SAFE & SOUND:
Clean Slate Host and Network Architectures for Secure, Resilient Computing in a Hostile Environment

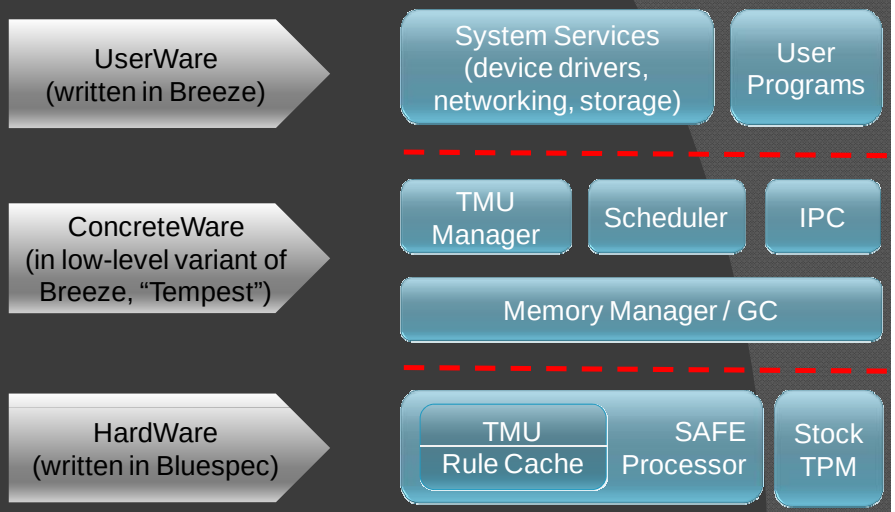
For Layered Assurance Workshop Panel,
The Future of Highly Trustworthy Systems, Networks, Apps, and Clouds
December 5, 2011, Orlando FL
Presenter: Greg Sullivan (BAE Systems)

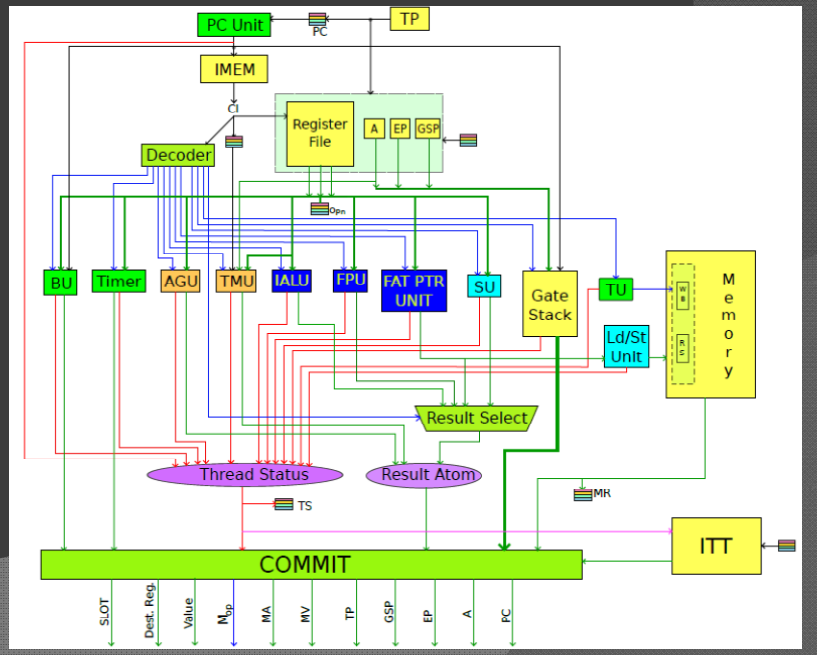
CRASH SAFE Project

BAE SYSTEMS

Penn

- Fine-Grained, Secure Checking
  - All data tagged, with arbitrarily complex metadata
  - Every operation runs Tag Rules against all tags involved
  - ⇨ Tag of result and of PC
- "Concreteware" is proven correct
  - Including compiler for Breeze Programming Language
- "Zero Kernel" OS made up of least privilege, mutually suspicious components.
- Protection in Depth: Multiple layers of protection.

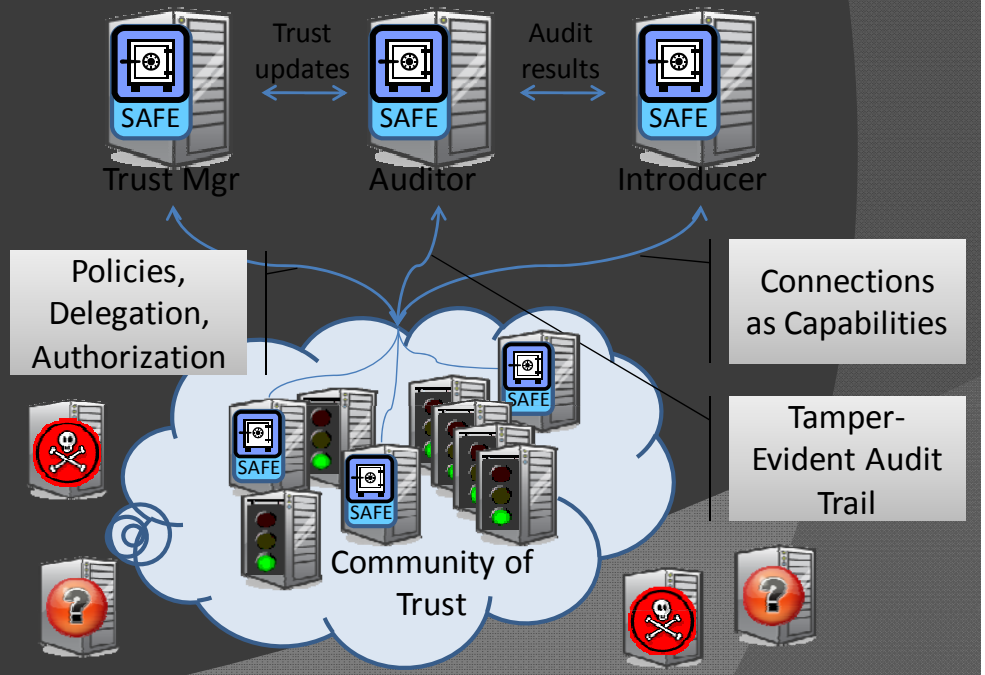




MRC SOUND Project

BAE SYSTEMS
Portland State UNIVERSITY
Penn University of Pennsylvania

- **Communities of Trust** establish Collective Immunity built upon:
  - **Quantitative Dynamic Trust Management** - A distributed architecture for specifying and maintaining context-sensitive policies for delegation and authorization.
  - **Introduction-Based Routing** – a distributed mechanism for dynamically adapting trust based on feedback from performance and audit.
- **Transparent Accountability** for Dynamically Verifying Behavior.
- **Formal methods & languages** – for verified implementations of core components.
- **Extension & Use of SAFE** technology – from the CRASH project, is basis for system-wide public health infrastructure.



SAFE & SOUND

BAE SYSTEMS

Portland State UNIVERSITY

Penn

- CRASH SAFE: Clean Slate Tagged Architecture + Secure Programming Language + Zero Kernel OS + Formally Proven Correct Components.
  - Dedicate silicon and processing to security, from the beginning.
- MRC SOUND: Inject secure hosts into a heterogeneous distributed system to globally increase security and resilience.
  - Peer-to-peer reputation management via Introduction-Based Routing.
  - Accountability based on tamper-proof audit trails.
  - Foundation of trust using CRASH technologies.

The Future of Highly Trustworthy Systems

- Hardware and cycles dedicated to security:
  - Data path includes metadata (tags, audit, information flow, capabilities).
  - Compute path includes monitoring, audit, redundancy, n-version, sampling, tag-based checking, …
  - Repair, Recovery, Adaptation, Planning.
- Formal methods as a Basis for Trust
  - Logical Security, along with Physical Security.
  - TPMs for everything.
- Trust is not absolute. Social Networks a close analogue to Networks of Trust.
  - Trust is constantly evolving, being re-evaluated, based on multiple sources, …