

*NSF Workshop on Assurable and Usable Security  
Configuration*



## **Community Based Trust Establishment and Provisioning for Distributed Networks**

Hong Li, Rita Wouhaybi, and Carlton Ashley  
Intel Corporation



Intel Information Technology

# Presentation Outline

- Problem Statement, Business Value and Challenges
- High Level Overview
- Architecture/Design
- Research Approach
- Summary
- Q&A

# Problem Statement

- Mobility, ad hoc, and unmanaged networks brought by new collaboration and compute models have made device introduction, device-to-device authentication, and access control into problems requiring urgent solutions
- Issues and challenges with existing trust models
  - Centralized scheme, e.g., PKI
    - Relying on infrastructure availability
  - Web of trust, e.g., PGP
    - Simple web of trust based on individual endorsement
    - No weight information
    - Man-in-the-middle (MIM) attacks
  - Both are certificate verification method for authentication, not scalable for trust decisions

# What's Needed

- Infrastructure independence
- Trust based on both individual network nodes and communities
- Differentiated trust levels based on the community references (vouchers)
- Inclusion of conflicting endorsement resolution
- Adaptive, self-monitoring and self-provisioning
- More effective against MIM attacks
- Micro and macro trust: multi-dimensional trust associations (application, device, user, etc.)
- Enterprise litmus test, will this approach work?

# Why Is This Important to Enterprise IT?

- Emerging business trends call for new trust models to enable assurable and usable security configuration
  - Cloud computing: *“trust in the cloud”*
  - Web 2.0/3.0, social networks: *“trust in the communities”*
  - Mobile internet, wireless mesh networks: *“ad-hoc trust”*
  - Internet substitution blurring the infrastructure boundaries: *“trust in the Internet”*
  - New client compute models: *“trust in the VM’s”*
- We are not proposing a silver bullet, rather
  - It’ll be a small game changing step for enterprise IT departments to make the “right hand turn”
- Supports a default deny trust model enterprise IT security likes and the self management business wants.

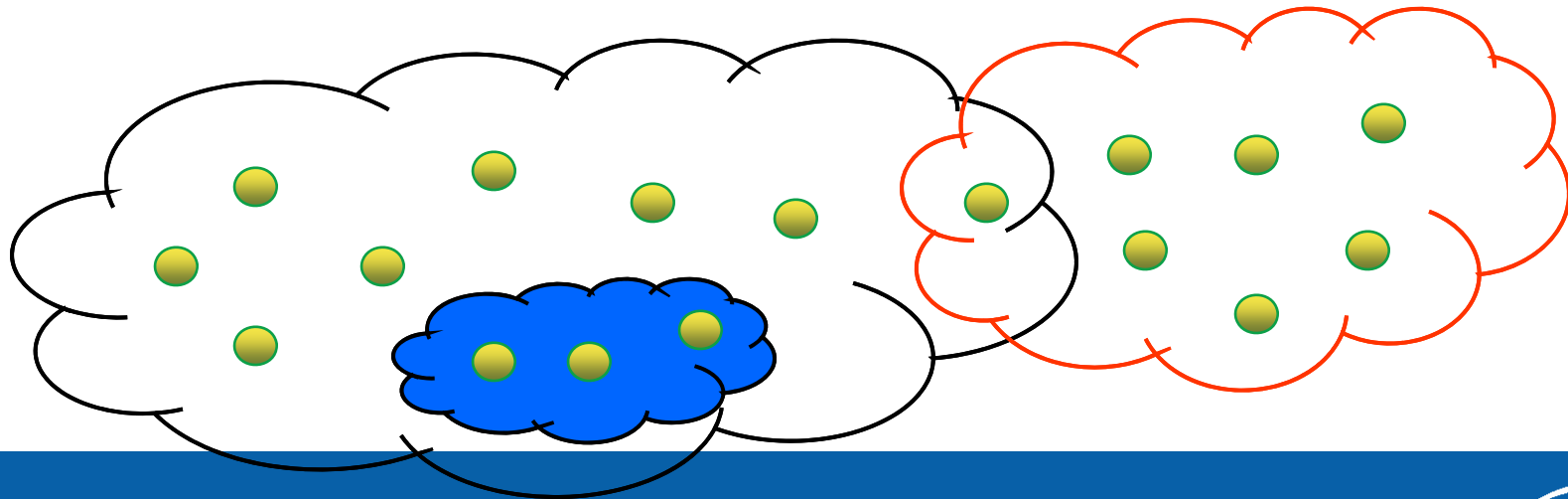
# Related Project

- Emerging research works seen in trust models for non-infrastructure based networks. For example:
  - Davis Social Links (DSL): UC Davis, Felix Wu *et al.*
  - Efficient Proving for Practical Distributed Access-Control Systems: University of North Carolina, Michael Reiter *et al.*
- How is our approach different from existing works?
  - Novel trust algorithm based on community vouchers
  - Ability to handle different trust levels
  - Ability to handle negative endorsement or mistrust
  - Self-forming, self-monitoring and self-provisioning based on social network models'

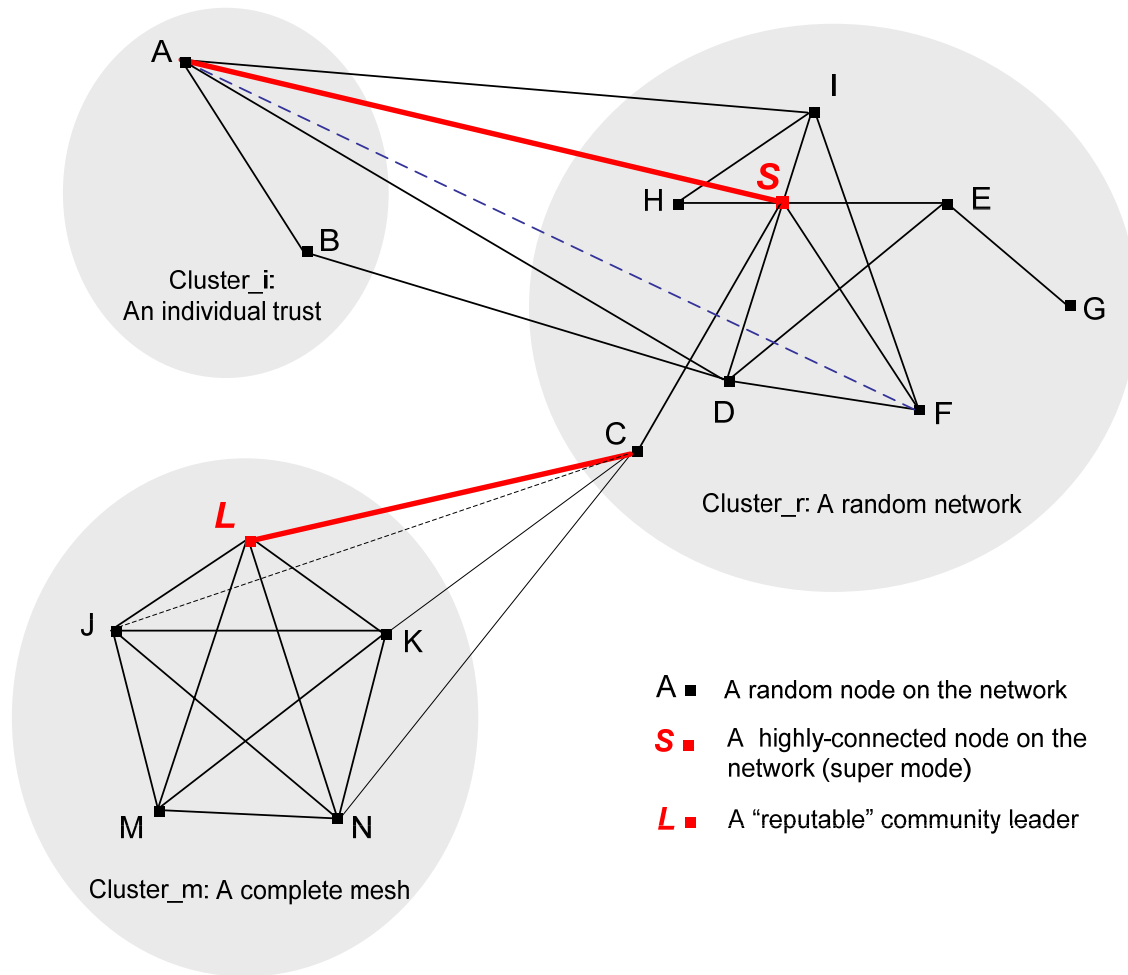
# Community Networks

- Based on common interest in a limited geographic area
- To include social introduction mechanisms
- Mix of trusted and untrusted nodes
- Maximize security ease-of-use, including setup
- Allow simultaneous participation in multiple communities
- Long-lived or ad hoc
- Targeted at both emerging and developed markets

*Ref: Meiyuan Zhao, Jesse Walker, et al, Intel Corporation*



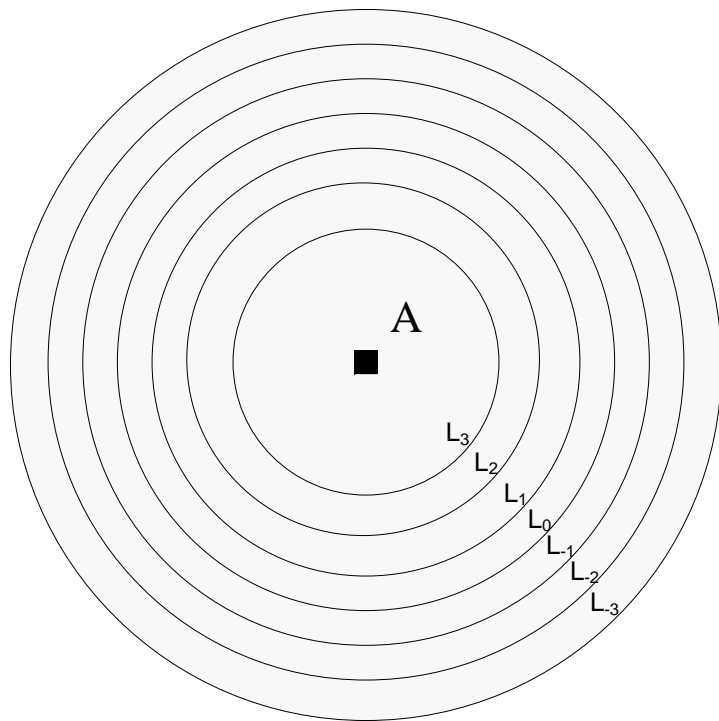
# Community Based Trust – Overview



F (in community\_r) may utilize one of the following existing trust routes as a “voucher” to gain node A’s trust (in community\_i):

- Trust between F and I (A trusts I),
- Trust between F and D (A trusts D), or
- Trust between F and S (A trusts S)
- Different vouchers carry different weights in A’s “Trust-Ring”
- Super node (S) or community leader node (L) usually carry more weight

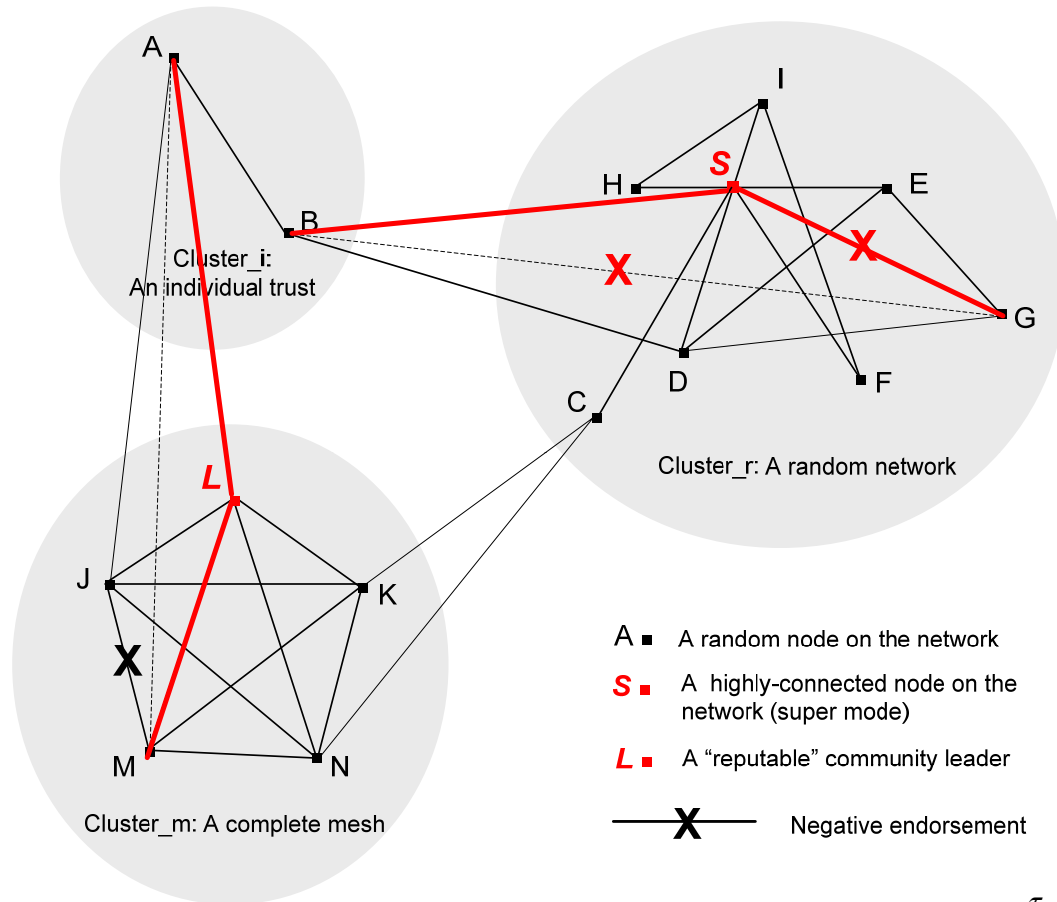
# Trust Ring for Different Degree of Trust



Trust level representation by a ring:

- A simple trust table with a list of nodes and assigned trust levels.
- Each node creates several rings around it representing its level of trust, and rank the nodes accordingly.
- The inner layers, L2 through L3, represent "trust".
- The middle L0, denotes a neutral state of neither trust nor dis-trust.
- The outer layers, L-1 through L-3, represent "dis-trust".
- A Node can be moved from one ring to another, either inward or outward, depending on the change in the relationship between the nodes.

# Negative Endorsement



- G attempts to gain trust from B
- G provides B a positive voucher from its trust relationship with D.
  - B may decide to verify with the super node S, and if S sends a negative endorsement (i.e., S distrusts G).
  - A voucher from S carries more weight, B may decide not to trust G.

- M attempts to gain trust from A
- Two conflicting vouchers are available to A from leader node L (+) and node J (-).
  - A may decide to trust M, however with a lowered trust level because of the negative endorsement from J

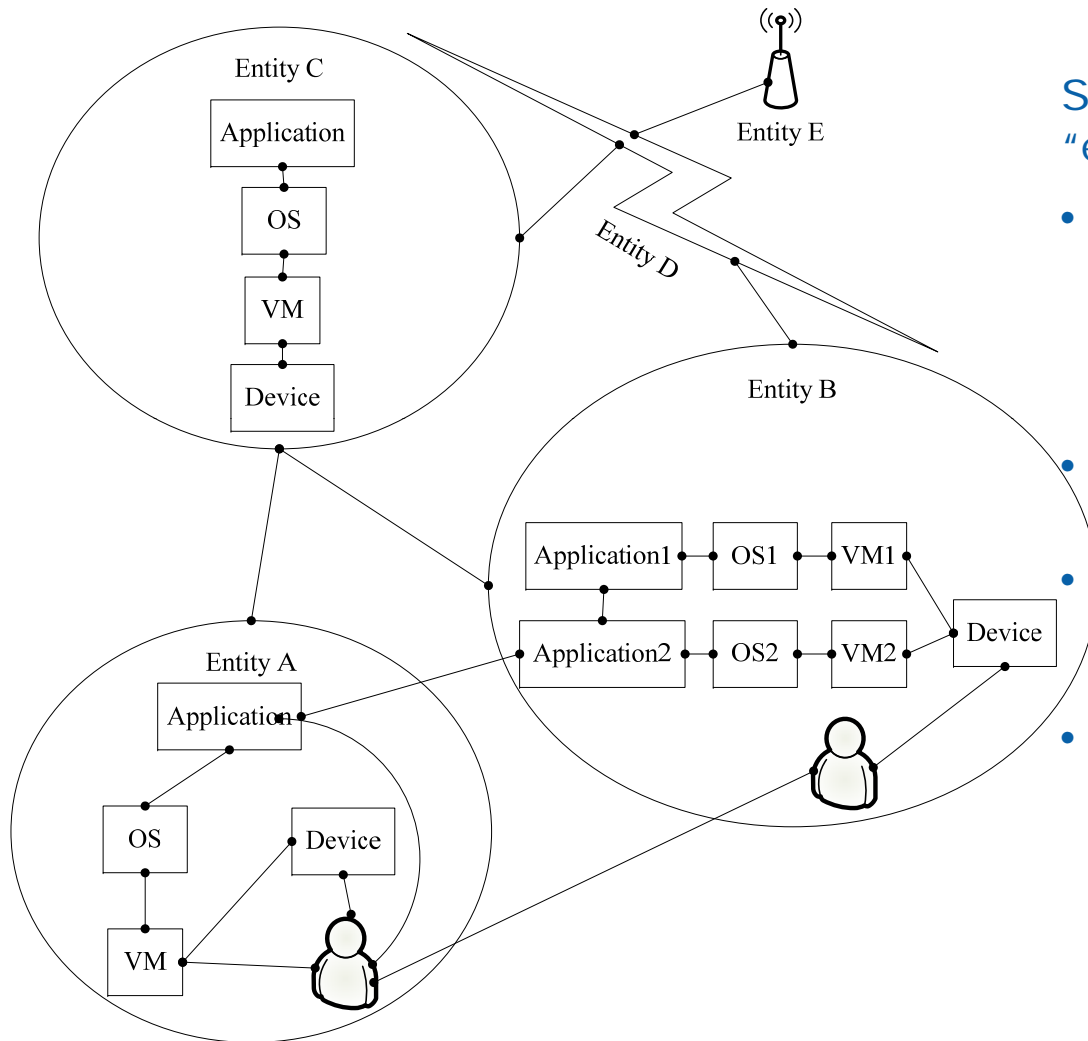
$$\tau_{ax} = \sum_{\forall pos\_rings} \alpha_r \sum_y \tau_{ay} \tau_{yx} + \sum_{\forall neg\_rings} \beta_r \sum_y \tau_{ay} \tau_{yx}$$

$\tau_{ab}$  denotes how much *a* trusts *b*,

$\tau_{ab} < 0$  denotes mis-trust

$\alpha_r$  denotes the weight associated with a trust ring *r*

# Macro and Micro Trust & Associations



Systems comprised of multiple “entities”:

- Entity A consists of a user, his/her computing device, a VM, a host OS and Applications; while Entity C represents a router and its software to forward packets over the Internet.
- A trust relationship exists between the respective components of A.
- Trust can also exist among entities such as the ones between Entities A and Entity C or Entity B and Entity C.
- In turn, the router (Entity C) trusts both Entity A and Entity B not to launch an attack by flooding its NIC with traffic.

# Summary

- A distributed trust model to enable emerging collaboration and compute models
- A small but game changing step to help enterprise IT to make a “right hand turn” in security & trust policy management
- Feasibility study using existing technologies
- Expect to see application in 2-3 years

Patent-pending concept

