %edi");
}
```

```
inline void abiStack::clear () {
  asm ("popl %edi");
  asm ("popl %esi");
}
```
Central Processing Unit — cpu

- the processor-dependent interface to the underlying physical machine
  - defines the CPU’s register set and specific CPU control functions
  - defines register access functions (RAF) for language-level manipulations
- an instance of the respective CPU abstraction(s) exists by default
  - namely the “hardware object” that represents the actual CPU
  - creation and {con,de}struction of that object at runtime is meaningless
- some kind of “support layer” to control CPU operation by C++ programs

Central Processing Unit — cpuStack

- context save and restore
  - stack-based
  - general-purpose registers
  - dedicated instructions
- platform dependency: Intel x86 processor family (in the present case)
  - compiler dependency exists only w.r.t. the inline assembler feature
- the overhead for context save/restore may be fairly high with RISC processors
  - e.g., a PPC: 32 (32-bit) integer and 32 (64-bit) floating-pointer registers

Central Processing Unit — cpuModel (1)

- major aspect is to access a CPU register by a register access function (RAF)
  - each register is considered a class having two public operators:
    ```
    struct RAF {
        type operator = (const type); // write into CPU register
        operator type () const; // read from CPU register
    }
    ```
  - whereby type specifies the width (in bits) of the particular register
- there are as many RAF definitions as CPU registers that need to be accessible

Central Processing Unit — cpuModel x86

- Register Access Functions

```cpp
class cpuModelGPR {
    __CLASS(EDI,bits32);
    __CLASS(ESI,bits32);
    __CLASS(EBP,bits32);
    __CLASS(ESP,bits32);
    __CLASS(EBX,bits32);
    __CLASS(EDX,bits32);
    __CLASS(ECX,bits32);
    __CLASS(EAX,bits32);

    cpuModelGPR ()
    cpuModelGPR (const cpuModelGPR&);
    public:
    EDI edi;
    ESI esi;
    EBP ebp;
    ESP esp;
    EBX ebx;
    EDX edx;
    ECX ecx;
    EAX eax;
};
```

```cpp
class cpuModelSR {
    __CLASS(CS,bits16);
    __CLASS(DS,bits16);
    __CLASS(SS,bits16);
    __CLASS(ES,bits16);

    cpuModelSR ()
    cpuModelSR (const cpuModelSR&);
    public:
    CS cs;
    DS ds;
    SS ss;
    ES es;
};
```

```cpp
class cpuModelFR {
    __CLASS(Flags,bits16);

    cpuModelFR ()
    cpuModelFR (const cpuModelFR&);
    public:
    Flags flags;
};
```
# Register Access Functions

```c
#include "cpu.h"
extern int foo();

int main () {
    bits16 flags = cpu->flags;
    cpu->block();
    bits16 ds = cpu->ds;
    cpu->ds = cpu->cs;
    *(int*)foo = 0xC3;
    cpu->ds = ds;
    cpu->flags = flags;
    cpu->eax = 4711;
    return foo();
}
```

## Exploitation

```c
#include "machine/cpuModel.h"
#define cpu ((cpuModel*)42)

main:
    pushl %ebp
    movl %esp,%ebp
    pushf
    pop %cx
    cli
    mov %ds,%dx
    mov %cs,%ax
    mov %ax,%ds
    movl $195,foo__Fv
    mov %dx,%ds
    push %cx
    popf
    movl $4711,%eax
    call foo__Fv
    leave
    ret
```

## Central Processing Unit

```c
inline void cpuModel::block () {
    asm ("cli");
}
inline void cpuModel::admit () {
    asm ("sti");
}
```

## cpuModel (2)

```c
cpuModelGPR
- cpuModel()
- cpuModel(const cpuModel&)
+ block()
+ admit()
```

### cpuModelFR

```c
cpuModelFR
- cpuModelFR()
- cpuModelFR(const cpuModel FR&)
+ Flags flags
```

### cpuModelSR

```c
cpuModelSR
- cpuModelSR()
- cpuModelSR(const cpuModelSR&)
+ DS ds
+ SS ss
+ ES es
```

### cpuModelFR

```c
inline bits16 cpuModelFR::Flags::operator = (const bits16 aux) {
    aam volatile ("push 00" : "g" (aux));
    aam ("popf");
    return aux;
}
inline cpuModelFR::Flags::operator bits16 () const {
    bits16 aux;
    aam volatile ("push");
    aam volatile ("pop 00" : "g" (aux));
    return aux;
}
```
State Buffering

- buffered save/restore of a thread’s ABI state
  - RAF is used for CPU-register access
  * read/overwrite register contents
  - the state buffer is not stack-bound

- ABI-state manipulation then can be accomplished in the following way:
  1. flush the ABI state into the buffer by reading the CPU registers
  2. access selected ABI registers within the buffer
  3. apply the buffer contents to the CPU by writing to the CPU registers

```
inline void abiImage::flush () {
    cpu->edi = (*this)[ABI_EDI];
    cpu->esi = (*this)[ABI_ESI];
    cpu->ebp = (*this)[ABI_EBP];
    cpu->ebx = (*this)[ABI_EBX];
}
```

```
inline void abiImage::apply () const {
    cpu->edi = (*this)[ABI_EDI];
    cpu->esi = (*this)[ABI_ESI];
    cpu->ebp = (*this)[ABI_EBP];
    cpu->ebx = (*this)[ABI_EBX];
}
```

```
inline bits32& abiImage::operator [] (int slot) const {
    return (bits32&)gpr[slot];
}
```

State Buffering

```
inline void cpuImage::flush () {
    cpu->eax = (*this)[CPU_EAX];
    cpu->ecx = (*this)[CPU(ECX)];
    cpu->edx = (*this)[CPU_EDX];
    cpu->ebx = (*this)[CPU_EBX];
    cpu->esp = (*this)[CPU_ESP];
    cpu->ebp = (*this)[CPU_EBP];
    cpu->esi = (*this)[CPU_ESI];
    cpu->edi = (*this)[CPU_EDI];
}
```

```
inline void cpuImage::apply () const {
    cpu->edi = (*this)[CPU_EDI];
    cpu->esi = (*this)[CPU_ESI];
    cpu->ebp = (*this)[CPU_EBP];
    cpu->esp = (*this)[CPU_ESP];
    cpu->ebx = (*this)[CPU_EBX];
    cpu->edx = (*this)[CPU_EDX];
    cpu->ecx = (*this)[CPU_ECX];
    cpu->eax = (*this)[CPU_EAX];
}
```

```
inline bits32& cpuImage::operator [] (int slot) const {
    #ifdef hackOperatorSubscription
        return ((bits32*)this)[slot];
    #else
        return (slot < ABI_NGPR) ? (*((abiImage*)this))[slot] : ((bits32*)gpr)[slot - ABI_NGPR];
    #endif
}
```
State Buffering

```c
void foobar () {
    cpuImage foo;
    foo.flush();
}
```

cpuImage (2)

```c
void foobar () {
    cpuImage bar;
    bar = foo;
    bar.apply();
}
```

Thread Interface Extension

- **pointer to parametrized function**
  - parameter is the function’s thread
  - i.e., a `tieThing`
  - an “objectless” function otherwise

- **ordinary C functions become threads:**
  ```c
  void gadget (tieThing* self) {
    self->grant(...);
  }
  ```

- **member functions of derived (single-inheritance path) classes may work also**
  ```c
  T* self;
  self->grant(...);
  ```

  *This is a “hack”, absolutely dirty, not recommendable—yet efficient, but it depends on the C++ compiler.

Thread Interface Extension — *tie*

- logical separation of the thread abstraction(s) from the user abstraction(s)
  - encapsulation of thread instantiation and activation by a single method

- different ways of interfacing are provided by different (minimal) extensions to make the user thread a
  ```c
  / { pointer to parametrized function
  \  virtual default
  / pointer to member function
  /  ` TieObject`
  \  any method of a user-defined class
  / C++ methods become threads:
  \  ```c
  void T::entry (T* self) {
    self->grant(this->next);
  }
  ```

  *kind of delegation, with member-function execution by its own private thread

thread Joint
**Thread Interface Extension**

- **virtual function** (i.e., late binding)
  - redefined methods become threads
    
    ```cpp
    virtual function (i.e., late binding)
    void Foo::action () {
        grant(this->next);
    }
    ```
  
  - a user thread is considered the final specialization of the system’s abstraction(s)
    - it extends the system thread by user-defined attributes and methods
  
  - the price to be paid is the presence of (at least) two virtual-function tables

**Thread Interface Extension**

- **default function**
  - member of a user-defined class
    
    ```cpp
    default function
    void T::action () {
        this->self->grant(next);
    }
    ```

  - the (minimal) system extension supports the *inlining* of the member function
    - depending on the function’s specification/implementation—and the compiler
  
  - clients benefit from all (public) features of the system and user abstraction(s)