**Linux Security**

**Modules Verification**

- **Complete Mediation**: Ensure all security-sensitive operations are mediated.
- **Complete Authorization**: Ensure that authorizations are consistently applied.

---

**Computing Goals and Contributions**

**Mandatory Access Control in Xen-Linux Systems**

**Professor Trent Jaeger**

- **Joint work with IBM Research**

- **Protected Path Computing**
  - Unforgeable connection
  - Mutual authentication

**Contribution Areas**

- **Reference Monitors**
  - Linux Security Modules verification; Xen reference monitor design
- **Integration with Network Security Protocols**
  - LSM-IPSec network access control; Xen protected path
- **Policy Design and Analysis**
  - Goal-based policy design; Information flow-based policy analysis
- **System Attestation**
  - Hardware-based Integrity measurement; Information flow measurement

---

**Problem:**

- Enforce system security goals
- Leverage emerging security mechanisms
- Provide basis for depending on system integrity

**Challenges:**

- Goals are ill-defined; difficult to achieve in current systems
- Hypervisors provide resource partitions; LSM provides MAC in Linux; etc.
- Remote parties may be compromised; System/policies are mutable

---

**Integration with Network Security Protocols**

- **LSM-IPSec**
  - Per-packet Access Control for Linux
  - Label IPSec Security Associations to enable network control
  - **Clark-Wilson Lite**
    - Low Integrity Data Filtering
    - Allow only low integrity data processing via known filters
  - **Gokyo Policy Analysis**
    - Information Flow Integrity Conflict Identification
    - Finds permission assignments that result in low integrity reads

---

**Define Security Goal**

- **Protect Integrity of Application**
  - **Enforce Security Policy**
    - In Linux UserVM via LSM and SELinux policy
    - In Xen via isolation and coalition policy