

A Comprehensive Security, Privacy & Trust Management Framework for Ubiquitous Computing Environment

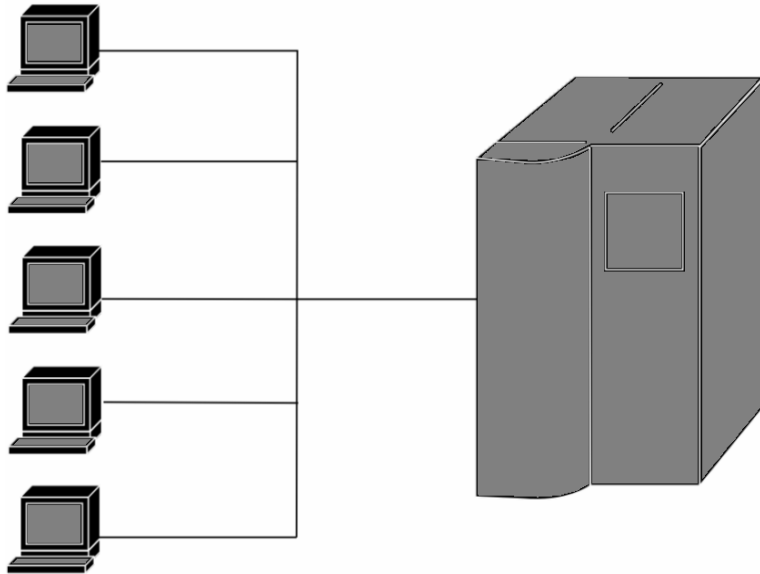
Lakshmi Eswari.P.R, Raghuram.N.C, Chaithanya.M.K,
Manjulatha.B, Jyostna.G, Sarat Chandra Babu.N
Centre for Development of Advanced Computing
(C-DAC), Hyderabad

Agenda



- Traditional Security
 - Centralized Environments
 - Networks
- Ubiquitous Computing Environments & Challenges
- Security Requirements
- Trust Management
- References

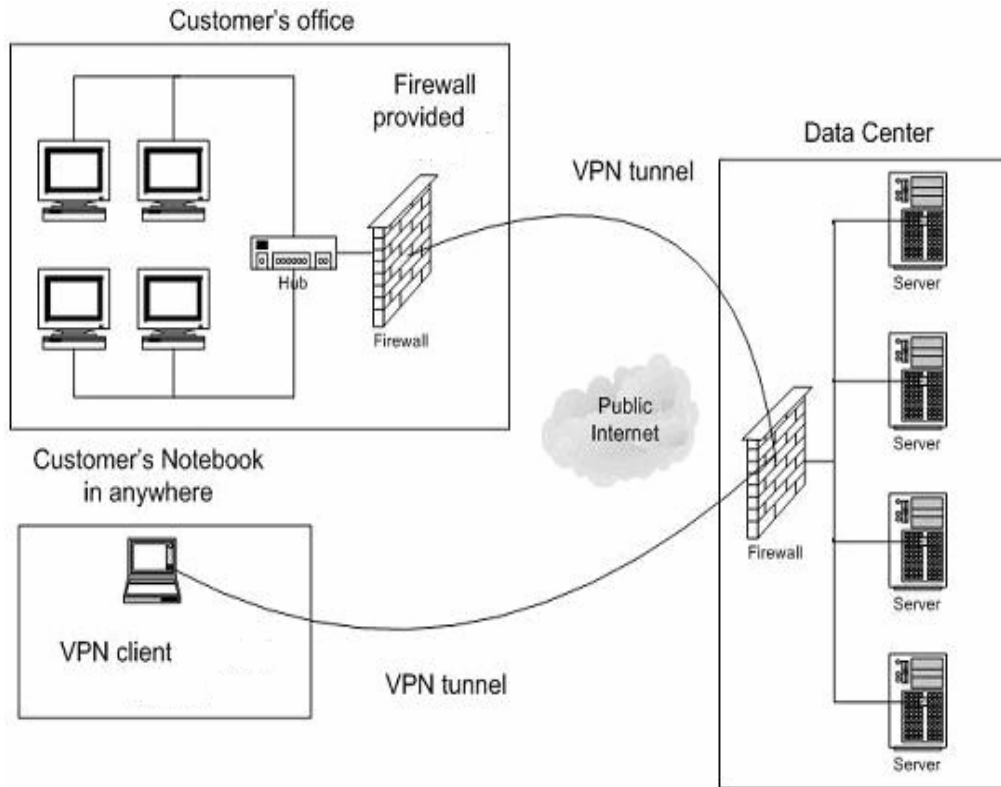
Centralized Environments



- Server is accessed through dummy terminals
- Setup is limited to a building

- ❖ Password based Authentication
- ❖ Access Controls for resources (files)
 - ✓ Privileges (Read, Write and Execute)
 - ✓ Type of user (owner, group, others)

Computer Networks



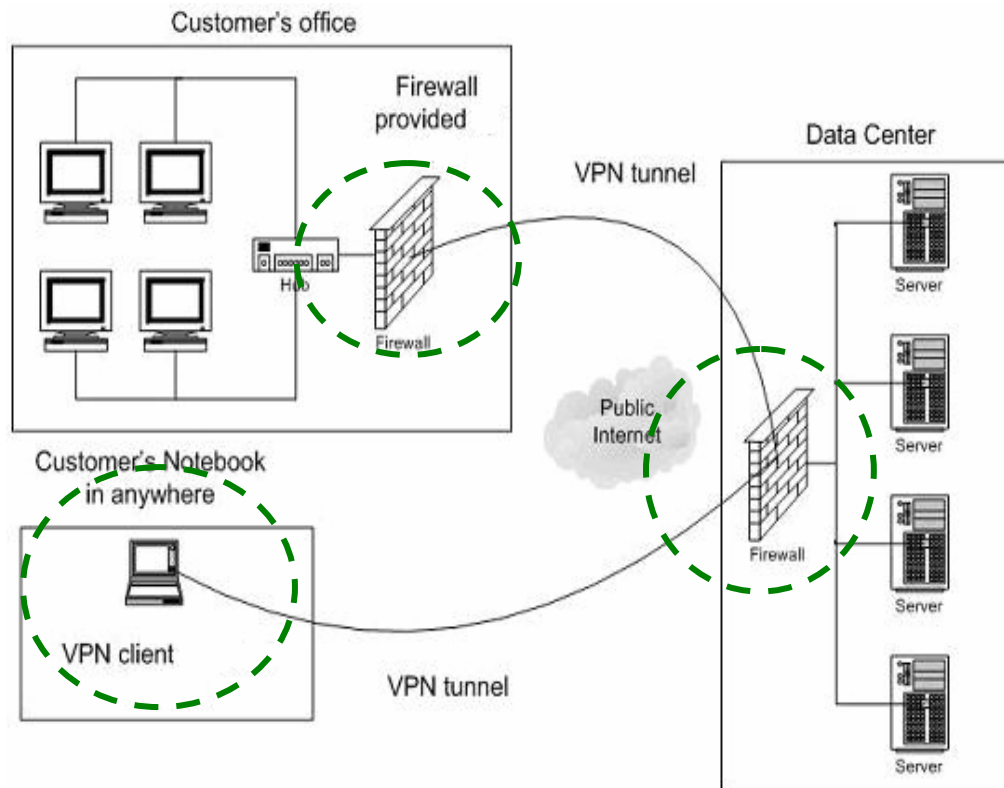
Threats - Services

- ❖ Interruption – Availability
- ❖ Modification – Integrity (Hash Algos)
- ❖ Interception – Privacy (Sym & Asym Cryptographic Algos)
- ❖ Fabrication – Authenticity (Digital Certificates)
- ❖ Repudiation – Non Repudiation (Digital Signatures)

- Interconnection of autonomous PCs, Client-Server architecture
- Access to services within/across networks
- Global Network - Internet

Perimeter Security Solutions

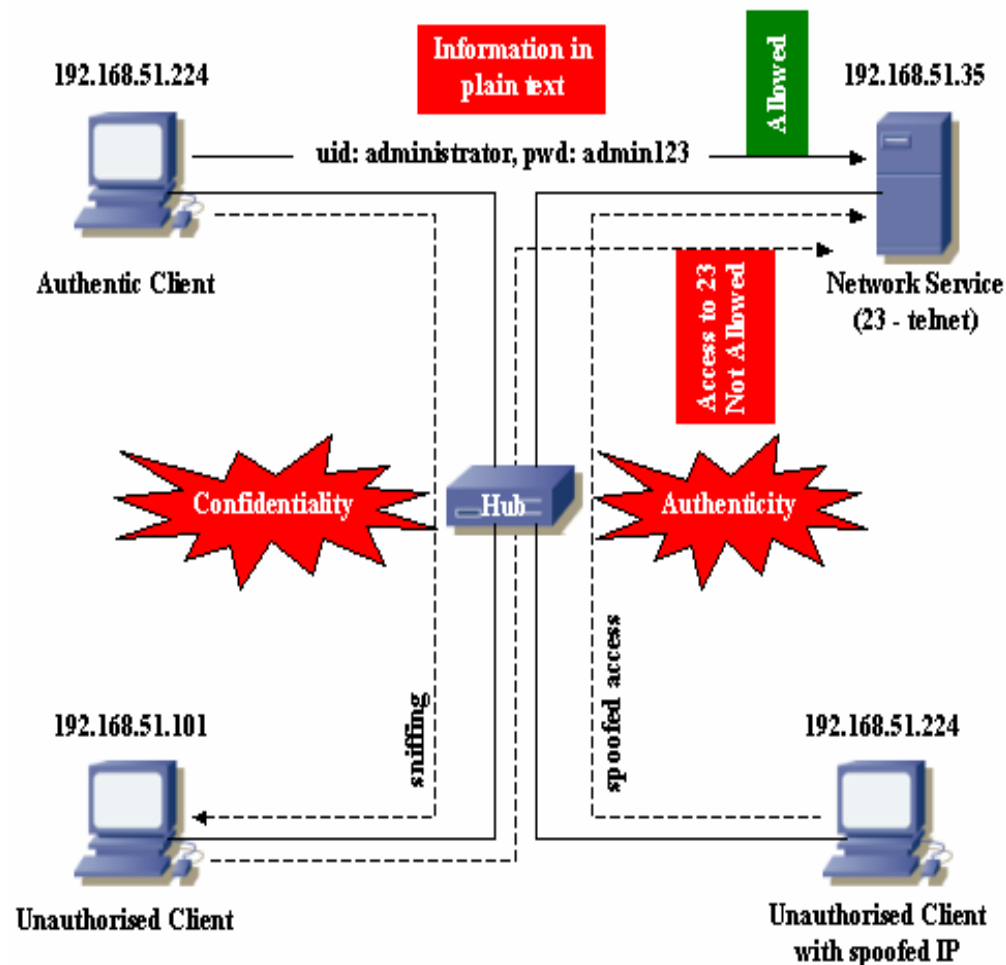
- Towards mitigation of external threat
 - Focus on perimeter security



- Firewalls
- Intrusion Detection Systems/Intrusion Prevention Systems
- Anti Virus
- VPN (IPSec)

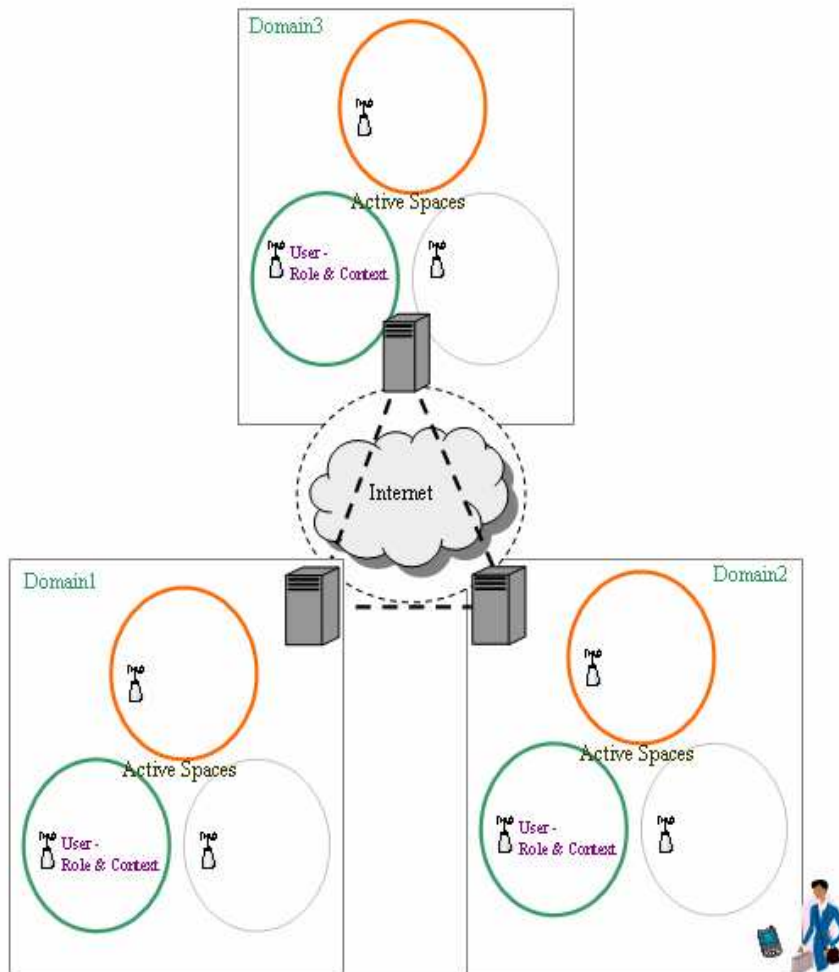
Growing Internal Threat!!!

Integrated End Point Security Management Solutions



- ❖ Multi layered end system security solution
 - Confidentiality
 - Integrity
 - Authentication
 - Network Access Control
- ❖ Transparent to applications
- ❖ Centralized policy administration
- ❖ EnSAFE, ZEN Works etc
- ❖ Anti malware Solutions

Ubiquitous Computing Environment



❖ Diverse Client nodes

❖ Mobility

❖ Context specific

❖ Minimal/No User Involvement

Limitations of Traditional Security Solutions

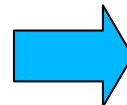


- Client-Server Architecture
- Centralized and Static Access Control Policies.
- User Interactions (Login, logout, file permissions etc)
- Context In-Sensitive
- Non-Adaptable

Security Requirements of Ubicomp Environment



Authentication



- ❖ User
- ❖ Device
- ❖ User – Device Binding

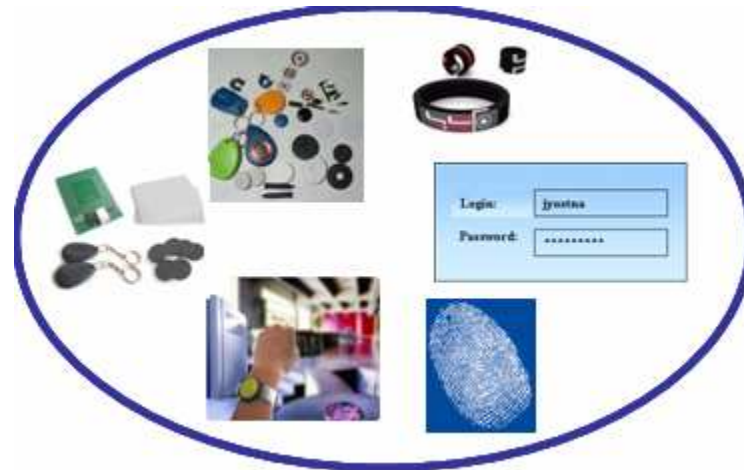


- Passwords
- Biometric
- Digital Certificate
- Pseudonyms

Security Requirements of Ubicomp Environment

Multi Mechanism Support

- Diverse Authentication & cryptographic mechanisms suiting the requirements of different UbiComp applications
- Different characteristics can be used for identification and authentication purposes
- New authentication mechanisms and devices keep evolving



Security Requirements of Ubicomp Environment



Transparency and Unobtrusiveness

- Less or no attention to Computing devices
- Security subsystem also should be transparent
- Blending into the environment without distracting users
- Biometric authentication is preferred



Security Requirements of Ubicomp Environment



Multilevel Security

- Provide different levels of security services based on system policy, services, context information, and available resources
- Ability to combine different identification and authentication mechanisms to build up confidence
- Configurable application specific security



Security Requirements of Ubicomp Environment



Context-Awareness

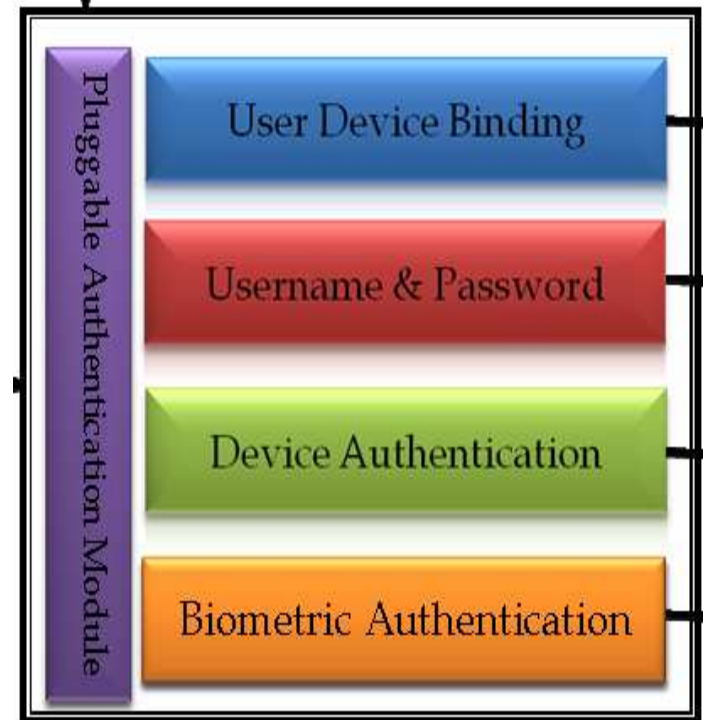
- Ubiquitous Computing integrates context and situational information
- Computing environment is transformed into an active space. Services should use context information
- Security policies should be able to change dynamically
- Need to verify the authenticity and integrity of the context information acquired.



Security Requirements of Ubicomp Environment

Flexibility and Customizability

- Security framework should be flexible and adaptable
- Support for plugging in new mechanisms without downtime or reconfiguration to existing ubiquitous applications and services
- It should support tools in defining and managing policies specific to environment
- Flexibility in interfacing with off-the-shelf solutions for context gathering, adding new mechanisms etc

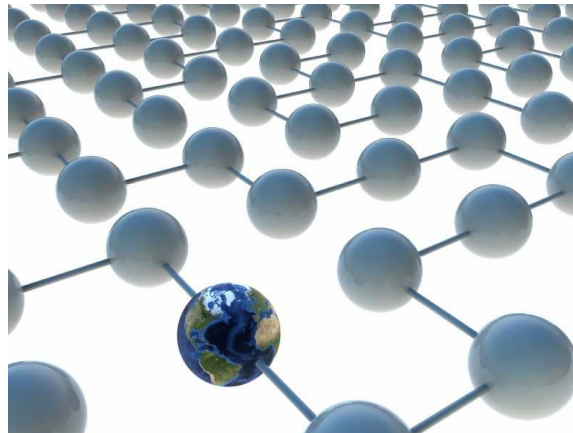


Security Requirements of Ubicomp Environment



Interoperability

- Security Framework should interface with other security solutions and negotiate security requirements
- Flexibility in interfacing with off-the-shelf solutions



Security Requirements of Ubicomp Environment



Extended Boundaries

- The critical requirement is interfacing physical world with the virtual world
- Security policies should get evolved dynamically specific to the active spaces in physical world considering the privacy issues



Security Requirements of Ubicomp Environment



Scalability

- Ubiquitous Computing environment can host hundreds or thousands of diverse devices
- The security services should be able to scale to wide variety of mobile and embedded devices
- Framework should be capable of getting extended to different domains
- Federated Identity Management

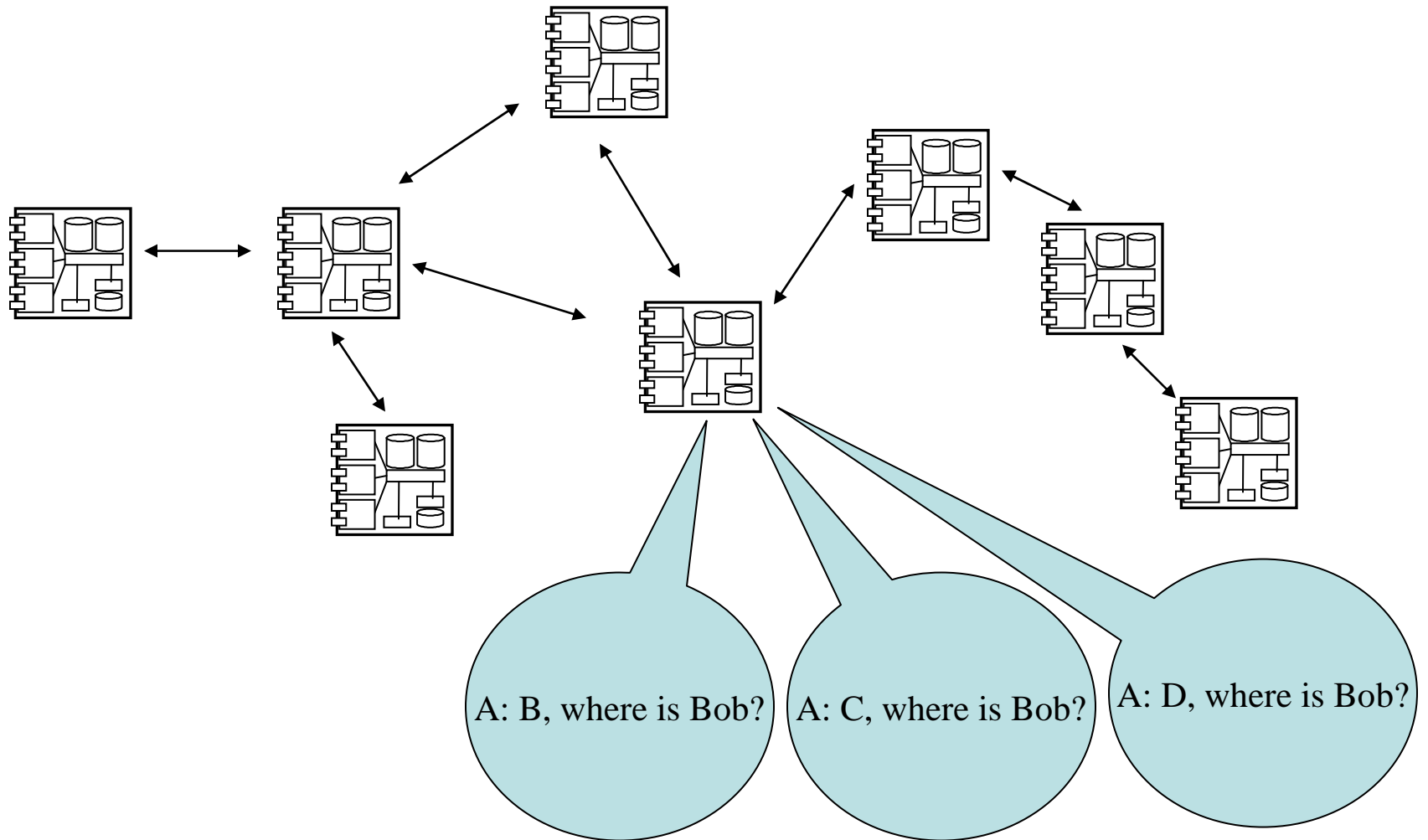


Trust

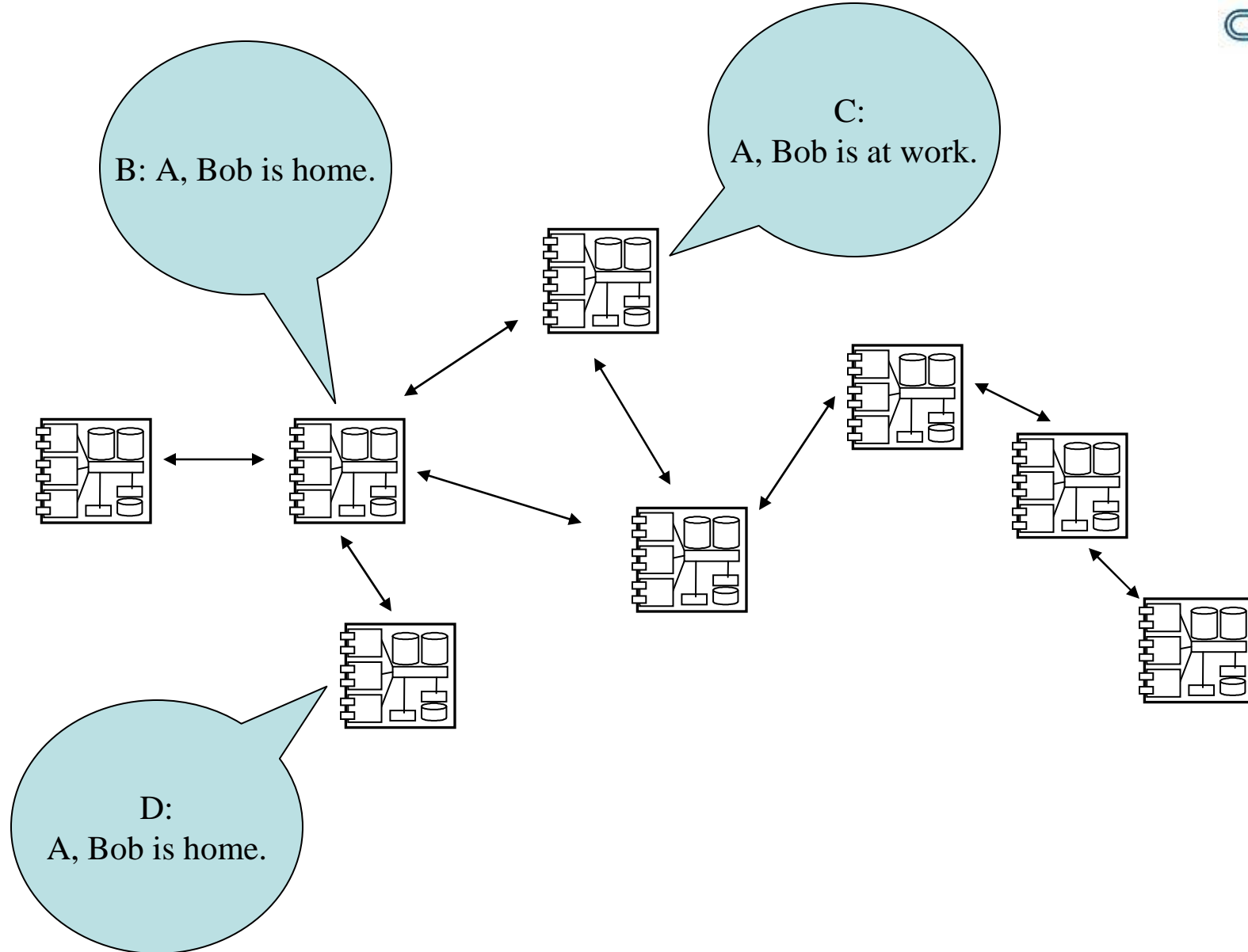
- Trust is a vital part of the holistic risk management system inbuilt in humans
- Building trust suggests that the parties agree to engage at certain levels of risk at certain stages of the relationships or agreement
- Human Trust plays a crucial role in our social life
- We constantly modify and upgrade our trust in other people based on our feelings in response to changing circumstances



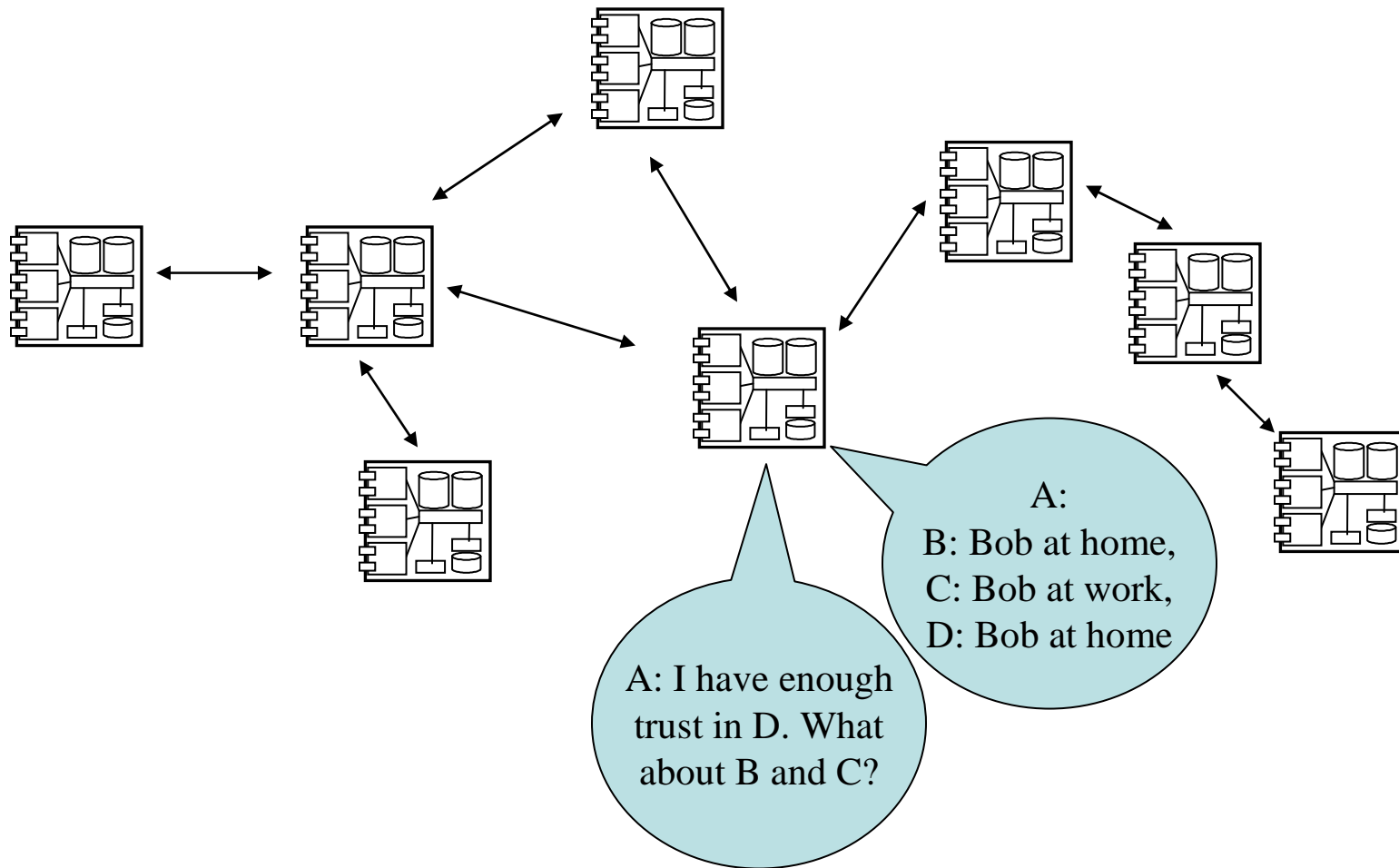
Trust Formation

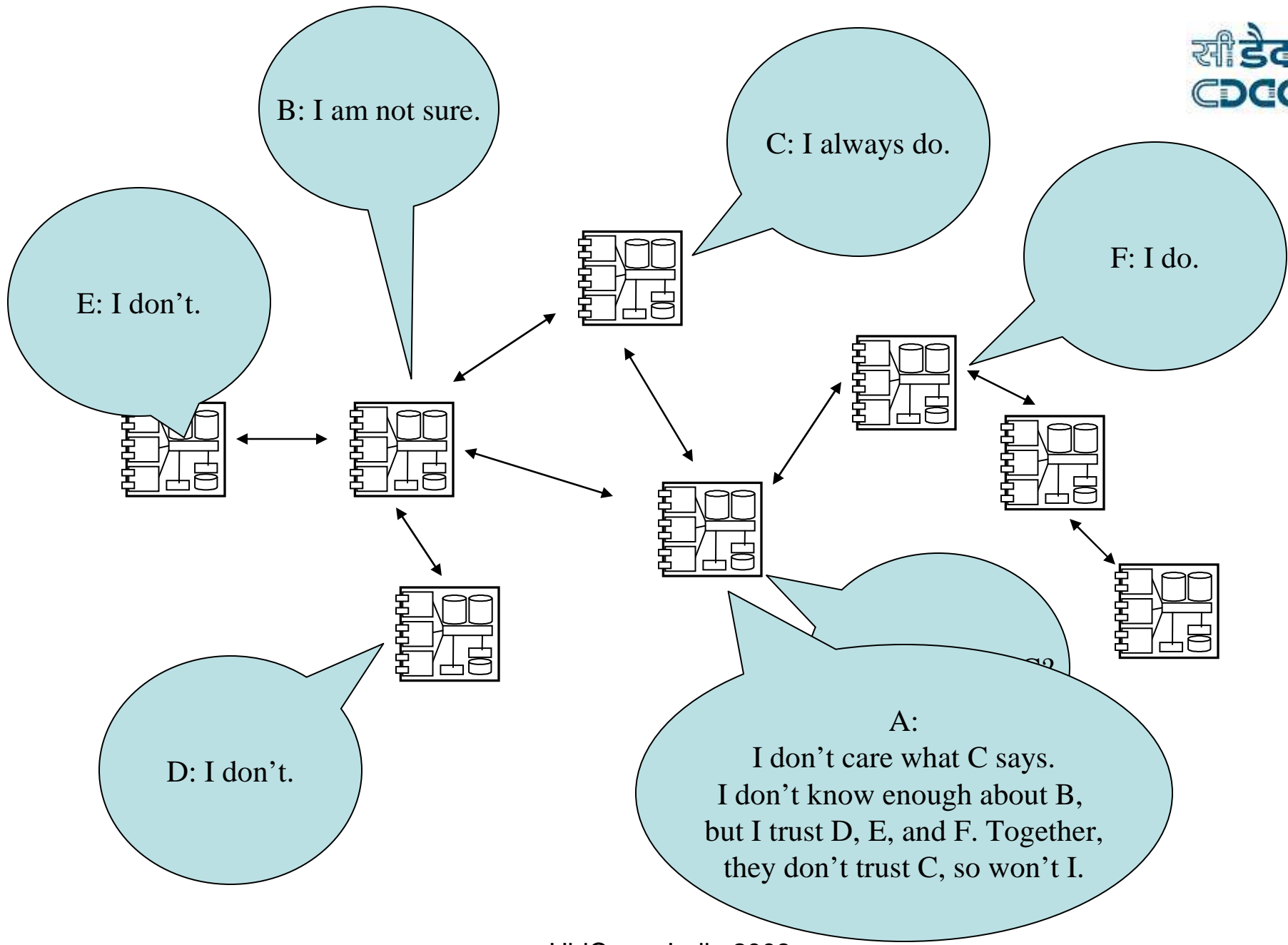


Trust Formation

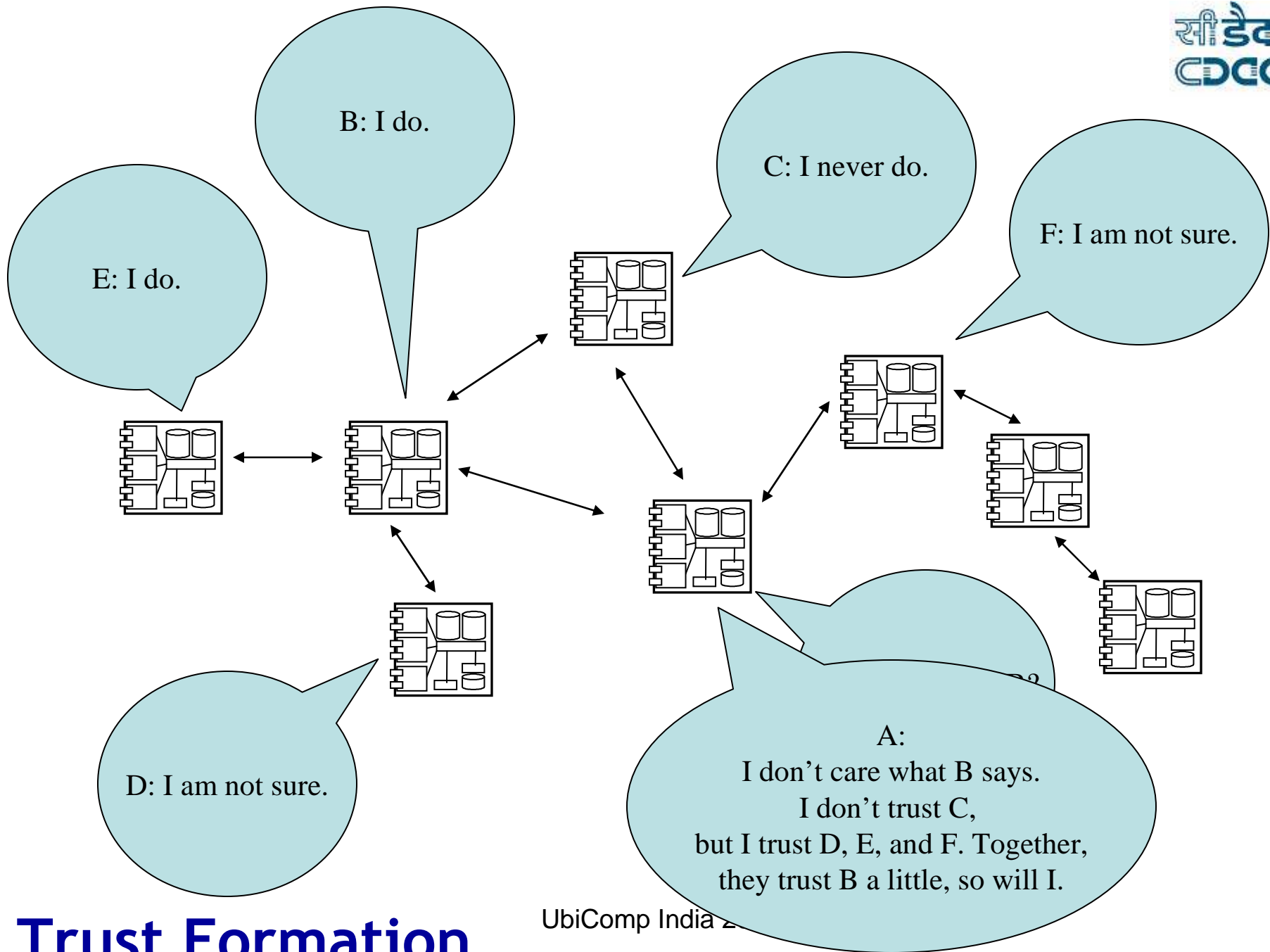


Trust Formation



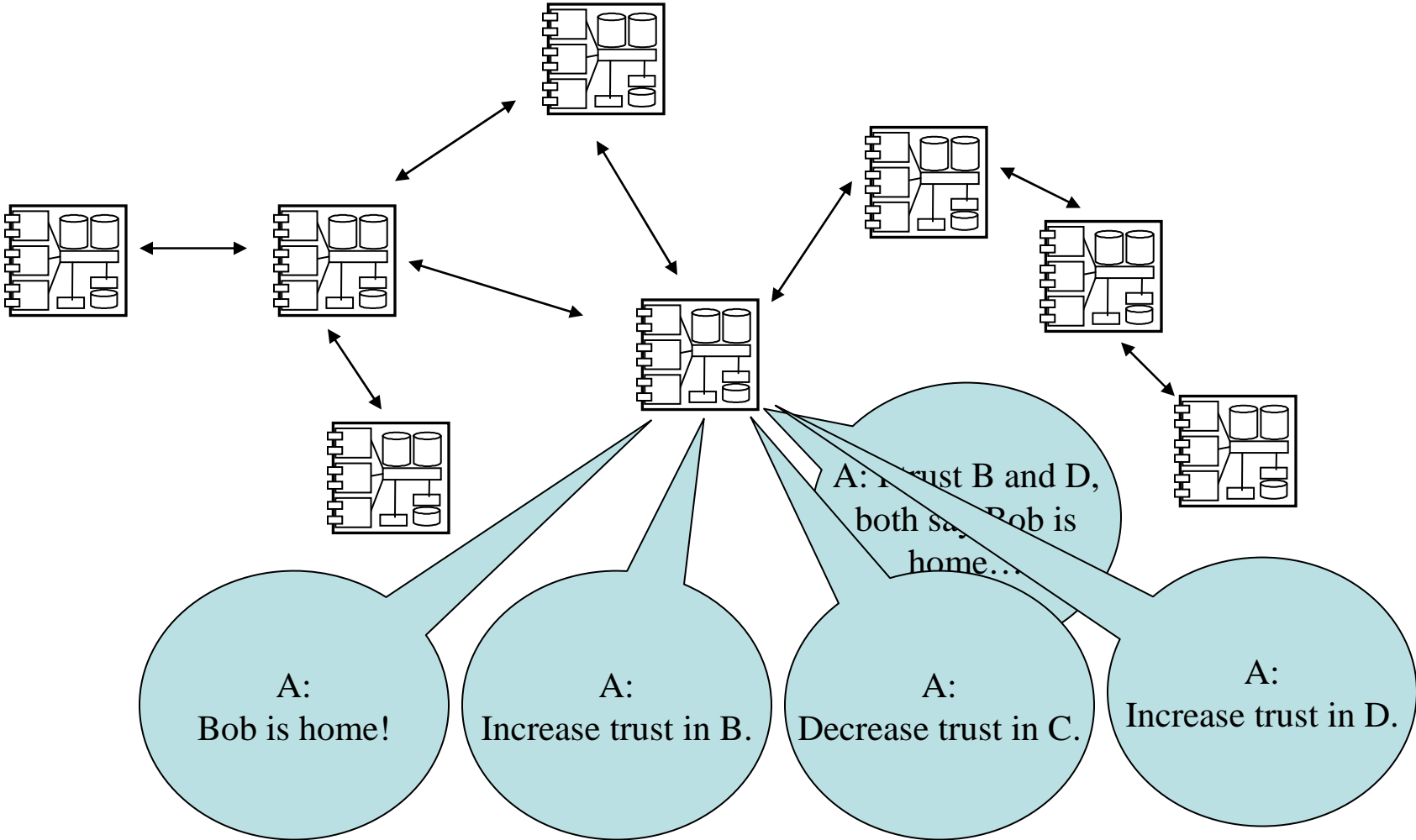


Trust Formation



Trust Formation

Trust Formation



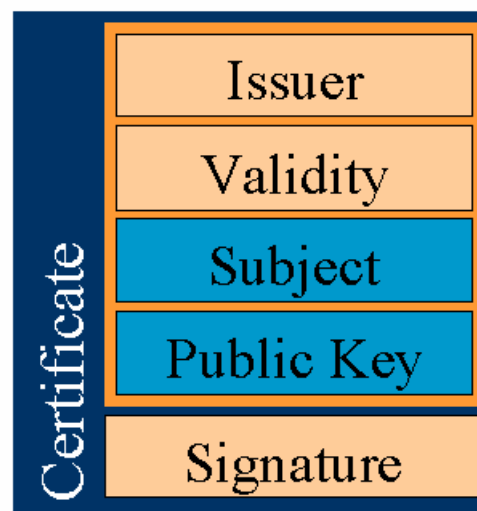
Trust

- Digital trust mechanisms must work well in a dynamic, interactive environment. Computational Trust applies the human notion of trust into the digital world
- The legal framework decreases the risk of misbehavior and secures the financial transactions
- With the rapid growth of global digital computing and networking technologies, trust becomes an important aspect
- The existing legal frameworks are often focused on local legislation



Trust Models

- Certificate based
- Reputation based



Major Security and Trust Management Initiatives



- SECURE (Secure Environments for Collaboration among Ubiquitous Roaming Entities)
- hTRUST (A Human Trust Management Model and Framework)
- STRUDEL (Supporting Trust in the Dynamic Establishment of peering coalitions)
- Risk Aware Decision Framework for Trusted Mobile Interactions and
- TuBE (Trust Based on Evidence) projects.

Survey of Trust Models



Trust Model	Target Environment	Idea
AT&T labs(1996, 1998)	PKI	A lot like Access Control
Abdul-Rahman & Hailes (2000)	Virtual comm.	Intro to Reputation-based Trust Models & agents autonomy
Aberer & Despotovic (2001)	P2P	Attempts distributed Storage of Trust info.
CONFIDANT (2002)	Mobile Ad-hoc	Attempts incorporation of Detection & isolation of misbehavior
SECURE (2003)	Ubiquitous roaming entities	Attempts Incorporation of risk model with Trust
hTrust(2004)	Mobile ad-hoc	Trust Management & dispositional trust. Detection & isolation of malicious recommenders. The HOW question is answered.
McNamara et al. (2006)	Mobile ad-hoc	Mobility introduced as a factor
MATE (2006)	Mobile ad-hoc	Attempts integrated management of trust and risk (an element of dispositional trust).

Privacy

- Ubiquitous applications requires continuous monitoring, gathers vast amounts of sensitive electronic information about the users
- Opportunities for data interception, theft and Ubiquitous surveillance will grow



Technology, Law and Privacy policies together help us to move towards ubiquitous society

References



- Shuxin Yin, Indrakshi Ray, Indrajit Ray, “A Trust Model for Pervasive Computing Environments”, IEEE, 2006
- Jalal F. Al-Muhtadi, “An Intelligent Authentication Infrastructure for Ubiquitous Computing Environments”, Dissertation Work, Urbana, Illinois, 2005
- Craig Chatfield, Rene Hexel, “User Identity and Ubiquitous Computing: User Selected Pseudonyms”, Smart Internet Technology CRC Project, 2006
- Verisign, “Trusted Federated Identity Solution Architecture”, Whitepaper
- Xianzhi Huang, Haiyang Wang, Zhenxiang Chen, Jinjiao Lin, “A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment”, International Symposium on Pervasive Computing and Applications, 2006
- Ramiro Liscano, Kaining Wang, “A Context-based Delegation Access Control Model for Pervasive Computing”, International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2007

References



- John Buford, Rakesh Kumar, Greg Perkins, “Composition Trust Bindings in Pervasive Computing Service Composition”, IEEE International Conference on Pervasive Computing and Communications Workshops PERCOMW’06), IEEE, 2006
- Jean-Marc Seigneur, Christian Damsgaard Jensen, “Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss”, ACM, 2004
- Maria Moloney, Stefan Weber, “A Context-aware Trust-based Security System for Ad Hoc Networks”, IEEE, 2005
- Pho Duc Giang, Le Xuan Hung, Riaz Ahmed Shaikh, Yonil Zhung, Sungyoung Lee, Young-Koo Lee and Heejo Lee, “A Trust-Based Approach to Control Privacy Exposure in Ubiquitous Computing Environments”, Information Technology Research Center, 2006
- Anand Ranganathan, Jalal, Al-Muhtadi and Roy H.Campbell, “Reasoning About Uncertain Contexts in Pervasive Computing Environments”, IEEE Pervasive Computing 2004
- Licia Capra, “Engineering Human Trust in Mobile System Collaborations”, TAPAS European Project, 2001

Acknowledgement



- Our Sincere thanks to Department of Information Technology for supporting Ubiquitous Computing R&D Activities of the centre

Thank You