Trustworthy Commodity Computation and Communication
Enables dynamic, "transient trust" security policies for achieving the appropriate availability of highly sensitive information during emergencies in the face of determined adversaries.

- Research goal: Worked example of architectural foundation for trustworthy commodity mobile devices
  - Multi-use, multi-context operations
- Approach: Clean-slate, HW/SW co-design
  - Clean-slate design allows “break-through” ideas
  - Secure-by-design architecture via tight integration
- Design goal: Security with performance, low cost and usability
  - New least privilege separation-kernel and trusted services software to enforce MAC and securely manage resources

Accomplishments
- Concept of operation
  - Multilevel-secure (MLS) multi-use handheld device
  - Different functional contexts correspond to different user roles:
    - Everyday and emergency
    - Normal or trusted
  - Support inter-context secure sharing of information
- Trustworthy security architecture that can support dynamic security policies and services
  - Core building blocks
    - Security-aware processor extensions
    - Least privilege separation kernel
    - Trusted security services
    - Secure operating-system services
    - Trusted path application

SecureCore Software Architecture
<table>
<thead>
<tr>
<th>Layer</th>
<th>Functions and Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPA</td>
<td>Trusted Path interface to security-critical services</td>
</tr>
<tr>
<td>SecureCore Operating System</td>
<td>Application Management, Identification and Authentication, Operating System Services</td>
</tr>
<tr>
<td>SecureCore Security Services</td>
<td>MLS Support and Interpretation, Resource Virtualization, Object Management, Focus Management, Trusted Channel Management, Inter-Partition Flooding</td>
</tr>
<tr>
<td>LPSK</td>
<td>Partitioning of Resources, Resource Management, IAC Enforcement, Partitioning Scheduling, Cross-Partition and Inter-Process Communication</td>
</tr>
</tbody>
</table>

Concept of Operation
- Normal Data
  - Multi-use
  - Identification
- Fast Responder Data
  - Focus
  - Emergency
- Medical Data
  - Review
  - Authorize
- Government Data
  - Private
  - Authorized

SecureCore Hardware Architecture
- User-mode: enables controlled and secure access to user's secrets
- Authority mode: enables transient, policy-controlled access to third-party protected information, remotely
- Reduced mode: for use in low power applications

Contributing Members
(alphabetically ordered)
- Ganesha Bhaskara*
- Paul Clark*
- Timothy Levin*
- Thuy Nguyen*
- Mark Orwat*
- David Shifflett*
- Timothy Vidas*