

***A Security Architecture Based on Trust Management for  
Pervasive Computing Systems***

***Lalana Kagal, Jeffrey Undercoffer,  
Filip Perich, Anupam Joshi, Tim Finin***

***Computer Science and Electrical  
Engineering Department***

***University of Baltimore County***

## *INTRODUCTION*

- Ordinary Computing and Pervasive Computing!
- What is pervasive computing?
- Solution based on distributed trust management – create security policies, assign credentials, revoking it and even reasoning them.
- Solution complements PKI and RBAC.
- Smart Spaces – NIST Sponsored Project.
- Many other attempts were already made but none used distributed trust as a way to secure the system and the policies.
- Attempts : 1. Smart Homes by Unisys ( uses WAP and PDA ), 2. Centaurus infrastructure system, 3. UCB's Ninja and its problem 4. Policy Maker
- The proposed solution drew good points from all the above systems and uses PKI to enforce policies and security features.

- Policy in this context contains what? Or what exactly does it mean about rules and rights?
- What do they actually propose or what does it have?
- Vigil is the proposed system.
- Can be used in wireless and wired – main point is that security has to be dynamic.
- Vigil uses PKI and RBAC – but not totally like RBAC which uses only role heirarchies. Uses its own set of properties and constraints expressed in a XML based language.  
There are six components : Service Manager, Communication Manager, Certificate, Controller, Security Agent, Role Assignment Manager, and Clients (users and services).
- Service Manager – broker between clients and services.
- Communication Manager – communication gateway between the service managers and the different spaces.