Security-oriented languages provide programmers with high level abstractions such as built-in notions of principals and digital certificates. Providing language-support for these abstractions means that program analyses, done statically by the compiler before the program is run, can detect many security errors. These constructs also provide a way for programmers to document the security policy intended for the system.

**Approach and Impact**

**New approach**
- Combine information-flow analysis with cryptographic enforcement.
- Dependently typed policies
- Unified authorization logic with multilevel security constraints

**Research Impact**
- Novel language constructs for building secure systems
- Proven soundness properties
- Prototype language implementations

**Example code from an example File System sample application written in Aura:**

```
let ownerPolicy : (pf (self says ((o:Prin) -> (r:Prin) -> (p:Prin) -> (f:FileHandle) -> (soinfo : (f:FileHandle) -> Prop) -> Prop)) -> (OwnerInfo f) =
  assert OKToRead : FileHandle -> Prop;
  assert MayRead : Prin -> FileHandle -> Prop;
  assert Owns : Prin -> FileHandle -> Prop;

let anonPolicy : (pf (self says (MayRead r f | soinfo : (f:FileHandle) -> Prop) -> Prop)) -> Prop =
  assert OKToRead : FileHandle -> Prop;
  assert MayRead : Prin -> FileHandle -> Prop;
  assert Owns : Prin -> FileHandle -> Prop;
```

**Representative Publications:**
- A Cryptographic Decentralized Label Model • Oakland 2007
- Preserving Sevcy Under Refinement • ICALP 2006
- Enforcing Robust Declassification and Qualified Robustness • JCS 2006
- Encoding Information Flow in Haskell • CSFW 2006
- Unifying Confidentiality and Integrity in Downgrading Policies • FCS 2005
- Designing a Security-typed Language with Certificate-based Declassification • ESOP 2005
- Information-flow Control in Web-based Information Systems • CSFW 2005
- Downgrading Policies and Relaxed Noninterference • POPL 2005

**SOL Project Participants:**
- Steve Zdancewic, Assistant Professor (PI)
- Limin Jia, Ph.D. student
- Peng Li, Ph.D. student
- Karl Mauzarak, Ph.D. student
- Stephen Tse, Ph.D. student (Graduated 2007)
- Jeff Vaughan, Ph.D. student
- Jianzhou Zhao, Ph.D. student
- Limin Jia, Undergraduate student
- Joseph Schor, Undergraduate student