



Security and Trusted Computing

Vijay Varadharajan

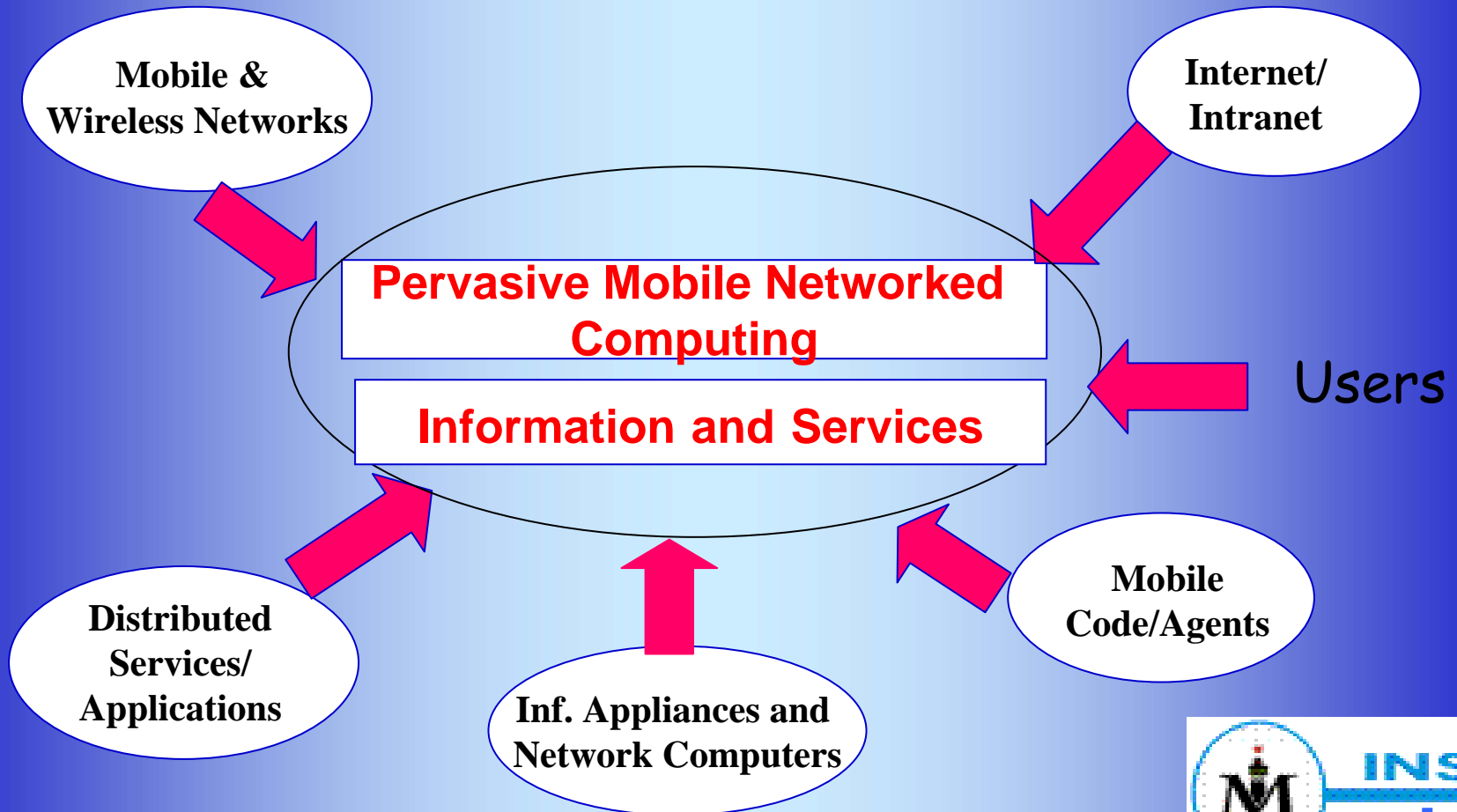
Professor and Microsoft Chair in Computing, Macquarie University
Director : Information and Networked System Security Research
Technical Board Director, Australian Computer Society



Talk Overview

- ◆ ICT Context & Drivers
- ◆ Security and Trust
- ◆ Trust Enabled Secure Systems
- ◆ Research Projects in INSS at Macquarie

Context and Drivers



Some Glimpses of Future Computing

- ◆ Computing power doubles every 18 months (Moore's Law)
 - ❖ 100-fold improvement every 10 years
- ◆ Disk Densities double every 12 months
 - ❖ 1000-fold improvement every 10 years
- ◆ Optical bandwidth doubling every 9 months
 - ❖ 10000-fold improvement every 10 years
- ◆ Every home with giga PCs connected by gigabit networks
 - ❖ Near Future : Giga-PC, 2015 : Tera-PC, 2030 : Peta-PC

ICT Trends and Business Opportunities

- ★ Pervasive Mobile Networked Computing Technology
 - ★ Always On Networking Infrastructure
 - ★ Wired and wireless interconnected networks based on Standards
 - ★ Useful Information and Services
 - ★ Personalization and Customization of Services
 - ★ Services embedded in Environment
 - ★ Delivery via easy to use Mobile Information Appliances
 - ★ Task oriented Information Appliances

- ➔ Both Technical Challenges and Business Opportunities

Challenges

◆ Some Technical Challenges

❖ Scalability

- ◆ How can a billion users access the same item at once?

❖ Dependability

- ◆ Availability, Security, Reliability of Information

❖ Content Management

- ◆ How to manage and extract useful information?

❖ Policy Management

- ◆ Propagation, Administration and Enforcement of Policies

Security : A Key Enabling Technology

◆ Security

- ❖ Peace of Mind
- ❖ Trust
- ❖ A Business Necessity

◆ Security

- ❖ Relative to Threats
- ❖ Cost, Time, Customer Expectations
- ❖ Penetrator versus Designer

Mobile Networked Computing Security Challenges

◆ Challenges

❖ Pervasiveness

- ◆ Operating Systems, Networks and Protocols,
- ◆ Databases, Applications, Hardware, Users

❖ Multiple Platforms

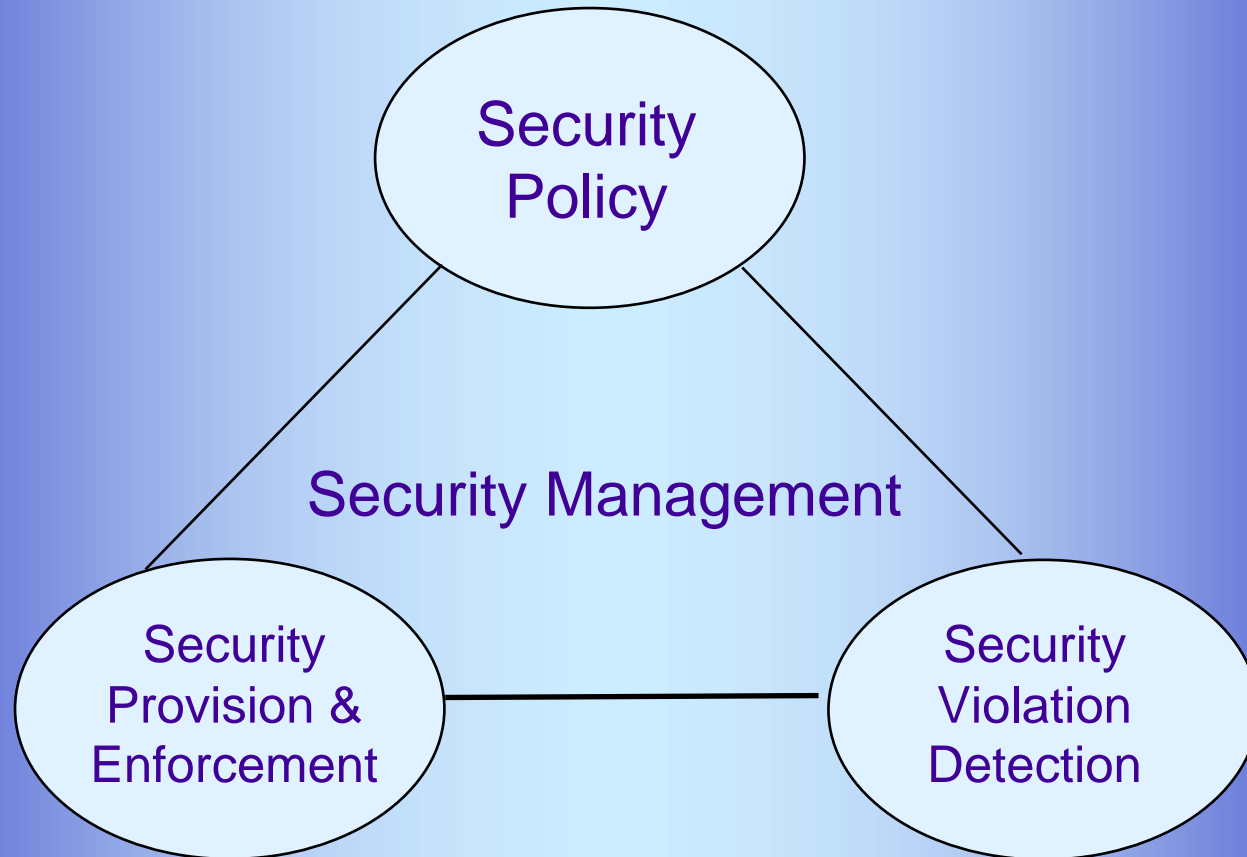
❖ Different Vendors

❖ Different Security Policies

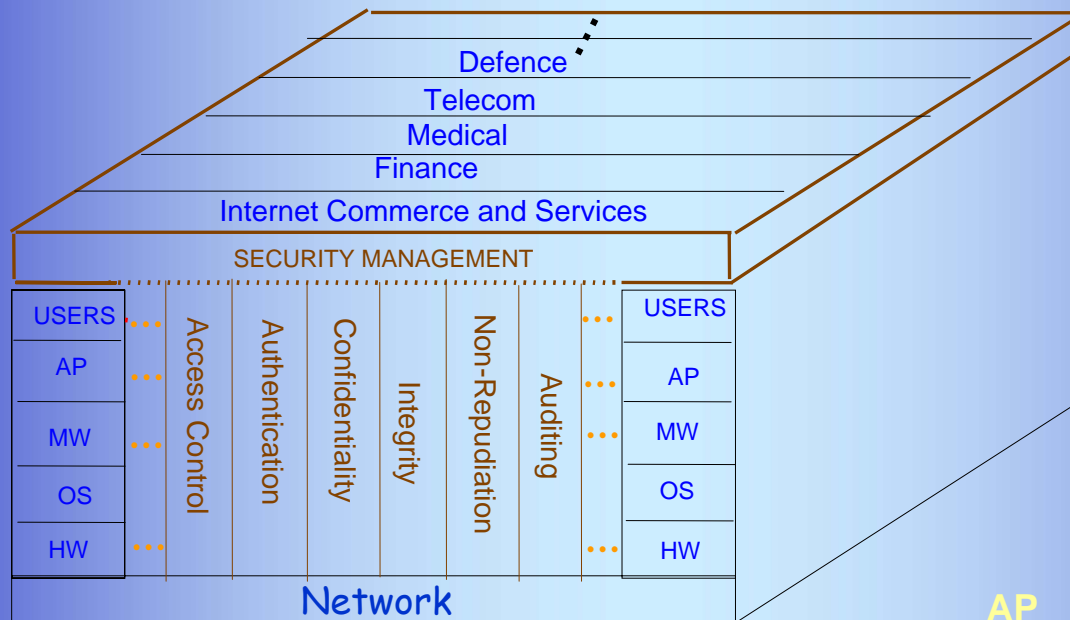
❖ Several Security Standards

❖ Interoperability

Security Philosophy



Networked Computing Security Solutions



AP = Application
MW = Middleware
OS = Operating System
HW = Hardware

Security and Privacy

- ◆ Security
 - ❖ *Owner* of Information has control
 - ❖ Security is Not Privacy
- ◆ Privacy
 - ❖ *Subject* of Information has control
 - ❖ Privacy requires Security
- ◆ Anonymity
 - ❖ Has no subject
 - ❖ Requires Security and guarantees Privacy, but is neither

Security and Trust

- ◆ Trust has been around for many decades (if not for centuries) in different disciplines in different disguises
 - ❖ Psychology, Philosophy, Sociology as well as in Technology
- ◆ Some Notions
 - ❖ Luhman: “we as humans would not be able to face the complexity of the world without resorting to trust”
 - ❖ Gambetta: “trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends”
 - ❖ Trust : “It will not harm me”, “No Surprises”
 - ❖ Trust : From a malicious point of view

Security and Trust

- ◆ Trust Relationship
 - ❖ Trustor : an entity that trusts another entity (target)
 - ❖ Trustee : an entity that is trusted
 - ❖ Action
 - ❖ Context
- ◆ Trust Relationship is a belief by a trustor on the trustee's actions
 - ❖ Competency : Ability
 - ❖ Honesty : Intentions
 - ❖ Reliability : Correctness and commitments
 - ❖ Availability : Resourceswithin a context

Trusted Systems

- ◆ Trusted Computer System Evaluation Criteria (TCSEC) (Orange Book) in the late 1970s and early 1980s
- ◆ Trust → Process of convincing the observers that a system (model, design or implementation) is correct and secure
- ◆ Set of ratings is defined for classification of systems
 - ❖ Higher the level, greater the assurance that one has that the system will behave according to its specifications → higher level of “trust”
 - ❖ C1, C2, B1, B2, A1
 - ❖ TCSEC, ITSEC, Federal and Common Criteria
 - ◆ Functionality and Assurance

Trusted Systems

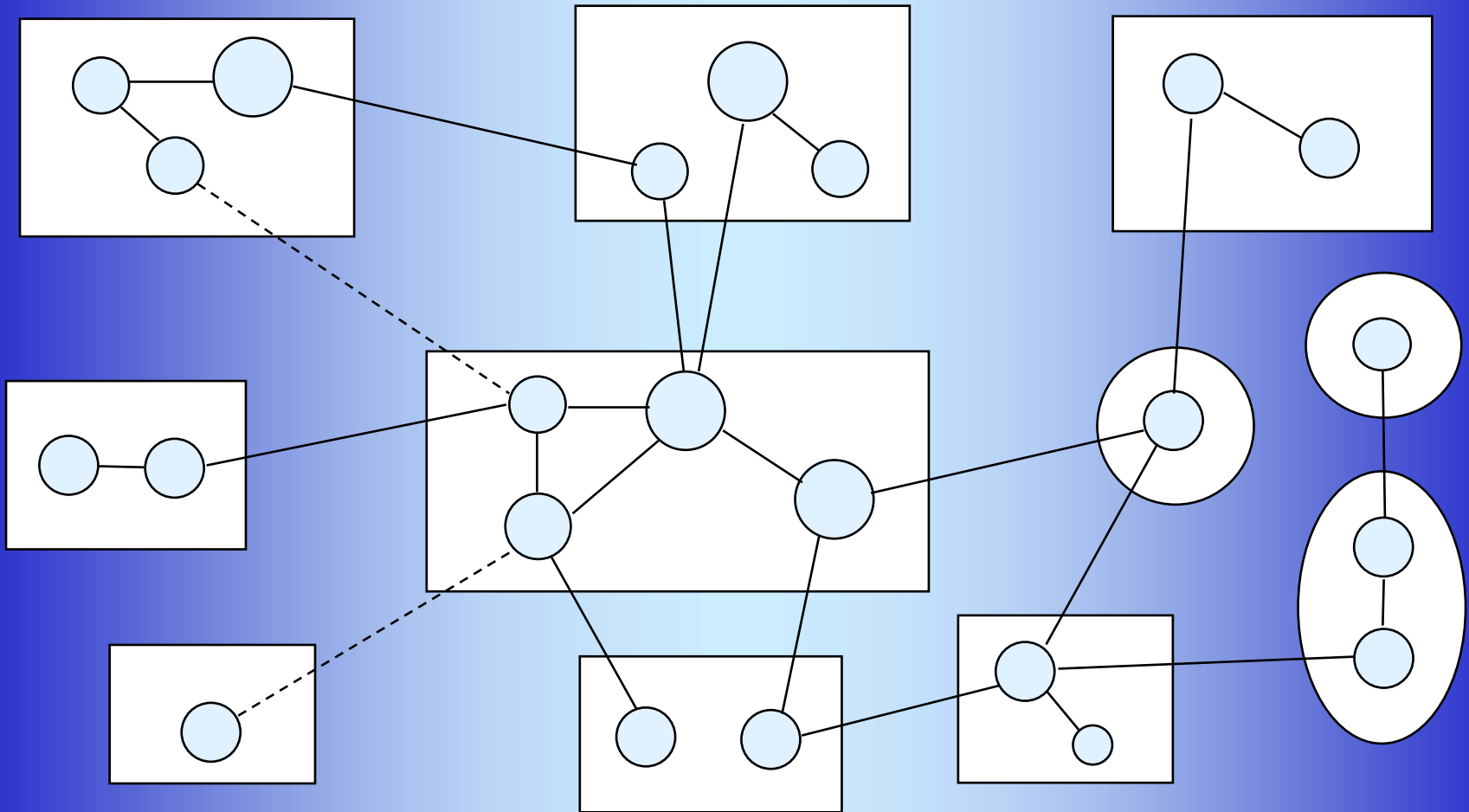
- ◆ Trusted Computing Base (TCB)
 - ❖ “totality of protection mechanisms needed to enforce the security policy”
 - ◆ Hardware and Software
- ◆ Particularly in the Operating System Context
 - ❖ Reference Monitor
 - ❖ Security Kernel based OS Architectures
- ◆ “Trusted” Processes
 - ❖ These processes are trusted in that they will not do any harm even though they may violate the security policies of the system

Security and Trust in Distributed Systems

◆ Some Examples of Trust

- ❖ Trustor “trusts” a trustee entity to access and use the resources s/he owns or controls (e.g. application or service)
- ❖ Trustor “trusts” a trustee entity to provide a service
- ❖ Trustor (e.g. a user) “trusts” a trustee entity (e.g. CA/AS) to perform authentication and certification of another entity (Authentication Trust)
- ❖ Trustor (e.g. a user) “trusts” a trustee entity (e.g. ACS) to perform authorization actions (Authorization Trust)
- ❖ Trustor “trusts” a trustee entity to make a delegation on its behalf (Delegation Trust)
- ❖ Trustor (e.g. a user) “trusts” a trustee entity (e.g. network) to provide certain services (Infrastructure Trust)

Trust in Federated Distributed Environment



Security and Trust in Distributed Systems

◆ Mobility

◆ Software Mobility

- ◆ Programs may come from unknown or untrusted sources
- ◆ Difficulty : Identification of creator and/or sender principal associated with a program
- ◆ How to associate a level of trust with the program ?
 - The principal most relevant for determining trust may not be known to the system
- ◆ Complicates the issue of determining whether or not an action requested by the program is to be allowed
 - May not be safe to assume that when a program requests a certain action, any particular person intends that action

Trusted Computing Platforms

- ❖ A Trusted Computing Platform
 - ❖ has a trusted component (s) in the form of built-in hardware and uses this to create a foundation of trust for software processes
 - ❖ PC, Server, PDA, Printer, Mobile Phone
 - ❖ “Trusted” by local and remote users and software and entities
- ❖ Basis of Trust: Declaration on
 - ❖ the computing platform behaves as expected
 - ❖ the software running on a machine behaves as expected
 - ❖ what entity and to whom the user is talking to
 - ❖ the information is transmitted accurately and its privacy protected

Trusted Computing Platform Alliance (TCPA/TCG)

◆ TCPA view of Trust

- ❖ Something is trusted “if it always behaves in the expected manner for the intended purpose”

◆ TCPA: Vouches for the State of the Machine

- ❖ Whether a platform *can* be trusted?

- ◆ Collect and provide evidence of system behaviour

- ❖ Whether a platform *should* be trusted?

- ◆ Provide confidence on the collection and evidence mechanisms
- ◆ Provide confidence that particular values of evidence represent that the platform is in a “good” state”

Security and Trustworthy Computing

◆ Microsoft

❖ Trustworthy Computing Initiative

- ◆ Making something trustworthy requires a social infrastructure as well as solid engineering
- ◆ Software, Systems, Computers, Services and Organizations

❖ Basis for someone to trust a system

- ◆ Security
- ◆ Privacy
- ◆ Reliability
- ◆ Business Integrity

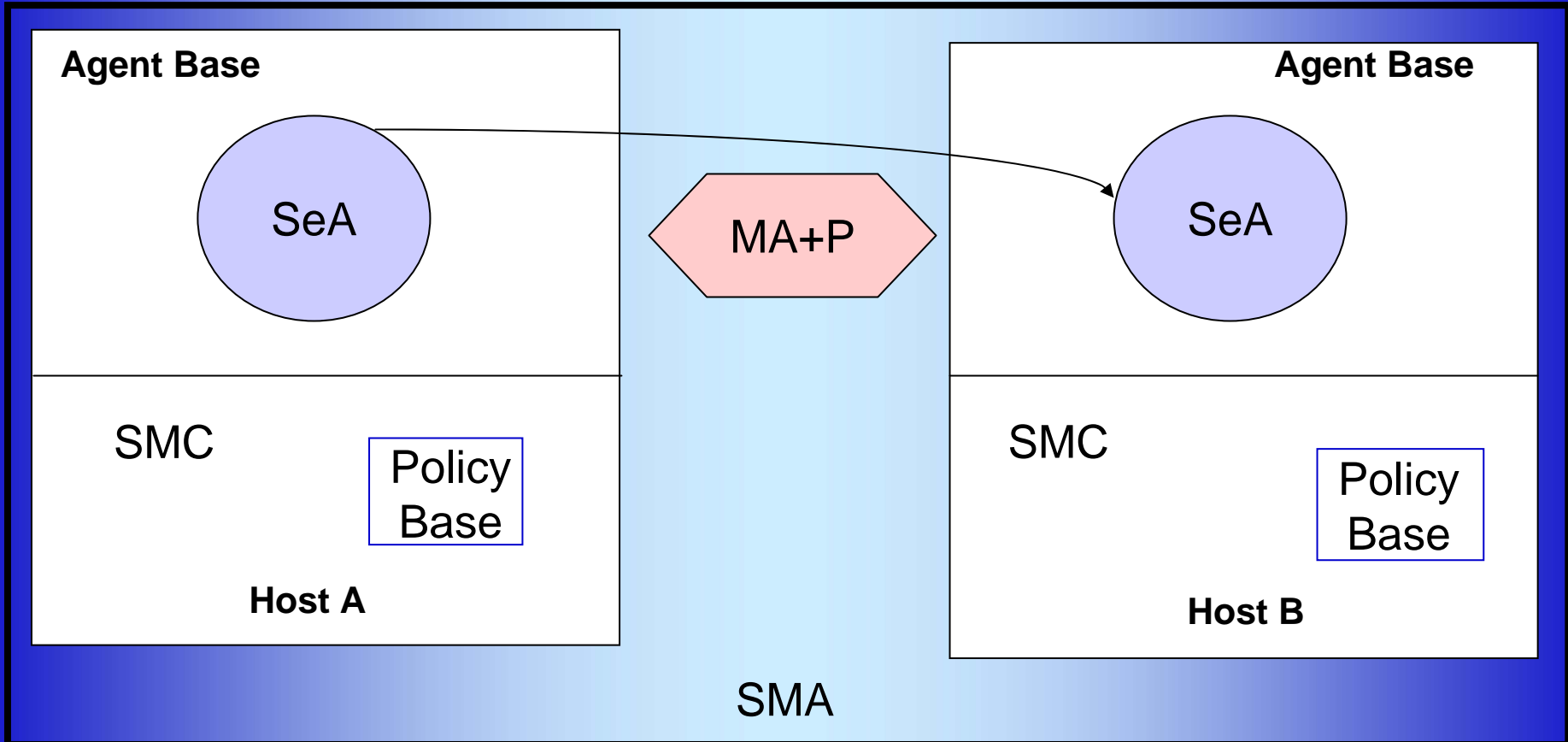
Trustworthy Computing & Distributed System Security

- ❖ Impact of Trusted Platforms on Security Architectures
 - ❖ “Distribution” of the Security Service to the “most appropriate” location
 - ❖ Authentication
 - ❖ Capturing Aspects of Authentication Server within the Trusted Platform of the Client/Server
 - ❖ Authorization
 - ❖ Creating instances of authorization service.
 - ❖ Mutual or two-way authorization policies at both requester and service provider ends
- ❖ Applications based on Trusted Platforms

Security and Trusted/Trustworthy Computing

- ◆ Tour of some Trust Concepts in the Secure Computing World
- ◆ Concept of Hybrid Trust
 - ❖ “Hard” and “Soft” Trust
- ◆ Model and Design of Trust Enabled Secure Systems
 - ❖ Explicit use of Trust in Secure Decision Making
- ◆ Application to Mobile Software Agent based Internet Systems
Distributed Web Services and Peer to Peer Computing
Applications
- ◆ Research Projects in INSS at Macquarie

Security Enhanced Mobile Agents

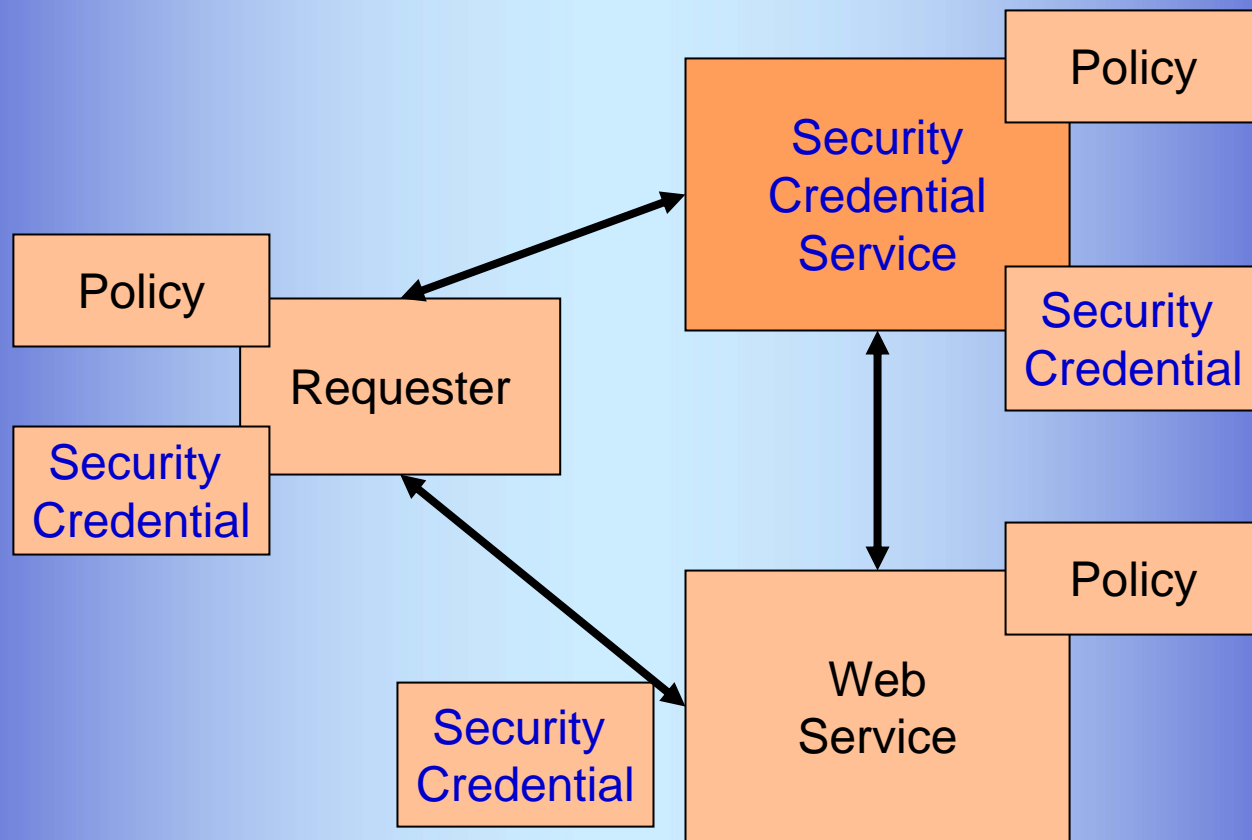


Trust Enabled Secure Mobile Agent System

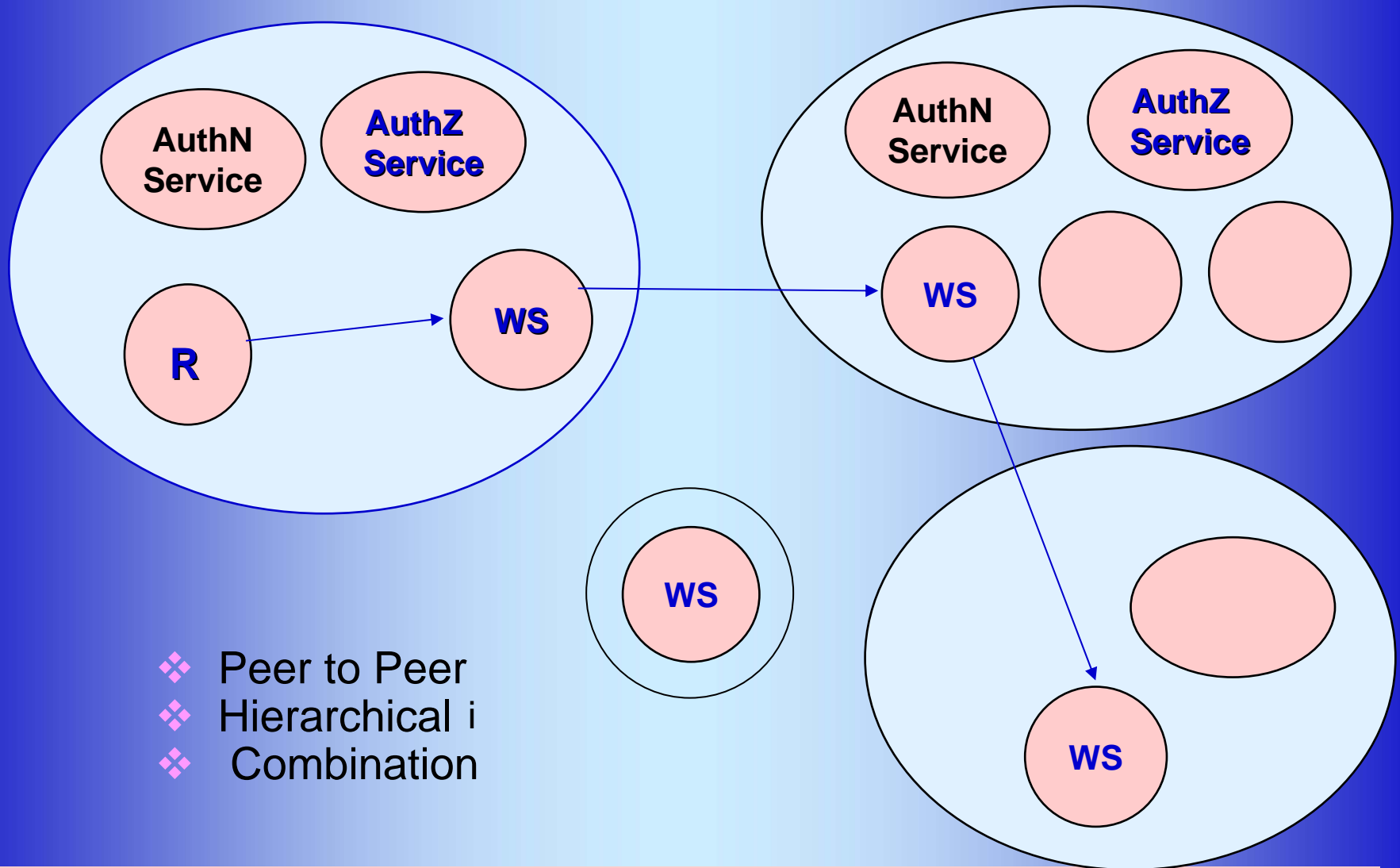
◆ Trust Enhanced Security Solution

- ❖ Trust Model that is capable of capturing
 - ◆ Range of Trust Relationships
 - Direct, Recommended, Derived
 - ◆ Different types of Trust
 - Authentication, Execution and Code
- ❖ Trust Management Architecture
 - ◆ Representation, Evaluation and Updating of Trust Relationships and Decisions
- ❖ Trust Outcomes Enhance Security Model and Decision Making

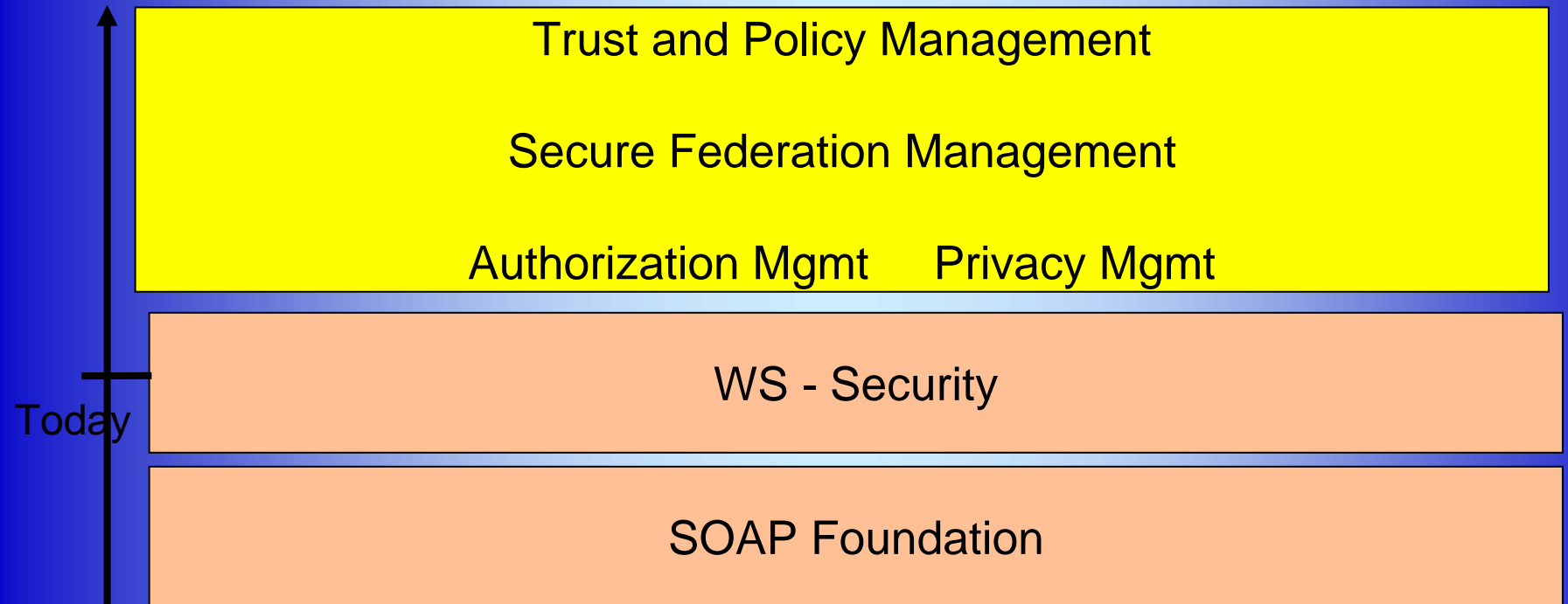
Secure Web Services



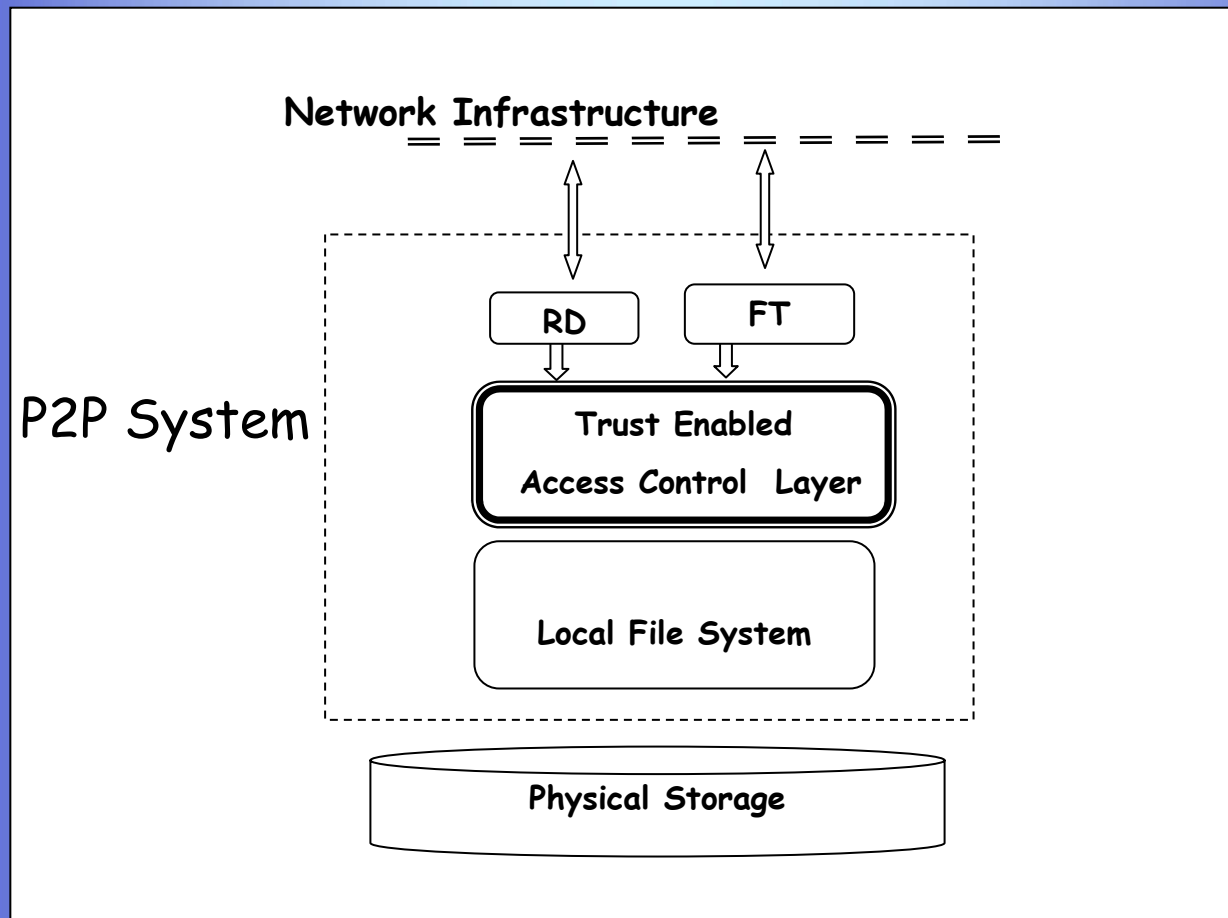
Securing Distributed Web Services



Trust Enabled Secure Web Services



Trust Enabled P2P File Sharing System



Information and Networked Systems Security (INSS) Research Mission

Achieve fundamental advances in security concepts and techniques and their application to mobile networked computing technologies

Through conducting and exploiting world class research

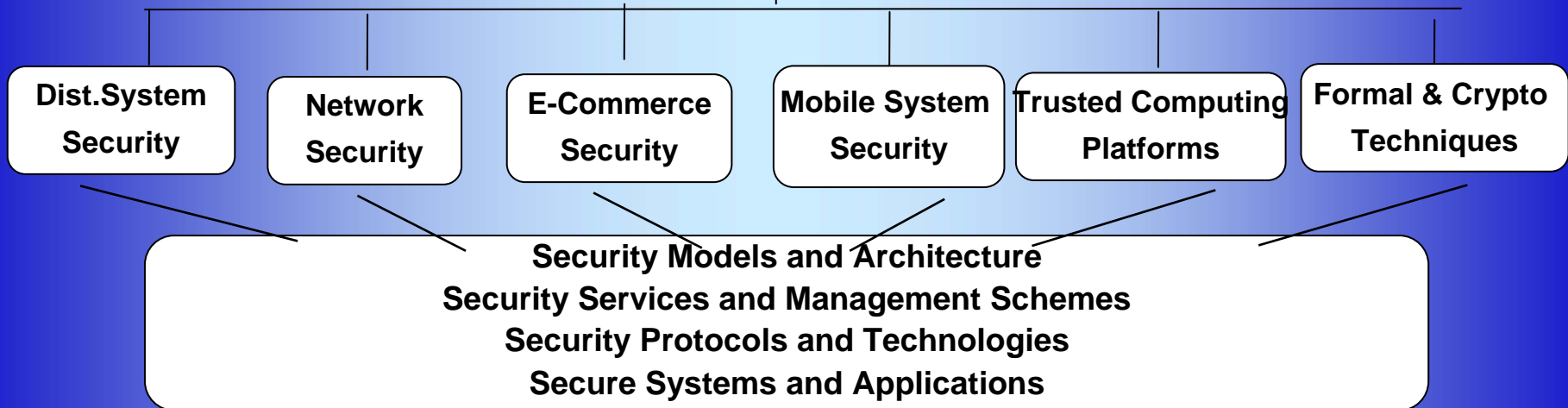
To enable secure design of systems and applications and to improve security in organizations

Research Significance and Objectives

- ◆ Our research addresses security techniques for Wired and Wireless Networks, Fixed and Mobile Distributed Applications, Small Information Appliances to Large Scale Distributed Systems.
- ◆ Our research
 - ❖ Improving the understanding of the security requirements for distributed systems and networks
 - ❖ Development of security models and trust schemes
 - ❖ Design of Security Services and Mechanisms and their Security Management
 - ❖ Formal Security Models and Verification of Security Properties
 - ❖ Development of Practical Security Solutions for various Business Segments

Information and Networked System Security Research

(<http://www.comp.mq.edu.au/research/inss>)



Research Team

Professor Vijay Varadharajan

Dr. Michael Hitchens (Macquarie)
Dr. Yi Mu (Macquarie/UoW)
Dr. Yan Wang (Macquarie)
Dr. Paul Watters (Macquarie)
Dr. Chun Ruan (UWS)
A/Prof. Doan Hoang (UTS)
Prof. Isabelle Chrisement (INRIA)
Dr. Ghassan Chaddoud (London)
Dr. Hua Wang (USQ)

Mr. David Foster
Mr. Weilang Zhao
Mr. S.Indrakanthi
Mr. Uday Tupakula
Mr. Venkatesh Balakrishnan
Mr. Janson Zhang
Mr. Ching Lin
Mr. Huu Truan
Mr. Rajan Shankaran
Mr. Aungkhon



Concluding Remarks

- ICT Context
 - Security and Privacy
 - Trust, Trusted and Trustworthy Computing
 - Trust Enabled Secure Systems and Apps

- ❖ Several Significant Challenges and Issues in Secure Trustworthy Computing and Applications