



# Scalable Trusted Computing

Peter A. Loscocco

[loscocco@tycho.nsa.gov](mailto:loscocco@tycho.nsa.gov)

National Security Agency

National Information Assurance Research  
Laboratory (NIARL)



# Focus of Presentation



- Ideas about the meaning of STC
  - Some observations
  - Some design considerations
  - Some problems that need to be addressed
  - Some conclusions



# Trusted Computing



- Different notions of trusted computing
  - Traditional notions of a trusted system
    - Can a system be trusted for some purpose?
  - Establishing trusted relationships on the network
    - Who is really on the other side of the connection?
    - What is really running on the other side of that connection?



# Observation

- Although ideas are different, they are closely related
  - Establishing and maintaining trusted relationships requires placing trust in system components
  - Security architecture, feature sets, and implementation choices ultimately determine trustworthiness of system components
- Shouldn't be talking about one without the other



# Trusted System Design



- Designing trusted systems requires an understanding of the trust relationships between every system component
  - How is trust established between each pair?
  - What must be trusted about each peer?
- Trust analysis of components requires following chains of trust back to all service providers
  - Failure creates potential for unwarranted trust



# Traditional Trust

- Correctness of implementation
- Correctness of design
  - Proper feature set
    - MAC/trusted path/protected path
  - Good security design principles
    - Least privilege, separating policy from enforcement, etc.
  - Proper reliance on other components/systems
    - Are trust assumptions being met?
- Must show for each component and entire system



# Trust Argument

- System wide security objectives
  - Showing satisfactory design
- Trustworthiness of components
  - Proving correctness
- Establishing initial trust
  - Must show secure initial state can be reached
- Maintaining trust
  - Must show only secure state transitions possible



# Validating Trust Assumptions



- Security mechanisms rely on implicit assumptions
  - Must make assumptions explicit
- Must validate assumptions
  - Code and Data Integrity/Confidentiality
  - Nonbypassability
  - Input and Interfaces
  - Environmental
- Threat assessment impacts tolerance of unproven assumptions
- Trust in system rests on correct analysis



# New Trust Emphasis



- Know something about networked machines
  - Condition of data access/sharing
  - Access control includes questions of trust
    - Joining enterprise networks
  - Continued network operation
    - Integrity Monitoring
- Questions of trust answered by showing “expectedness” of system



# Showing Expectedness



- Stages of process
  - Establishing a root of trust
  - Evidence collection through measurement process
  - Evidence presentation through attestation protocols
  - Evidence appraisal to support a decision process
- New trust notions rest totally in the ability to trust the process



# Properties in Support of Trust



- Measurement Properties
  - Completeness: Degree complete running state of target is reflected in measurement data
  - Freshness: How recent is measurement data
- Attestation properties
  - Authenticity: Ability to guarantee authenticity of evidence to decision process
  - Semantic Explicitness: Delivering appropriate evidence to a decision process



## Properties (Cont.)



- System properties
  - Protection: System must protect the components to enable them to meet trust obligations
- Implementation properties
  - Correctness: Sound design and correct implementation



# Observation

- Properties are a measure of ability to establish trust
  - Completeness, Freshness and Semantic Explicitness -> possibility of better trust decisions
  - Authenticity, Protection, Correctness -> ability to trust evidence
- Building a trusted computing platform requires adequately meeting requirement for these properties
- Appraisal process should consider trustworthiness



# Trusting Updated Trust



- Traditional trust required for guarantees
  - Protected execution environments
    - Safe place to stand for measurement
      - Measurement process and data storage
    - Protocol execution
    - Access control over protected resources
  - Protected communications
    - Authenticated channels between components
  - Correctness
    - Attestation protocols



# Scalability

- Ability to project trust relationships anywhere on the network
- Ability to adapt to changing and differing notions of trust
  - One size does not fit all
    - Different requirements for evidence
    - Different requirements for mechanisms
- Ability to project trust across administrative domains
  - Need to understand peer capabilities and requirements



# Properties in Support of Scalability



- Flexibility
  - Need mechanisms that meet requirements of different administrative domains
    - Need ability to support multiple mechanisms
  - Need mechanisms that can support variable evidence
    - Need support for privacy
- Usability
  - System measurement data should be presentable in whatever form is necessary to make sense in the context of a specific decision



# Observation

- Scalability introduces complexity
  - Need to support different measurement techniques
    - Can't expect only one kind of evidence
    - Degree of flexibility determined by deployment
  - Need to support different attestation protocols
    - Support for different appraisal capabilities
    - Enable specialized trusted third parties
  - Need to support automatic discovery and/or negotiation
    - Should tie into a selection service
  - Need infrastructure to enable evolving mechanisms
    - Should allow registration of new mechanisms



# Observation

- Scalability magnifies need to prove trustworthiness of trust infrastructure
  - Need mechanisms to measure and attest to all components relevant to trust decisions
    - OS, Hypervisors, support domains
    - Measurement and attestation mechanisms
      - Must be able to break recursive chain
      - Likely will require new hardware support
  - Need solid understanding of reliability of attestations
    - Was evidence reliably collected?
    - Does evidence really provide necessary proof?



# Observation

- Complexity/flexibility increases dependency on traditional trust
  - Need confidence in correctness of design
  - Need policy enforcement support to ensure proper mechanisms
  - Varying degrees of trust in different mechanisms need isolation



# Strategy for building Prototype STC



- Utilize existing technology
  - Push envelope to increase trust through architecture
  - Understand how pieces fit to make a STC
  - Build something more trustworthy than its parts
    - Limit what components need to be trusted for
- Ensure architecture can lead to a general solution.
  - Flexibility of measurement and attestation
  - Transparent platform service
- Don't give up on trusted implementation technology



# Existing Technology for STC Platform



- Technology largely in place for functionality
  - TPMs and support for dynamic root of trust
    - VTPM implementations
  - Hypervisors supporting functional operating systems
  - Technology for boot and runtime measurements
  - Attestation protocols with selection mechanism
- Needs assembly into STC with desired properties
  - Work towards missing features in existing pieces
  - Create missing infrastructure pieces



# Features to Support Trust



- Hypervisor as secure base
  - Features to support security
    - Ability to enforce MAC policy
    - Control plane security
    - Authenticated inter-VM communication channels even for untrusted domains
    - Lightweight Domains
  - Work progressing with Xen
    - XSM/Flask, Secure IVC, HalVM
    - Decomposition of Dom0
      - Isolated Domain building and Xen Store
      - Support for platform storage and VTPMs



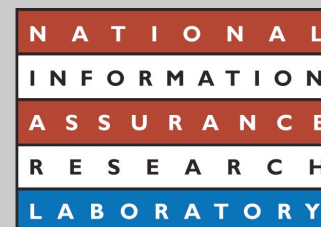
# Features to Support Trust (Cont.)



- Secure booting with DRTM and TPM support
  - Measured launch of all components
  - Attestation of all components to ensure secure initial state
- OS security features in domains
  - SELinux for Dom0 and complex critical domains
- Measurement and attestation from isolated domain
  - Limit privileges needed for measurement
  - Protection of mechanisms and data



# Total Platform Measurement



- Need total picture for trust decisions
- Layers of measurements
  - Critical Applications
  - OS and system functions within a VM
  - Critical support domains
  - Measurement and attestation domain
  - Hypervisor
- Should support M&A properties across all levels



# M&A Mechanisms

- User-space measurement
  - Special purpose functions protected by OS
  - OS support for privileged functions (e.g. LIM)
- VM M&A isolated in specialized VM(s)
  - Support for flexible mechanisms
    - Specialized measurement agents (e.g. LKIM)
    - Support for registration and selection
    - Attestation protocols independent of evidence
    - Support for negotiation of protocol and evidence
  - Policy enforcement (i.e. privacy, protection in VM)



# M&A Mechanisms (Cont.)



- Measuring M&A VM as a special case
  - Complex M&A VM requires separate measurement
  - Capability measureable by a hash to break chain
- Hypervisor Measurement
  - Static measurements at boot
  - Capability to provide runtime measurements (e.g. XHIM)



# Measurement Problems



- How are measurements from various layers used in attestations?
- How do we properly use TPMs in layered architecture?
  - Are we getting the trust we think?
- How is M&A best integrated transparently?
- From where are hypervisor and M&A measurements done?
  - Specialized HW support



# Conclusions

- Design systems with trust as holistic property
  - Increase trust through good security architecture
  - Work towards trust beyond expectedness
- Design systems that meet general purpose needs
  - Flexibility of mechanism and policy
  - Much of needed technology exists
- Interesting work remains
  - Kernel supported measurement of user-space
  - Trust relationships and conveying notions of trust
  - Negotiation of attestation protocols and evidence



# Questions?

Peter A. Loscocco

[loscocco@tycho.nsa.gov](mailto:loscocco@tycho.nsa.gov)

National Security Agency

National Information Assurance Research  
Laboratory (NIARL)