Kestrel Institute, Kestrel Technology Inc.

- Kestrel Institute: non-profit research
  - research & technology for software
    - specification, analysis, refinement & generation
  - high-assurance systems
  - software engineering productivity
  - high-performance software
  - contact: www.kestrel.edu, 650-493-6871
- Kestrel Technology Inc.
  - supporting high-assurance software throughout its lifecycle
  - government and commercial customers
  - top secret clearances
  - contact: www.kestrel-technology.com, 650-320-8888

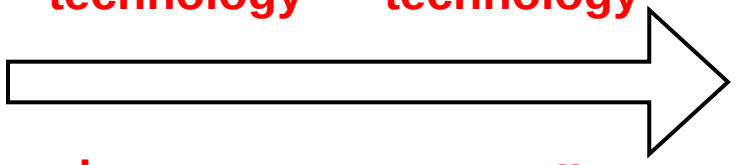
Effective Modeling Technology

Technology for DSLs

Languages for expressing problems in a domain
e.g., specification of a software application

Languages for expressing solution techniques
e.g., generic algorithms, data types

Languages for expressing deployment environment
e.g., operating system, data profiles



reasoning technology

analysis technology

language transformation technology

compiler technology

Analysis tools
e.g., flaw finder

Problem solvers
e.g., executable code

Documentation
e.g., proof of code correctness

syntax & semantics

reusable across domains

optimized to domain, environment

Kestrel Institute • www.kestrel.edu • 650-493-6871
3260 Hillview Avenue, Palo Alto, California 94304 • mcdonald@kestrel.edu, fitzpatrick@kestrel.edu

Successful Application: Java/JavaCard

Java byte code semantics

Specification of Java byte code verifier

Specification of security characteristics for networked applications

Compact DSL for Java smart cards

Specification of JavaCard runtime environment

analyzer

verifier
translator

Security analysis of specification and reference implementation

Security analyses regarding untrusted input data

Type safety analyses
Java code for cards
Proofs of code correctness

FIPS Certification (future)

Kestrel Institute • www.kestrel.edu • 650-493-6871
3260 Hillview Avenue, Palo Alto, California 94304 • mcdonald@kestrel.edu, fitzpatrick@kestrel.edu

Successful Application: Communication Protocols

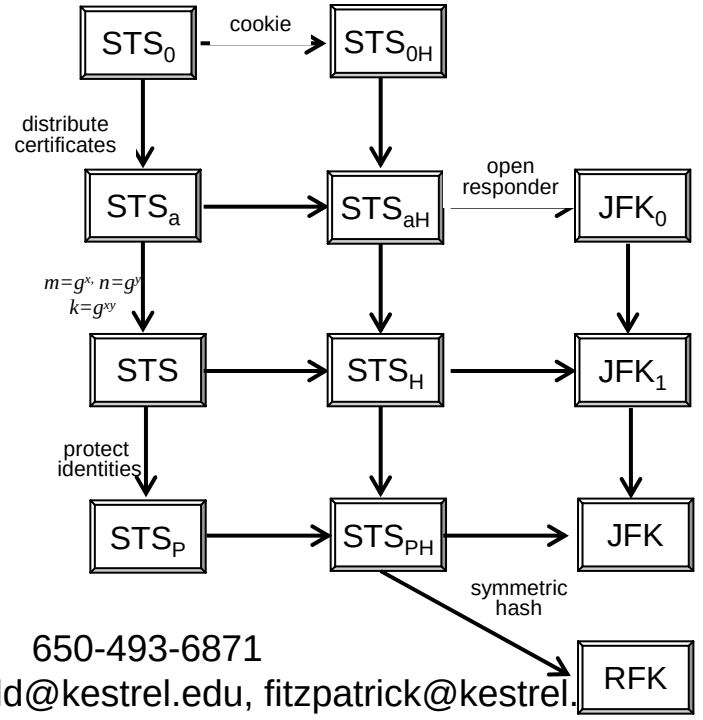
DSL for comm. protocols

Models of protocols — **code generator** — **executable code**

Models of protocol families — **protocol derivation tool** — **discovery of new protocols**

Model protocol attacks — **analyzer** — **discovery of security flaws**

Specification of separation kernel for AIM chip supported security endorsement



Kestrel Institute • www.kestrel.edu • 650-493-6871
3260 Hillview Avenue, Palo Alto, California 94304 • mcdonald@kestrel.edu, fitzpatrick@kestrel.

Other Areas of Expertise

Planning & Scheduling

- Resource & task modeling
- Algorithm specification
- Code generation & optimization
- Orders-of-magnitude code speed-up
- Vastly reduced cost for evolution

Coordination in Scalable Networks

- Application modeling as distributed constraint problems
- Truly scalable, anytime algorithms for distributed constraint optimization

Model-based Code Generation for Embedded Controllers

- Semantics for standard modeling languages
- Generate compilers (to C) based on semantics
- High-quality C code, 10x fewer errors

Kestrel Institute • www.kestrel.edu • 650-493-6871
3260 Hillview Avenue, Palo Alto, California 94304 • mcdonald@kestrel.edu, fitzpatrick@kestrel.edu