Remote and Transient Trust: Emergency Response

Secure Cache Architecture
- Problem: Information leak via software cache-based side channel attacks
- Our solution: Random Permutation cache (RP-Cache) randomly swaps cache lines on a cache miss so processes see different memory to cache mappings
- Hardware solution solves root of problem
- Applies to legacy software and future attacks
- No increase in cache access time with clever circuits
- Negligible performance degradation
- New work: improve performance and fault-tolerance and power consumption, in addition to security!

TEC-tree Memory Authentication
- Problem: Memory subject to spoofing, splicing and replay attacks (hardest)
- Our solution: Tamper-Evident Counter tree
- Can be parallelized check and update
- Confidentiality for free
- Block encryption with added redundancy
- Fast detection of spoofing and splicing attacks after 1st level tree check
- Detects replay attacks
- New work: from embedded systems to general purpose systems

Accomplishments:
- Emergency response with transient trust
- Secret Protecting (SP) architecture for security-aware processors
- New authority-mode and sensor-mode
- Trusted Path Application and Emergency Partition
- SecureCore Prototype with SP emulation
- New cache architectures that are immune from software side-channel attacks
- Integrated memory authentication
- Secure key management in sensor-nets
- Security metrics for networking protocols