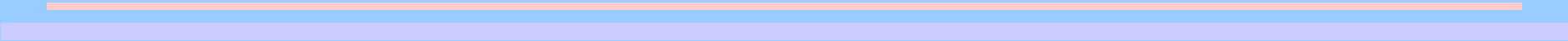




Trust and Security in Distributed Information Infrastructures

Vijay Varadharajan*

Visitor: e-Science Institute, Edinburgh

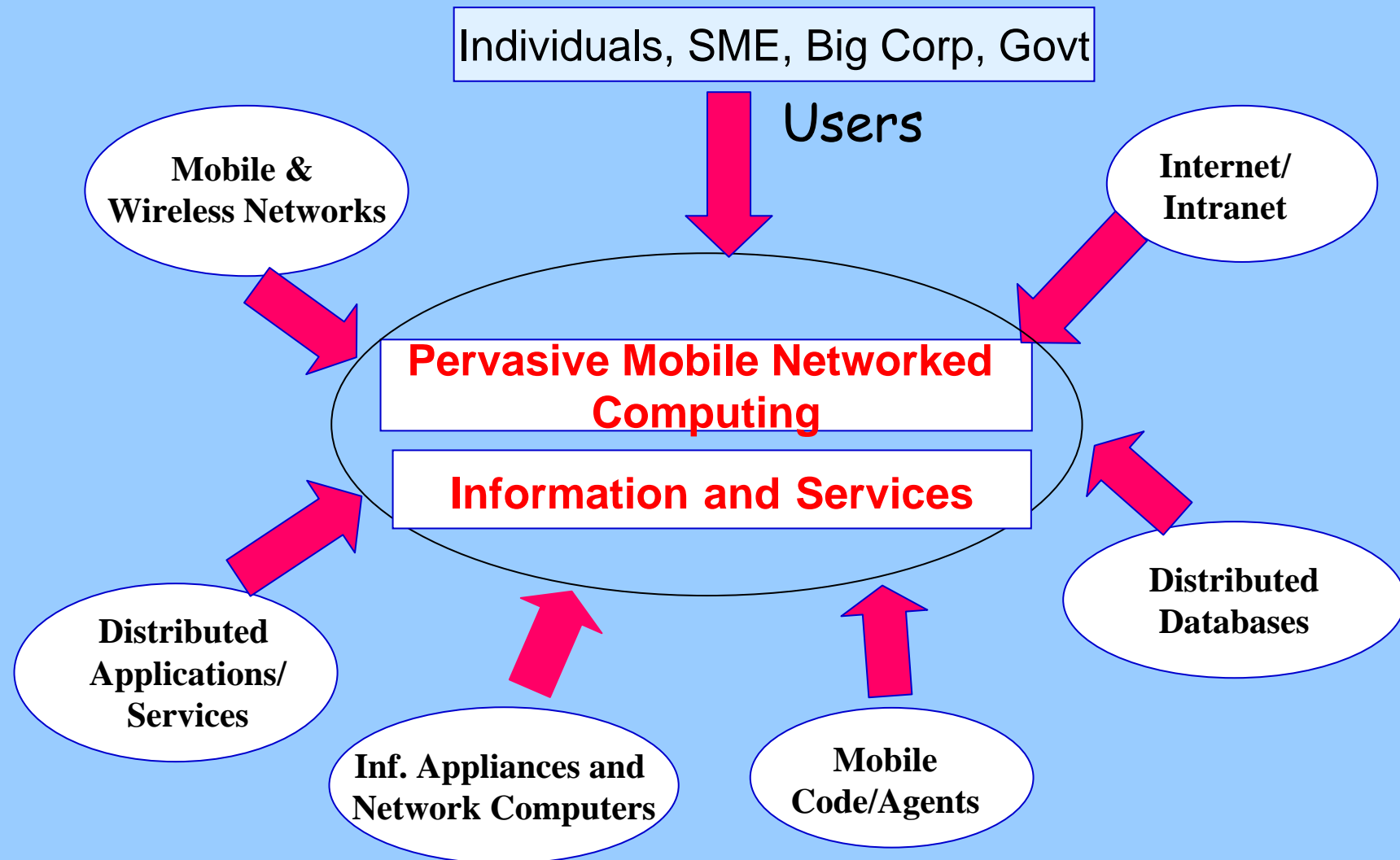


* Microsoft Chair Professor in Innovation in Computing, Macquarie University, Australia

Talk Overview

- ❖ ICT Context and Drivers
- ❖ Security and Trust
- ❖ Trust in Security Technologies
- ❖ Trust Models and Management
- ❖ Trust Enhanced Secure Mobile Agents
- ❖ Concluding Remarks

Technology: Context and Drivers



Distributed Infrastructures and Services

- ◆ Critical Information Infrastructures
 - ◆ Power, Utility, Logistics
 - ◆ Telecom
- ◆ Financial Infrastructures
 - ◆ E-Banking, E-Commerce
- ◆ Healthcare Information Systems
 - ◆ E-Health
- ◆ Government Services and Applications
 - ◆ E-Government, E-Voting, ...
- ◆ Peer to Peer Applications
 - ◆ Social Networking
- ◆ Transportation Systems
- ◆ ...

Some Glimpses of the Future

- ❖ Dramatic growth in computing power, storage and bandwidth
 - ❖ Giga → Tera → Peta Personal Computing Machines
- ❖ We can probably store almost everything
 - ❖ 300 Million Books : 100 terabytes (approx \$1M)
 - ❖ All Movies made todate : 1 petabyte
 - ❖ All Music recorded todate : 1 petabyte
 - ❖ 1 Billion Photos : 1 petabyte
- ❖ Capture everything you said from the time you are born to the time you die.
 - ❖ Less than one percent of a petabyte
- ❖ Everything you ever did and experienced can be captured in living color
 - ❖ With only a few petabytes.
- ❖ With 1.6 terabits per second on a single fiber
 - ❖ In one second, you can transmit 10 HDTV movies, or 40 regular full-length feature films.
 - ❖ Less than a minute to transmit all the books in a typical large national library

Characteristics of Emerging Computing

- ❖ Smaller, Cheaper, Embedded Computing
- ❖ Pervasive Networking and Mobility
- ❖ Systems of Systems
- ❖ Information Explosion
- ❖ Growth in User-Centric Services
- ❖ Growth in On-demand Services
- ❖ Global Reach and Participation: Large Scale

Several Security Challenges

- ❖ Secure Scalable Dynamic Distributed Systems and Applications
 - ❖ How can a billions of users securely access information?
- ❖ Dependability of Systems and Services
 - ❖ Availability, Security, Reliability of Information
- ❖ Trust Management and Trusted Online Communities
 - ❖ Managing Trust between Autonomous Unfamiliar Entities in the Provision of Services over the Internet
- ❖ Policies : Security, Trust, Privacy
 - ❖ Propagation, Administration and Enforcement of Policies
- ❖ Counteracting Epidemic Style Attacks (e.g. Critical Information Infrastructures)
 - ❖ Denial of Service Attacks, Phishing, Spam, Viruses and Worms
- ❖ Protection of Mobile Software Agents and Applications over the Internet
- ❖ Self-Organization and Management in Dynamic Networks
- ❖ Seamless Secure Integration of Wired, Wireless and Mobile Infrastructures

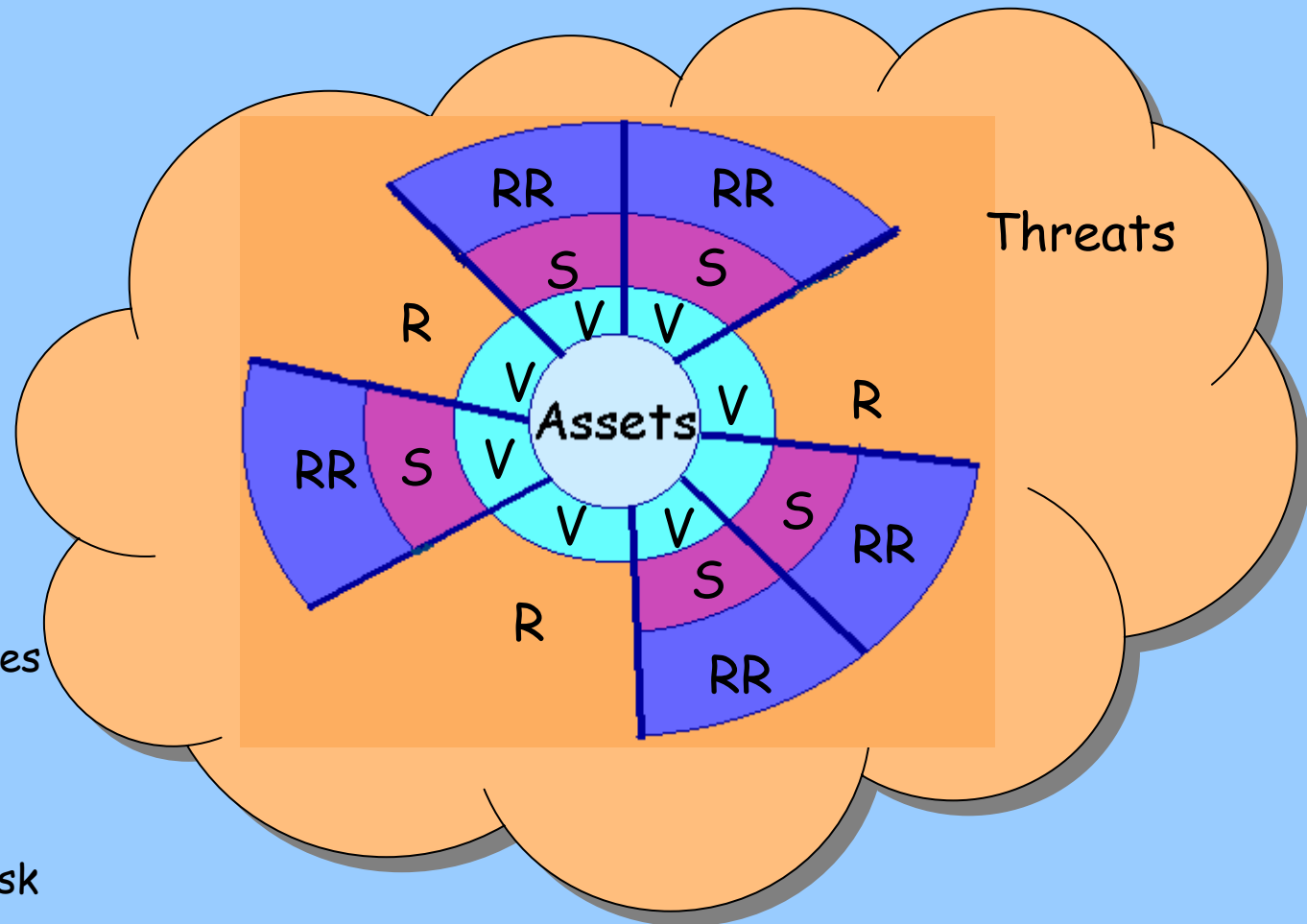
Security

- ◆ Security
 - ❖ Relative to Threats
 - ❖ Cost, Time, Customer Expectations

- ◆ Security
 - ❖ A Business Necessity
 - ❖ Part of the Cost of Doing Business
 - ❖ Peace of Mind

- ◆ Constant Race
 - ❖ Attacker versus Designer
 - ❖ Code Breaker versus Code Maker

Security



V = Vulnerabilities

S = Safeguards

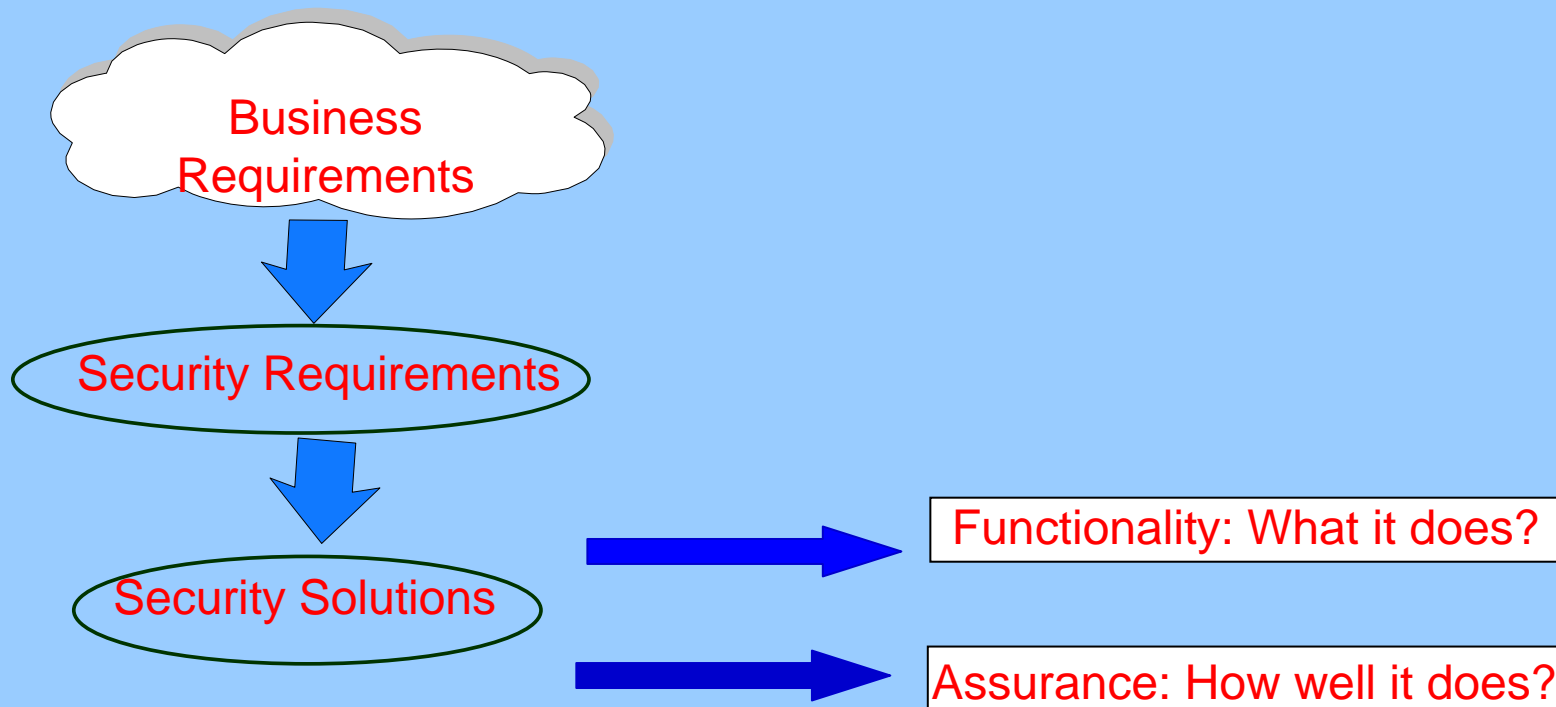
R = Risks

RR = Residual Risk

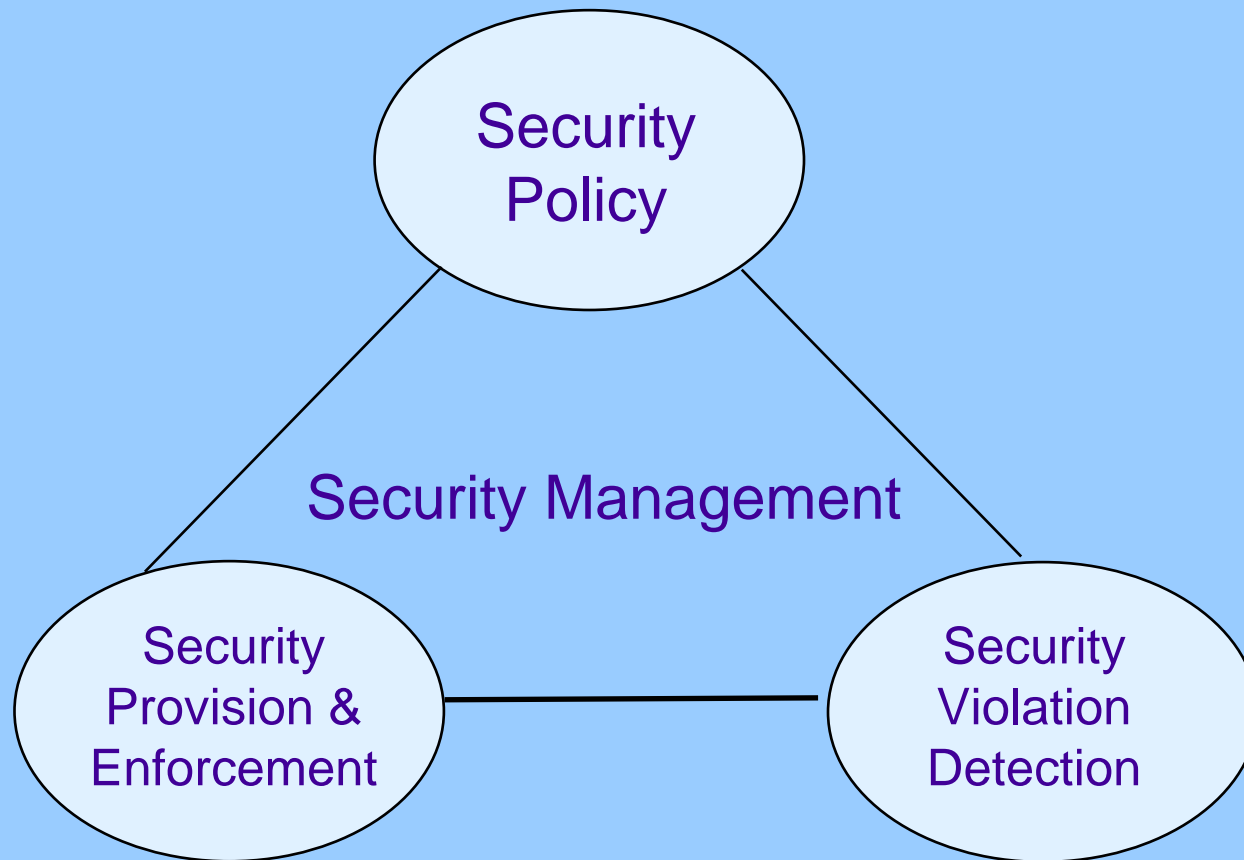
Security

- ❖ Challenges
 - ❖ Pervasiveness
 - ❖ Operating Systems, Networks and Protocols,
 - ❖ Databases, Applications, Hardware, Users
 - ❖ Multiple Security Models
 - ❖ Multiple Platforms
 - ❖ Different Vendors
 - ❖ Different Security Policies
 - ❖ Several Security Standards
 - ❖ Interoperability
- ◆ Some Consequences
 - ❖ Research : Different parts of the puzzle
 - ❖ Interconnections → Overall System
 - ❖ Organizational Challenges

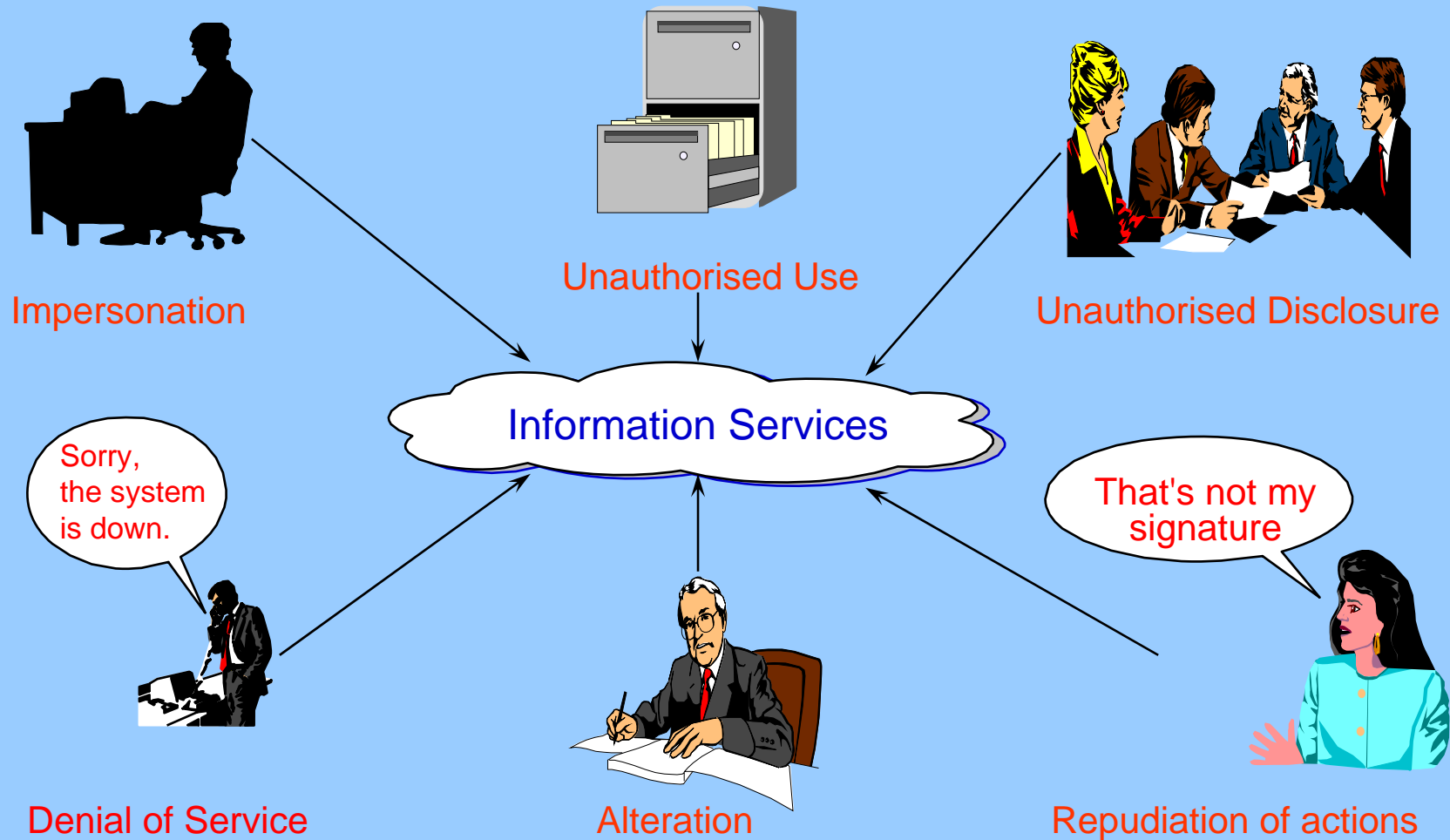
Security



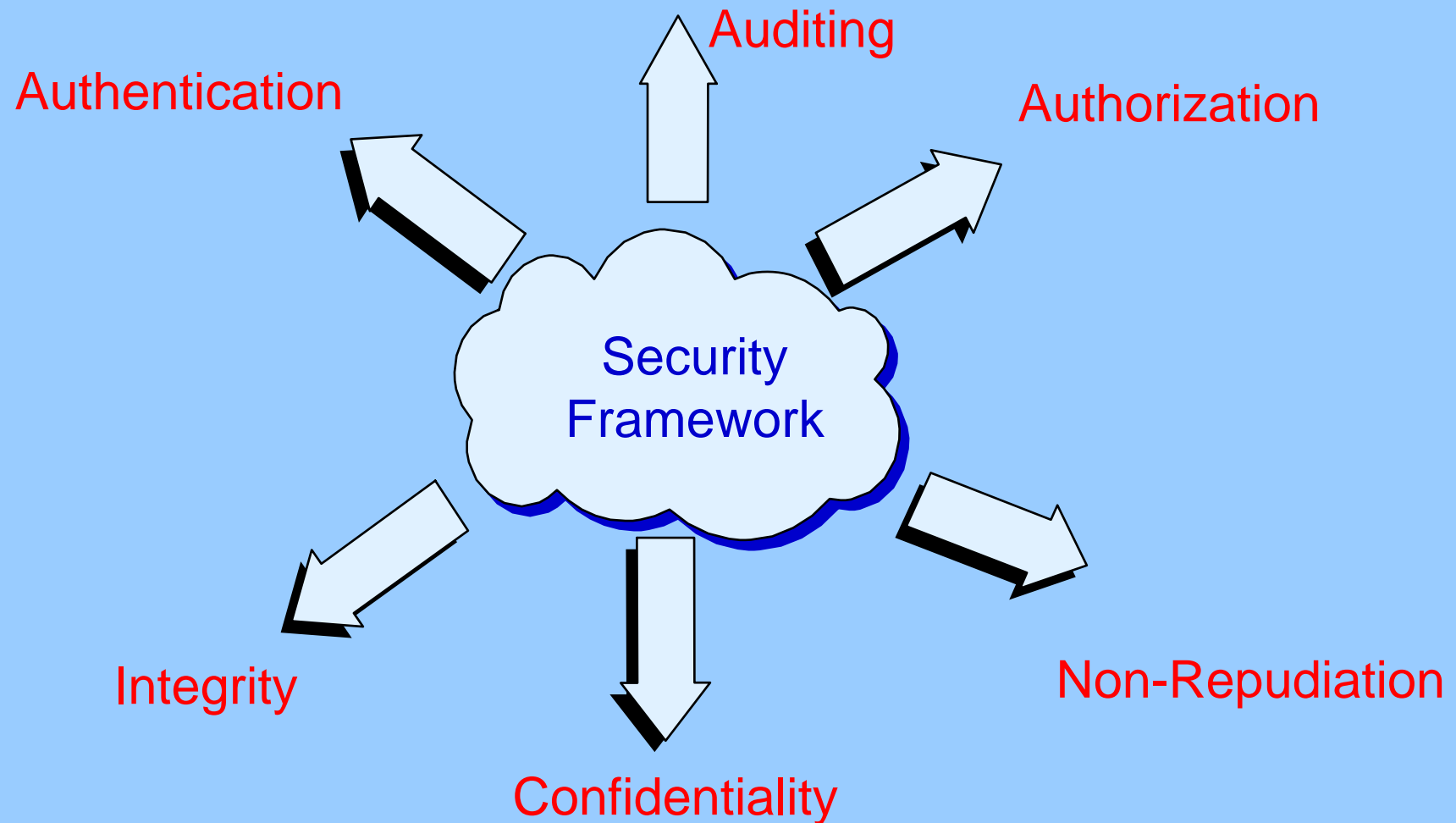
Security Philosophy



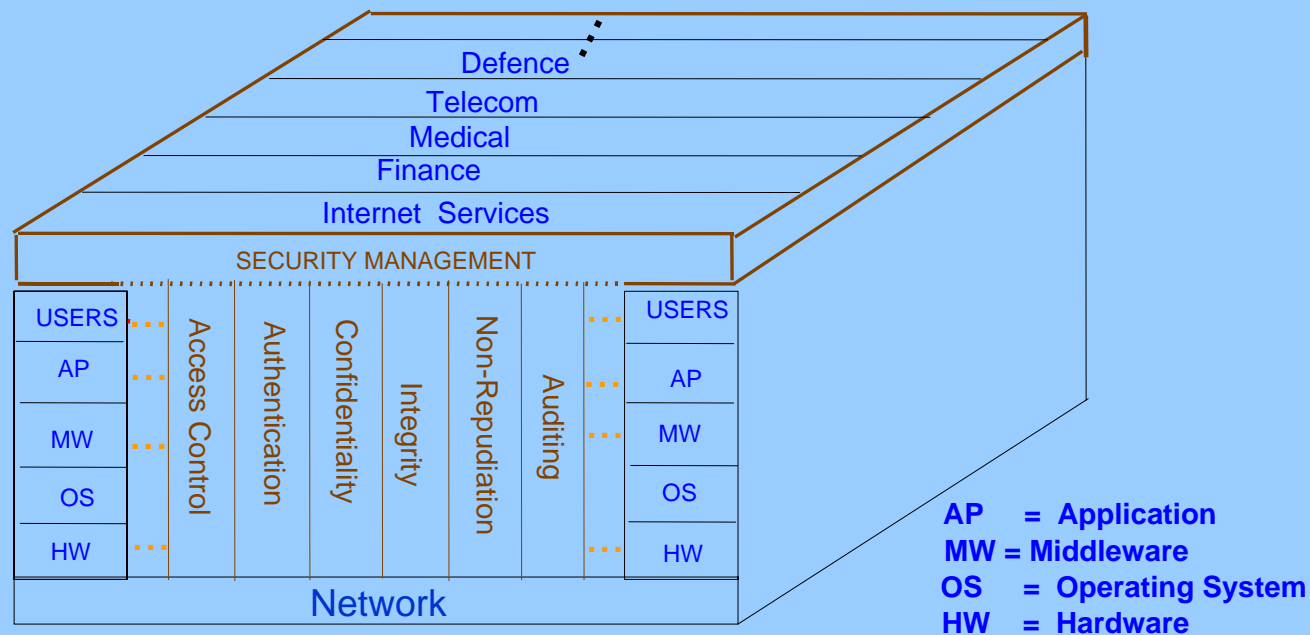
Distributed System Security Threats



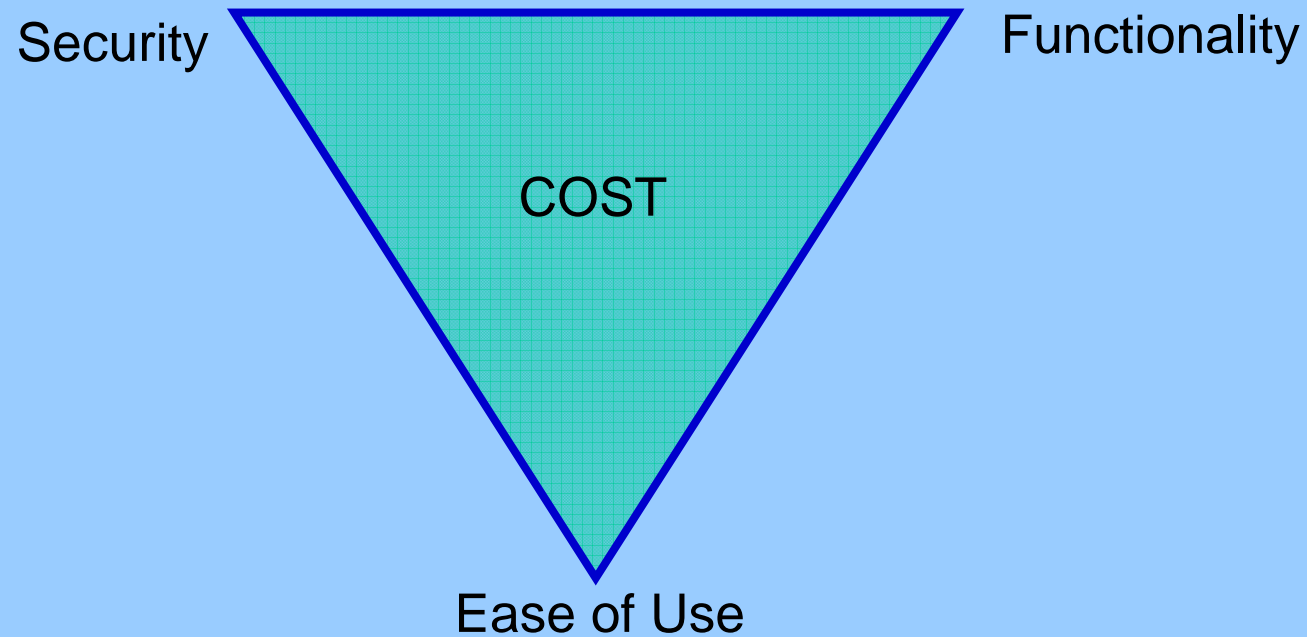
Distributed System Security Services



Distributed System Security



System Tradeoffs



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
- ❖ Several Notions
 - ❖ Luhman: “we as humans would not be able to face the complexity of the world without resorting to trust”
 - ❖ Sociology: ‘the very absence of conscious considerations is what characterizes trust’
 - ❖ Trust : “It will not harm me”, “No Surprises”
 - ❖ Trust : From a malicious point of view
 - ❖ 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

- Trust
 - Entities with free will (type A) and without free will (type B)
 - Trust in type A is the belief that it will behave without malicious intent
 - Trust in type B is the belief that it will resist malicious manipulation by a type A entity.
- Computing
 - Software agents and computing machines can be thought of as representatives of the human owner(s)
 - If so, special case → focus on type B trust
 - Develop models and mechanisms for reasoning about resisting manipulation by type A -- detecting and preventing such manipulations.

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 fulfilling of commitments
 - Availability : Resources

within a context

Trust

- ❖ Several Characteristics
 - ◆ Transitivity
 - General
 - Within a Context
 - ◆ Action-Dependent
 - ◆ Time-Dependent
 - Non Monotonic
 - ◆ Trust Building, Trust Destroying
 - ◆ Trusted Authorities
 - Multiple

Trusted and Trustworthiness

- ◆ Some Subtleties in Terminology
 - ❖ If a secret service employee is observed in a toilet at an airport selling material to a foreign diplomat, then assuming the operation is not authorized, we can describe him as “trusted and not trustworthy”
 - ❖ Trusted → “Failure can break the security policy”
 - ❖ Trustworthy → “A system that won’t fail”

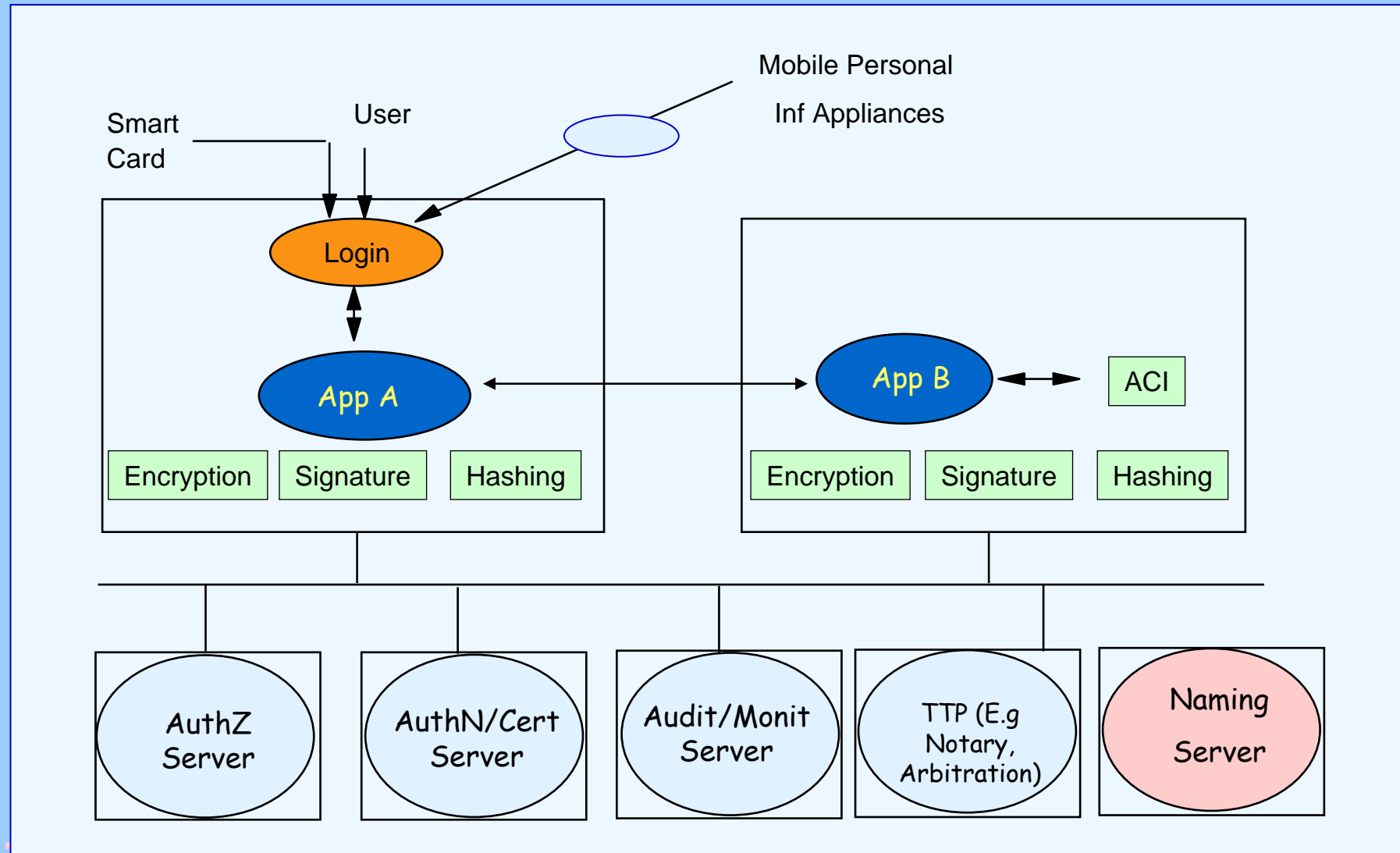
Trust and Trustworthiness

- ◆ Trust: *Subjective* probability by which the trustor expects that the trustee performs a given action on which the trustor's welfare depends
- ◆ Trustworthiness: *Objective* probability by which the trustee performs a given action on which the welfare of the trustor depends
- ◆ Misplaced trust is when trust is greater than the trustworthiness → increased risk
- ◆ Misplaced distrust is when trustworthiness is greater than trust → loss of opportunities

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”
 - ❖ Trusted Computing Base (TCB)
 - ❖ “totality of protection mechanisms needed to enforce the security policy”
 - ❖ Hardware and Software
 - ❖ “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

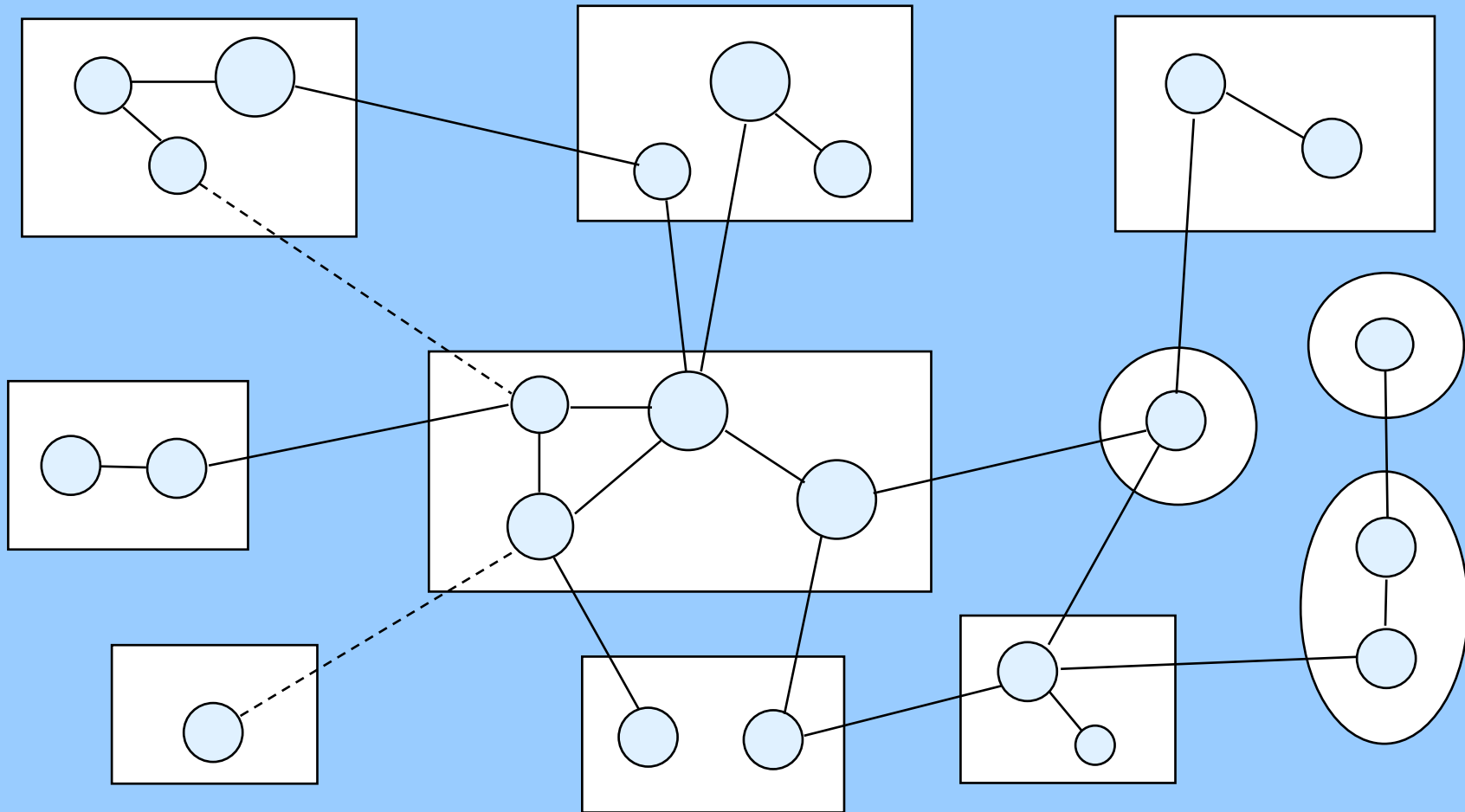
Security and Trust in Distributed Systems



Security and Trust in Distributed Systems

- ❖ Some Examples of Trust
 - ❖ Trustor “trusts” a trustee entity (e.g. application) 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. Authz/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



Mobility and Trust

❖ Mobility

❖ Software Mobility

- ◆ Programs may come from unknown 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

Mobility and Trust

- ❖ Proliferation of barriers and problems involved in crossing them
 - ◆ Programs cross administrative Domains
 - ◆ Domains may have different of levels of trust
 - Programs may not choose to perform certain actions in certain domains
 - Different programs coming from the same user but created at different sources, may need to be treated differently
 - Same programs coming from the same user passing via different domains may need to be treated differently.

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 Platforms

- ❖ TCPA/TCG view of Trust
 - ❖ Something is trusted “if it always behaves in the expected manner for the intended purpose”
- ❖ TCPA/TCG: 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”

Trusted Computing Platforms

- ❖ Basic Idea
 - ❖ A trusted party assesses the platform and declares that if the measurements for the platform are such and such, it can be trusted for such and such purpose.
 - ❖ Measurement Process
 - ❖ Storage and Reporting of measurements
 - ❖ Matching with standard expected values
- ❖ PC
 - ❖ BIOS Boot Block starts the measurements and stores the results in Trusted Platform Module (TPM) – tamper resistant chip. This is compared with the expected values
 - ❖ This happens for all loading of software and before their execution
 - ❖ BIOS → OS Loader → OS Kernel → Applications

Trusted Platform and Applications

- ❖ PC booted into a known state with an approved combination of hardware and software (e.g. whose licences have not expired).
- ❖ Now TPM can certify to third parties about the state of the PC.
 - ❖ E.g. certifying that the PC is currently running an authorised application program X
- ❖ Third parties can now have secure information transfer with the platform -- information protected with a key which is in turn protected by TPM key.
- ❖ TPM releases the appropriate key to the authorised application program X.

Some Issues with Measurements

- ❖ Measured Values (hash) → Platform Configuration Registers (PCRs)
 - ❖ Many components
 - ❖ Many revisions for each component: Updates/Patches
 - ❖ Fixed set of PCRs: 15 PCRs (e.g. for a PC)
 - ❖ Different ways of concatenation
- ❖ Policy expression difficult with binary hash values
 - ❖ Not possible to guess all possible states/values
 - ❖ Cumbersome
- ❖ Privacy
 - ❖ Challenger could learn exact implementation details/vulnerabilities

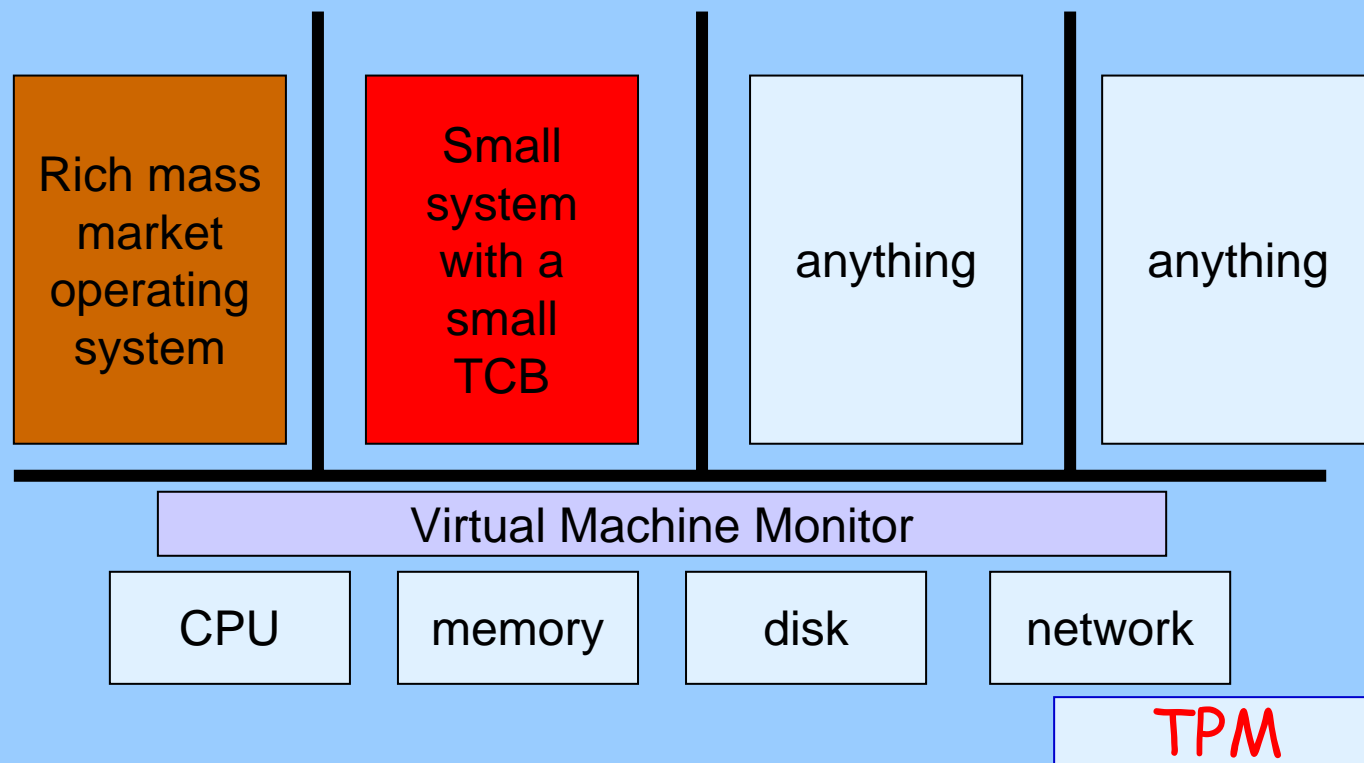
Property based Attestation

- ❖ Using properties instead of hash values for attestation of platforms
- ❖ Properties
 - ❖ Higher Level Abstraction
 - ❖ Many States to one Property mapping
 - ❖ States may change but relevant properties should not
 - ❖ Which state changes are security relevant?
- ❖ Granularity of Properties
 - ❖ Platform level properties
 - ❖ Coarser Granularity, Higher level of Privacy
 - ❖ Component level Properties
 - ❖ Finer Granularity, Lower level of Privacy
 - ❖ Combination

Challenges with Property Specification

- ❖ What properties are useful and relevant and how to define them?
 - ❖ Security Properties
 - ❖ Presence of certain security attributes and constraints
 - ❖ Absence of vulnerabilities
 - ❖ Certification standards such as ISO
 - ❖ Non-security properties
 - ❖ Correctness, Reliability
- ❖ Semantics of Properties
 - ❖ Requirements → Properties
 - ❖ Composition of Properties
 - ❖ Translation between Properties
 - ❖ Different Domains: Organizations, Applications
 - ❖ Dynamic Nature of Properties
 - ❖ Temporal (Measurement time vs Query time)

Security and Trust and Virtual Machines

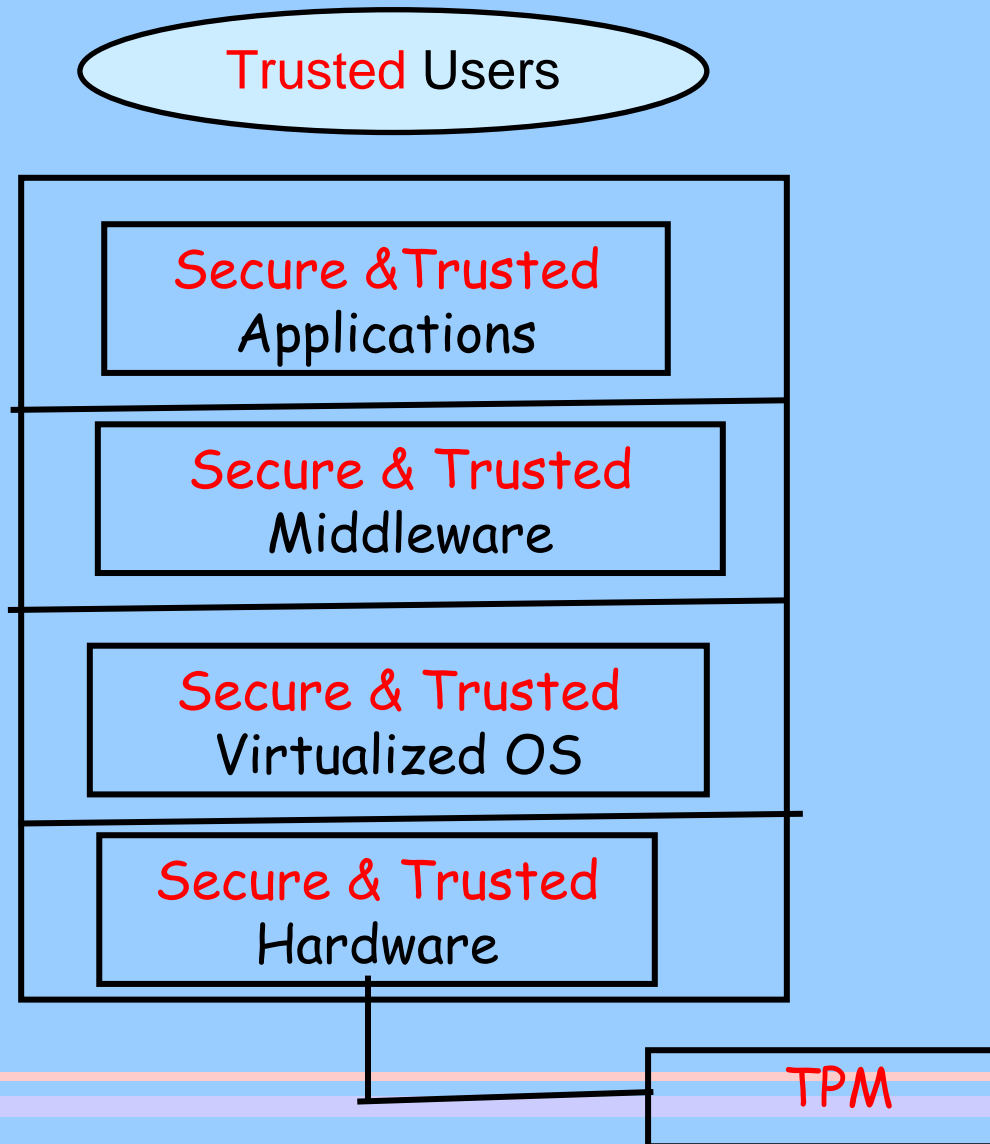


Security and Trust in Applications

- ◆ P2P Web Applications
 - ❖ User generated information content
 - ◆ Information Quality: Veracity, reliability
 - ❖ Source and author of information
 - ◆ Each user can create his or her own version
 - “There is no truth except the truth you create for yourself”

- ◆ Security, Privacy and Trust: Fundamental Challenges in P2P web Interactions
 - ❖ Who and what information do you trust
 - ❖ Confusing authorship and audience
 - ❖ Issues of authorship and ownerships
 - ❖ Giving end users privacy they can ‘control’ and security they can ‘understand’.

Trust Enhanced Secure Applications



Security and Trust

- ◆ Tour of some Trust Concepts in the Secure Computing World
- ◆ Current Research Projects at INSS@MQ
 - ❖ Secure Distributed Computing
 - ◆ Trust Management in Distributed Systems
 - ◆ Distributed Authorization in Web Services
 - ◆ Secure Virtualization
 - ◆ Property based Attestation in Trusted Platforms
 - ◆ Trust Enhanced Security in Mobile Agent based Systems
 - ❖ Secure and Trusted Network Infrastructures
 - ◆ Counteracting Security Attacks in Network Infrastructures
 - ◆ Secure and Trusted Mobile Ad hoc and Sensor Networks
 - ❖ Security and Trust in Peer to Peer Web based Applications
 - ◆ Trust Model for Web Interactions
 - ◆ Privacy Enhanced Distributed Applications
 - ❖ Formal Modelling and Analysis of Security Properties
 - ◆ Security Policy based Reasoning

Trust Models

- ❖ Trust Models
 - ❖ “Hard” and “Soft” Trust
 - ❖ Notion of Hybrid Trust

- ❖ Design of Trust Enhanced Secure Systems
 - ❖ Explicit use of Trust to enhance Secure Decision Making

- ❖ Application to Mobile Software Agent based Systems
 - ❖ Trust Management Architecture

Trust Enhanced Security

- ❖ Hard Trust
 - ❖ Trust beliefs derived from concrete security mechanisms
 - ❖ E.g. Authentication Trust
 - ❖ Belief on the trustworthiness of public keys derived from certificate digitally signed by a certificate authority binding the key to an entity
 - ❖ Characterized by “certainty”
 - ❖ Underlying belief is that the certificate authority is “trusted” in that it is honest and competent in correctly authenticating the user before signing the user’s public key.

Trust Enhanced Security

❖ Soft Trust

- ❖ Trust derived from social control mechanisms and intangible information such as reputation, experiences and cooperation
 - ❖ Beliefs not based on concrete security credentials such as authentication and privilege attribute certificates
 - ❖ Characterized by “uncertainty”
 - ❖ Dependent on past behaviours
 - ❖ Often involves recommendations from multiple entities (“web of trust”)
 - ❖ Progressively tune the beliefs over time

❖ Trust Saturation

- ❖ Long history of positive experiences
- ❖ A malicious entity cooperating for a certain period and accumulating high trust and then defaulting on a critical transaction

Trust Enhanced Security

❖ Hybrid Trust

- ❖ Combining “Hard” and “Soft” Trust
- ❖ Model more effectively the dynamic changes in trust that arise due to changes in behaviour of users and applications
- ❖ Improved Secure Decision Making and Optimizing Risk

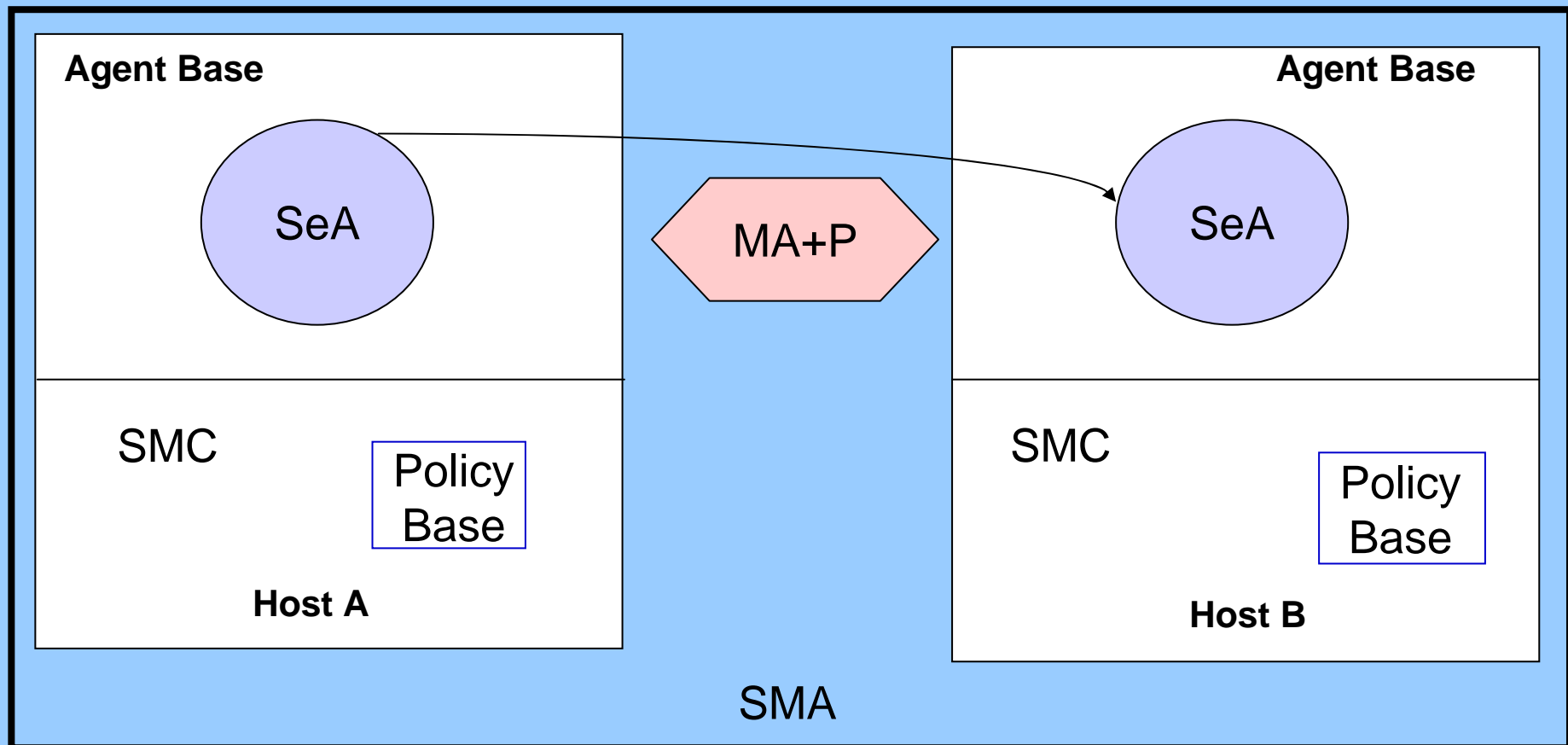
❖ Trust Management System based on Hybrid Trust

- ❖ Trust Management Architecture
 - ❖ Locating and Gathering Trust Information, Evaluating Trust, Consuming Trust (in Decision Making) and Updating Trust
- ❖ Applications to Mobile Software Agents, Web Services, Mobile Ad hoc Networks and Peer to Peer Applications

Mobile Agents and Security

- ❖ Mobile Agents are autonomous software entities that move from place to place and interact with each other and the environment to achieve their own goals on behalf of their owners
 - ❖ Executable Code
 - ❖ State
- ❖ Security
 - ❖ Agent attacking the Agent Base Environment
 - ❖ Agent Base Environment attacking the Agents
 - ❖ Agents attacking each other
 - ❖ Attacks against Agents during Network Transfer

Security Enhanced Mobile Agents



Security Enhanced Mobile Agents

- ❖ Security Enhanced Mobile Agent : Agent + Passport
 - ❖ Identifier
 - ❖ (SeA Identifier, Creator-Principal Certificate, Creator-SMC Certificate, Timestamp, Lifetime)
 - ❖ Privilege-Token
 - ❖ {<IdentifierNo,Privilege,Timestamp, Lifetime>}
 - ❖ Agent_Code
 - ❖ (Security Code, Application Code)
 - ❖ Data_Store
 - ❖ (Data, Propagation Path)
 - ❖ Security_Tags
 - ❖ (Security-Tag-C, Security-Tag-S)

Security Enhanced Mobile Agents

- ❖ Authentication
 - ❖ Principal which sent the Agent
 - ❖ Principal which created the Agent
 - ❖ Authentication of the Agent Base
- ❖ Authorization
 - ❖ Privileges of the Creator of the Agent
 - ❖ Privileges of the Sender of the Agent
 - ❖ Policy Base at the Agent Base
- ❖ Delegation of Privileges
 - ❖ Agent acts on behalf of Sender and/or Creator
- ❖ Non-Repudiation
 - ❖ Agent Base : Agent did such and such action at this time
 - ❖ Agent: Such and such an action was done at the Agent Base
- ❖ Secure Communication

Security Enhanced Mobile Agents

❖ Authorization

- ❖ SeA's Privileges and SMC's Policy Base
- ❖ Language Based Approach
- ❖ Variety of Access Policy Rules based on
 - ❖ Agent Identity
 - ❖ Agent and Agent Base Identities
 - ❖ Creator Principal and Agent Base
 - ❖ Creator and Sender Principals
 - ❖ Domain
 - ❖ Privileges
 - ❖ Attributes
 - ❖ Combination of All these

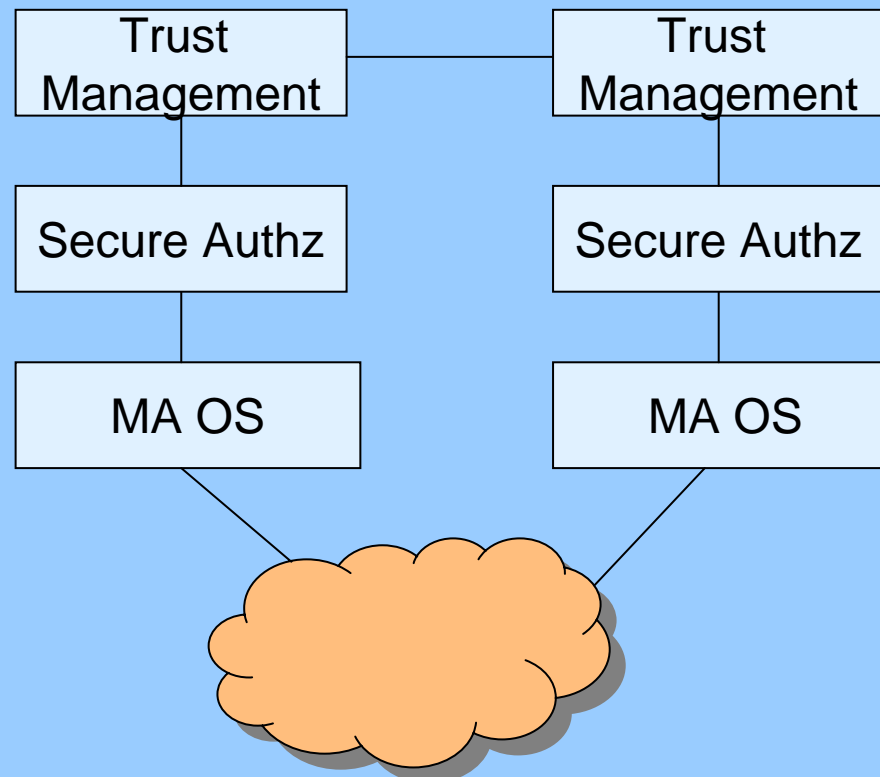
Security Enhanced Mobile Agents

- ❖ If all checks successful, SeA executed
- ❖ Results stored in the Data Store
- ❖ Integrity and Origin Authentication of Results
 - ❖ Hashed Digest of Results and Timestamp Signed using the Private Key of the SMC of the Target Agent Base that is providing the service
- ❖ If Confidentiality of Results needed
 - ❖ Target Agent Base SMC generates Secret Data Key.
 - ❖ Secret Data Key encrypted using Public Key of the Client that requested the operation
 - ❖ Secret Data Key used to encrypt results

Mobile Agent based Services Scenarios

- ❖ Single Hop Mobile Agent : Moves from one host to another and performs tasks
 - ❖ Agent returns back or returns results to originator in the form of messages
- ❖ Roaming Mobile Agents : Moves from host to host performing tasks.
 - ❖ Agent stores results until it returns to the originator in the end or sends results back time to time
- ❖ Applications
 - ❖ Flight Finder
 - ❖ Electronic Auction

Trust Enhanced Secure Mobile Agents



Mobile Agents Security and Trust

- ❖ Mobile Agent Issues
 - ❖ Prevention of mobile agent tampering by host
 - ❖ Prevention of unauthorized tampering of the host by the agent
- ❖ Types of Trust
 - ❖ Authentication Trust
 - ❖ Authorization at the host
 - ❖ Code Trust
 - ❖ Authorization at the host
 - ❖ Execution Trust
 - ❖ Itinerary Composition

Trust Enhanced Secure Mobile Agent System

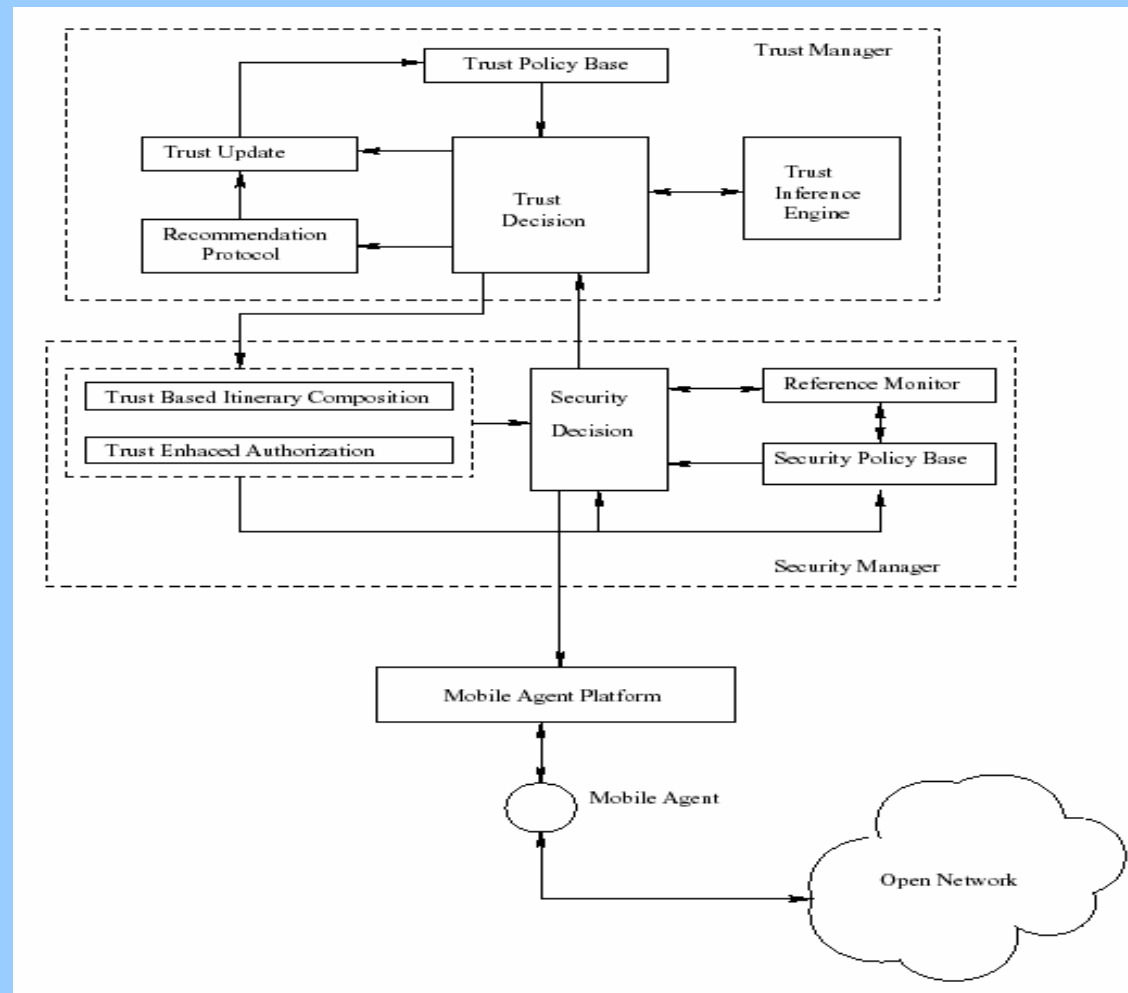
❖ Trust Enhanced Security Solution

- ❖ Hybrid Trust Model : Combining “Hard” and “Soft” Trust
- ❖ 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
 - ❖ Trust based Itinerary → Execution Trust (Mobile Code Security - Malicious Host Problem)
 - ❖ Trust based Authorization → Code Trust (Host Security - Malicious Agent Problem)

A Formal Trust Model

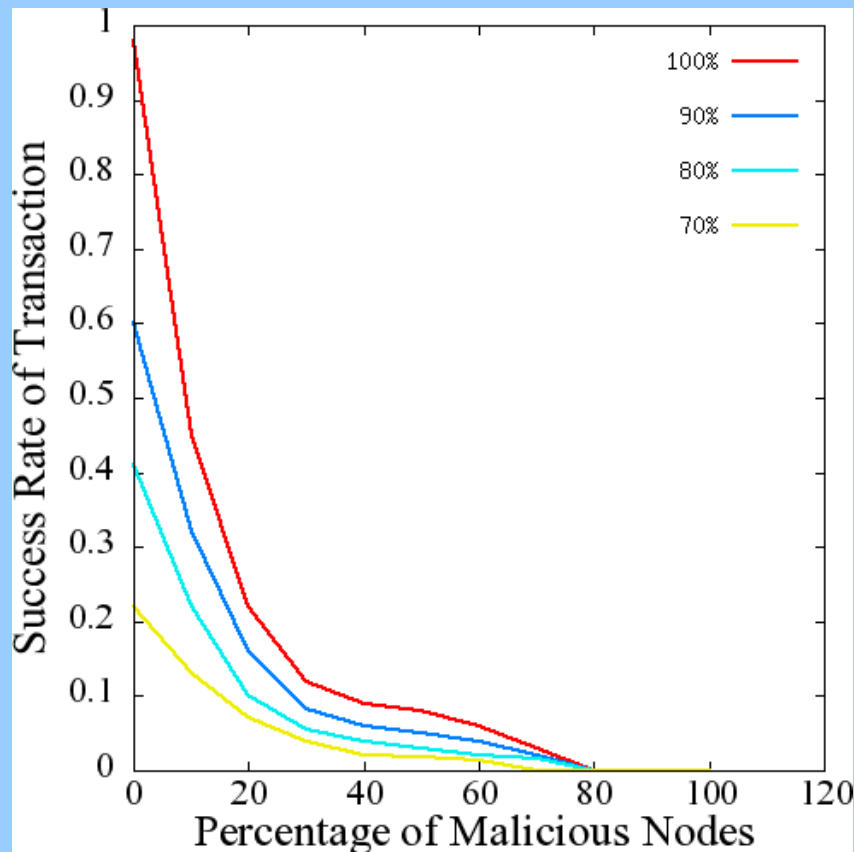
- ❖ Trust Relationship : $\langle P; Q; C; T; D; t; v; p; n \rangle$
 - ❖ P and Q are the subset of the set of all the entities in a mobile agent system.
 - ❖ C is defined as the set of {auth, exe, code}, denoting trust classes for authentication, execution and mobile code.
 - ❖ T is the set of {direct, recommended, derived}.
 - ❖ D is the set of domains of $\{ \langle dn; dt \rangle \}$, where dn denotes name of the domain and dt denotes the type of the domain belonging to {intra; inter}
 - ❖ t is the time constraint \rightarrow validity
 - ❖ v is the trust evaluation on this trust relationship
 - ❖ p is the number of positive experiences associated with this trust relationship
 - ❖ n is the number of negative experiences associated with this trust relationship

Trust Enhanced Security Architecture

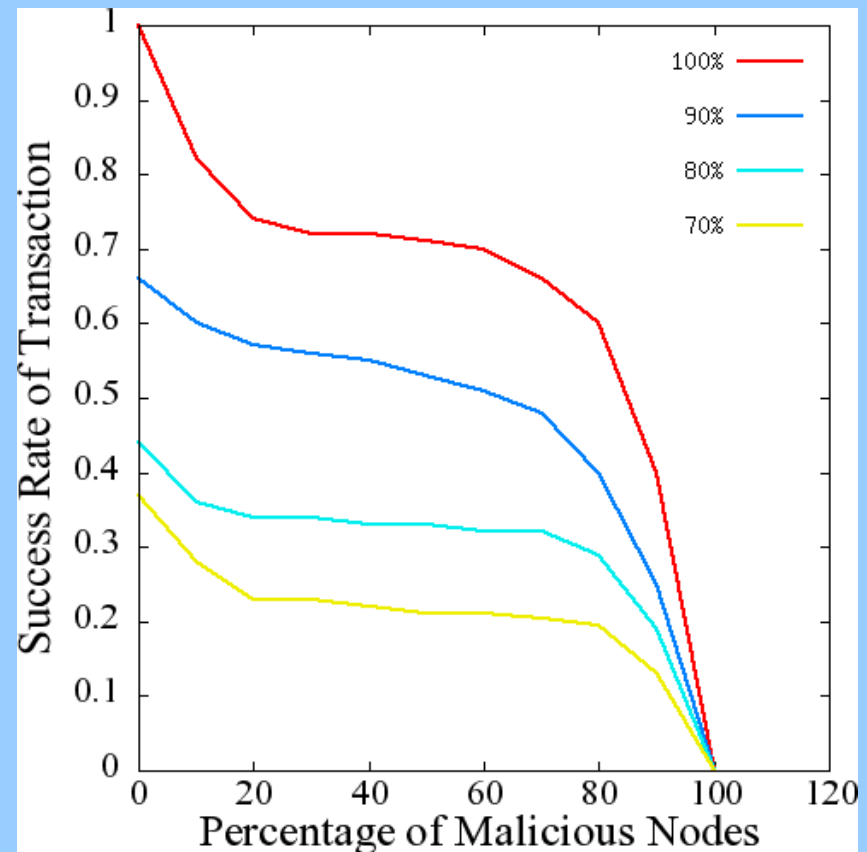


Agent Protection

Successful Transaction Rate



Without Trust



With Trust

Successful Transaction Rate for Agents

- ❖ STR : Ratio of successful transactions to total transactions by agent
 - ❖ Used as a metric for measuring agent protection performance

- ❖ Without trust model, agent protection is poor which is marked by high susceptibility to maliciousness of the system
 - ❖ STR decreases sharply as the percentage of malicious hosts increases and as the degree of maliciousness increases.

- ❖ With trust model, agent protection is enhanced significantly which is indicated by high resistance to maliciousness of the system
 - ❖ STR stays high for a greater part of the BP and PMH ranges.
 - ❖ **BP – Behaviour Probability: Prob good hosts behave good and bad hosts behave bad**
 - ❖ **PMH – Percentage Malicious Hosts: No of bad hosts over the the total number of hosts percentage.**

Some Challenges in Trust Enhanced Security

- ❖ Hybrid Trust Models for Distributed Systems
 - ❖ E.g. Combining Credential based Hard Trust with Reputation based Trust
 - ❖ Formal Semantics for Trust Models
- ❖ Trust Policies
 - ❖ Specification Language for Trust Policies
 - ❖ Trust Negotiation
- ❖ Trust Management Architecture
 - ❖ Locating Trust, Evaluating Trust, Consuming Trust
- ❖ Integration of Trust with the Distributed Infrastructure
- ❖ Trust Enhanced Secure Distributed Applications

Concluding Remarks

- ICT Context
 - Systems of Systems
- Security and Trust
 - Greater focus on security and trust properties and context aware behaviour in systems design
- Trust in Security Technologies
 - Trusted Stack
 - Trust Enhanced Security