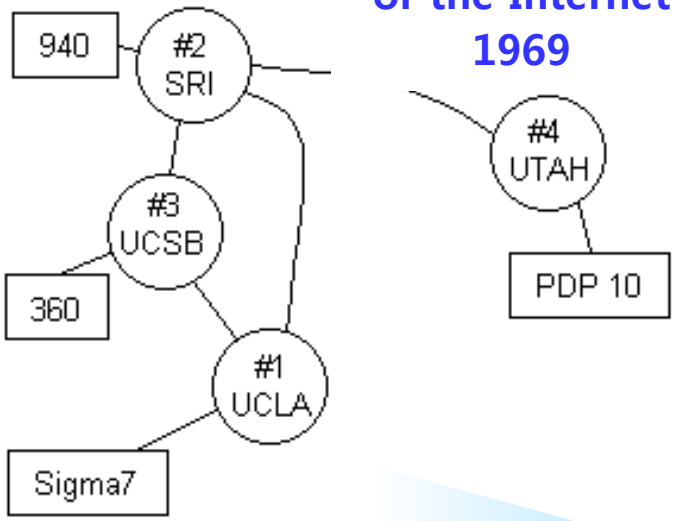
ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 2
Geneva, Switzerland
1 July 2016

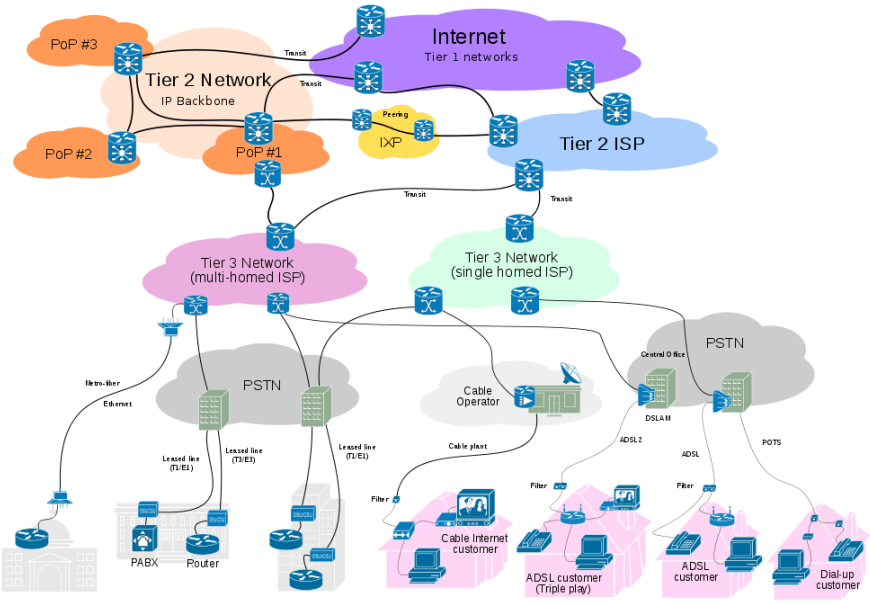
Trustworthy Communication Infrastructure:
Principles and Framework

Woojik Chun
Invited Researcher, KAIST
woordine@kaist.ac.kr

Introduction: The Internet is growing



The beginning of the Internet 1969



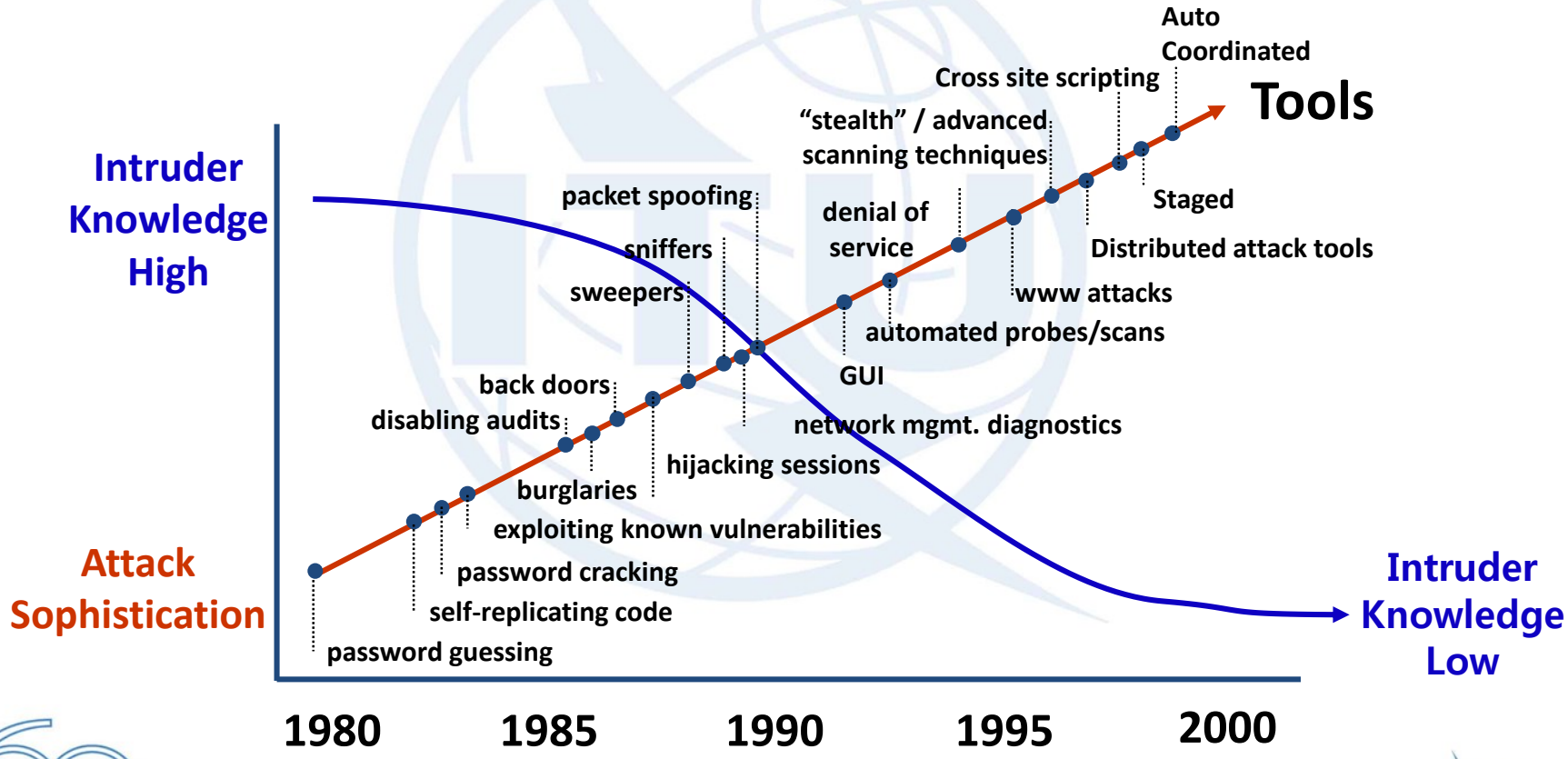
Know each other
Trustworthy envi
No concern on se

the more connectivity,
the less secure

Unknown public
Untrusty environment
Responsible to its own fate

Introduction: Malicious Cycle

- **Endless Battle of "Spear and Shield"**
  - ☞ ***Security is never secure enough***



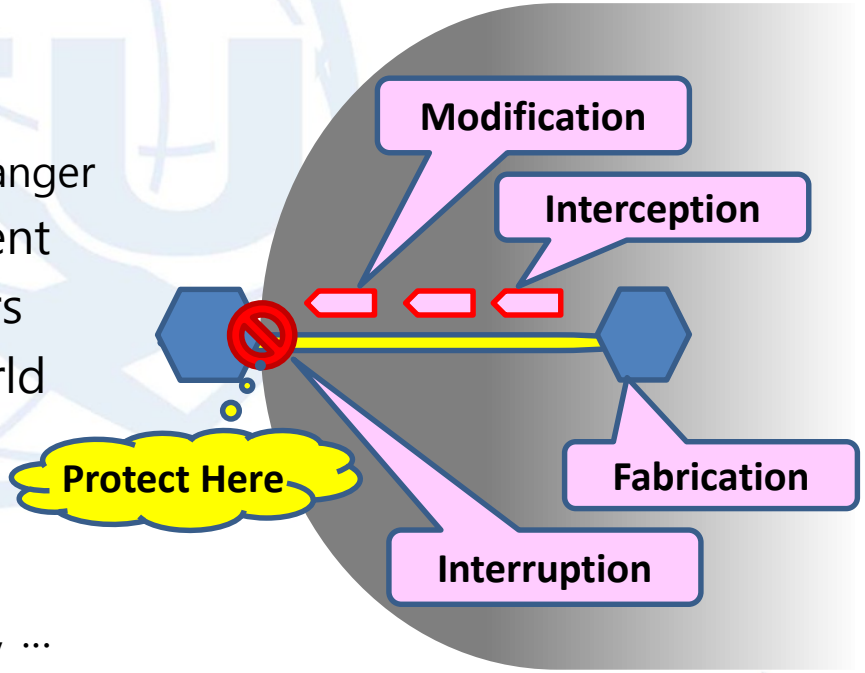
http://www.cert.org/archive/ppt/cyberterror.ppt

Security: What is Security ?

- **Definitions**
  - protection from risk and danger
  - freedom from doubt, anxiety, or fear
- **Why Security ?**
  - The Internet concerns only connectivity but not security
    - Everyone can send packets to every others
  - No responsibility on senders, but only receivers are responsible
  - No confidence on the network and everyone on the network
- **Examples of Threats and Countermeasures**
  - Packet Sniffing ➔ Encryption (SSH, SSL, HTTPS)
  - Unauthorized access to network ➔ Firewall
  - DoS (Denial of Service) ➔ IDS (Intrusion Detection System)
  - TCP Hijacking ➔ IPsec, VPN
  - Identity theft ➔ PKI

Security: The Model based in Suspicion

- **End Systems**
  - View the external world as a hostile environment
  - Consider all communications to be suspicious
  - Should protects itself against the whole external world
  - Don't know how secure is secure enough
- **Security Model**
  - Based on doubt, anxiety, fear
    - that may not be actual risk or danger
  - No confidence on the environment
  - No trust on communicating peers
  - Self-protection from external world
  - Deployed at endpoints
    - Network : IPsec
    - Transport(session) : SSL/TLS
    - Application : Secure Mail, HTTPS, …

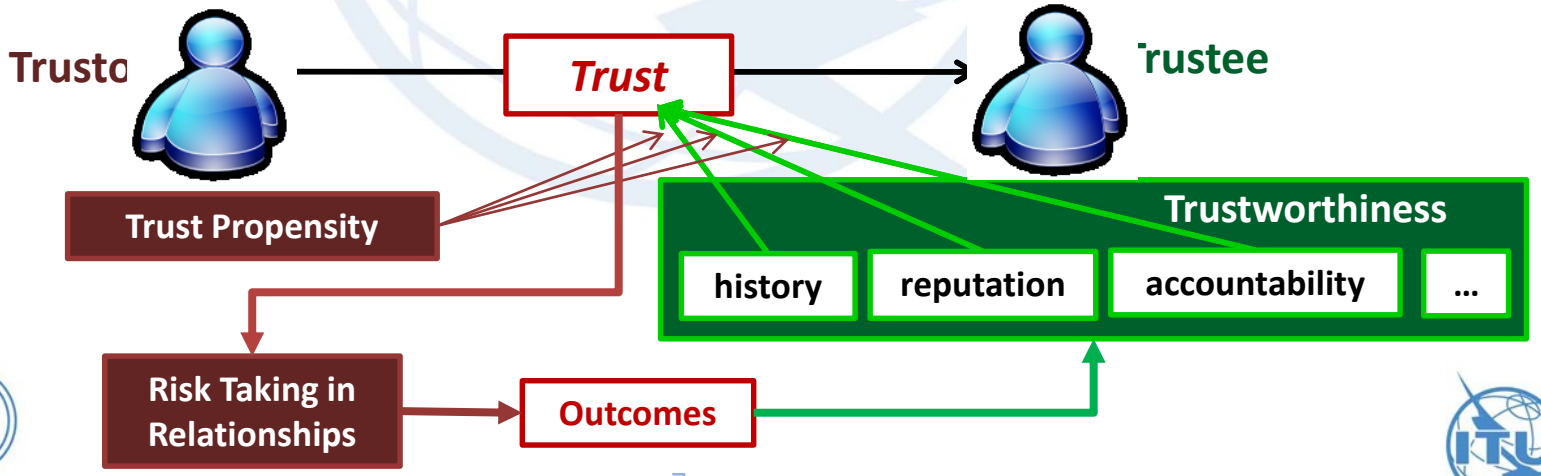


Trust: What is Trust ?

- **Many definitions on Trust**
  - **Johnson-George and Swap (1982)**
    - willingness to take risks may be one of the few characteristics common to all trust situations."
  - **Kee and Knox (1970)**
    - willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.
  - **Wikipedia**
    - One party (trustor) is willing to rely on the actions of another party (trustee)
  - **Note that**
    - Trust is not taking risk per se, but rather it is a willingness to take risk
    - Trust is a relationship with another identifiable party who is perceived to act and react with goodwill toward the trustor.

Trust: Integrative Trust model – *inspired from Mayer, 1995*

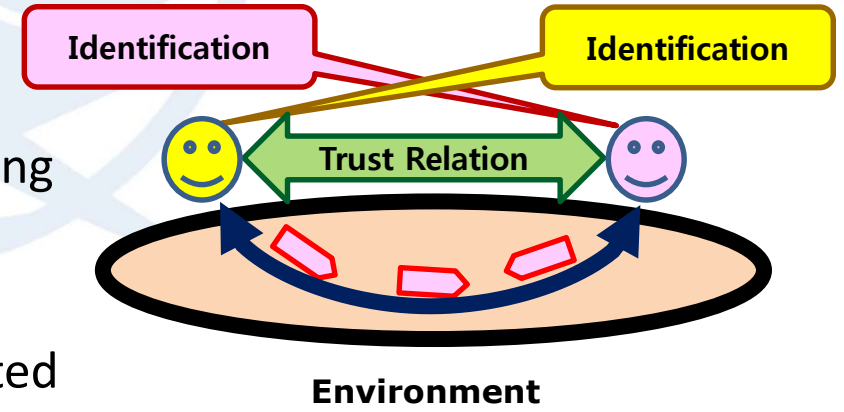
- **Trust is the relationship between two entities (tustor and trustee)**
- **Trustworthiness:** trustee's characteristics to be trusted more or less likely
  - Define the objective trustworthiness values as "$\boldsymbol{Trust\ Indexes}$"
- **Trust Propensity**: trustor's general willingness to trust others
  - Define the subjective trust propensity as "$\boldsymbol{Trust\ Metrics}$"
- $\boldsymbol{Trust_{A\rightarrow B} = func(Trust\ Metrics_A, Trust\ Indexes_B)}$
  - Trust can be defined with a value, "$\boldsymbol{Trust\ Level}$"
- **Risk Taking in Relationships:** decision to take actions
  - a function of "$\boldsymbol{Trust\ Level}$" and perceived "$\boldsymbol{Risk\ Level}$" of the actions



Trust: Trust Communication Model

- **Observation**
  - An entity(trustor) must identify a peer entity(trustee)
  - The trustor makes trust relation with the trustee (with ***trust level)***
    - based on ***trust metrics*** of the trustor and ***trust indexes*** of the trustee
  - Communications as Risk Taking Relationships (RTR)
    - The trustor will engage in communications when ***trust level*** is surpassed the threshold of the ***risk level*** of the communication

- **Trust Communication Model**
  - **Identifications** of peer entities
  - **Trust relation** between communicating peers
  - **Environment** of communication in which the level of risk can be evaluated



Comparison: Security vs. Trust

- **The more trust, the weaker security**

	Trust Model	Security Model
Basis	Belief & Confidence	Doubt & Suspicion
Relationship	Binary (trustor & trustee)	Unary (self-protection)
Coverage	Limited within a context	Unlimited
Network Space	Bounded then Expanding	Unbounded then Diminishing
Risk	Willing to take	Attempt to avoid
Attacks	Prevention	Detection & Recovery
Policy	Autonomy & Accountability	Surveillance & Responsibility
Strategy	Evaluate then Accept	Monitor then Remove

Principles for Trustworthy Communication Framework

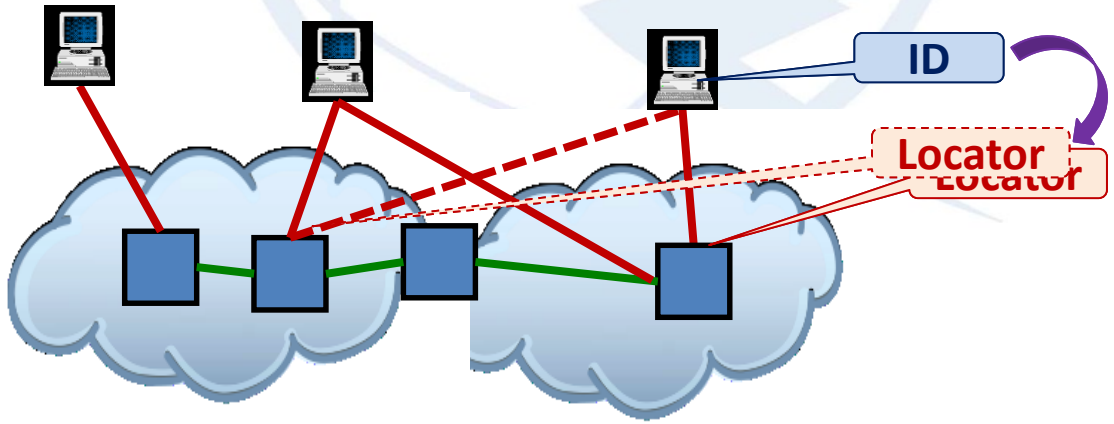
- **Separation of Concern Principle**
  - Separation of entities and communication environment
  - ID and Locator Separation
- **Principles for of Entities**
  - Identifiability and Privacy (Traceable Anonymity)
- **Principles for Communication Environment**
  - Spatial View on Networks
  - Modelling Network Spaces (Abstraction & Recursion)
  - Trust Domains
  - Accountability and Autonomy (self-governance)

Principle: Separation of Concerns

- **Separation of Purpose and Means**
  - **What is "Communication"? – from Wikipedia**
    - the purposeful activity — **Purpose**
    - of information exchange — **Semantics**
    - between two or more participants — **Entities**
  - **How is "Communication" performed**
    - Protocols to deliver — **Means**
    - Packets (messages) — **Syntaxes**
    - To the locations to reach the peers — **Environment**

Principle: Entity and Environment

- **Entity-Environment Separation**
  - Entity itself must be independent from environments
  - Entity may exist in multiple heterogeneous environments
  - Communication services can be provided by multiple environments
- **ID-Locator Separated**
  - **ID** denotes an entity unambiguously
    - **identifiable name** of an entity
  - **Locator** specifies the location in the network space (environment)
    - **locatable address** for an entity
  - An entity may exist in multiple spaces
    - bound to multiple locators

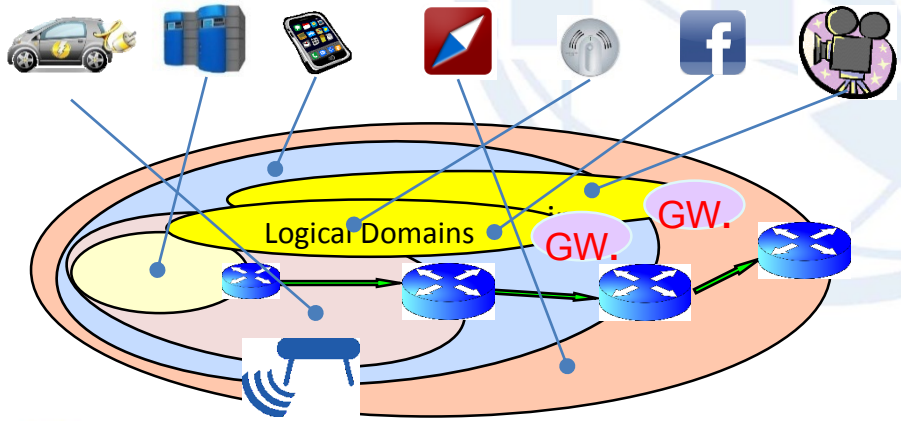


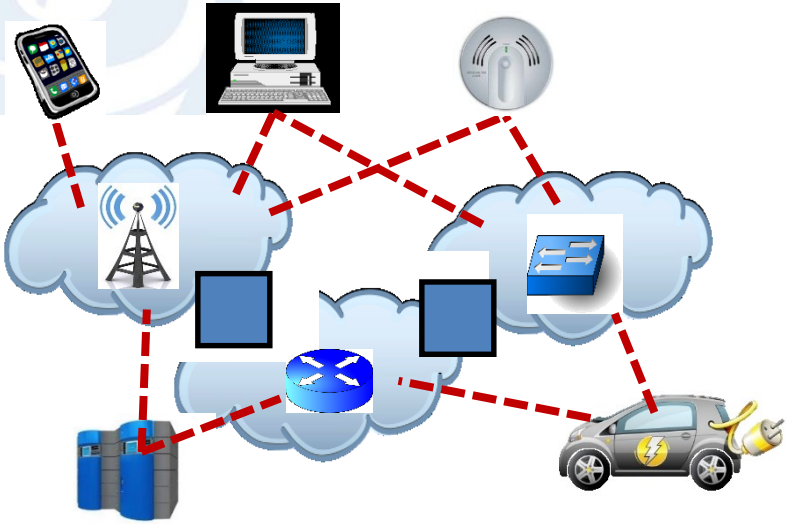
Principle: Identifiability and Privacy

- **Identification/Authentication**
  - may require some privacy sensitive information (Identities)
- **Privacy**
  - The claim of an entity to determine when, how, and to what extent information about itself is communicated to others
- **Traceable Anonymity**
  - Keep ID anonymous
    - ID may not be directly linked to identities of the entity
  - Register ID at a trust domain with identities
    - The domain is accountable to the ID (may issue a certificate)
  - Trace ID via domains that certifies the ID
    - Chain of certificates

Principle: Spatial View on Networks

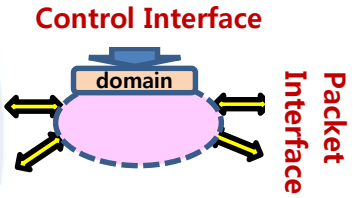
- **Horizontal Spatial View**
  - Network is viewed as collaborating spaces
  - Spatial decomposition of space (space structuring)
  - Procedures for passing spaces
  - Network Architect View
- **Polymorphic Network Spaces**
  - Enable different mechanisms in parallel
  - Enable easy deployment of new mechanisms
  - An entity selects a network space



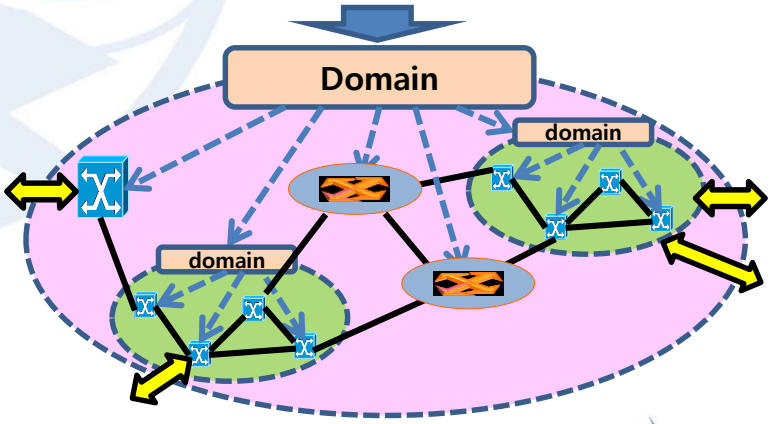


Principle: Modeling Network Spaces

- **Domain**
  - Abstraction for a network region distinguishable by a certain properties
    - Separate administration, Different media, Logical networks, Spontaneous networks, Coverage of Services, trust equivalence class …
  - Recursive Definition of Domain
    - domains can be member of another domain
  - Basic Building Blocks of network spaces
- **Domains are**
  - Units of Autonomy and Accountability
    - Intent and mechanism separation
  - Units of Insulation
    - Access via well-defined interfaces
  - Units of Federation/Composition

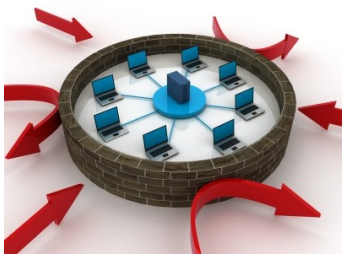


Abstract network view



Recursive network view

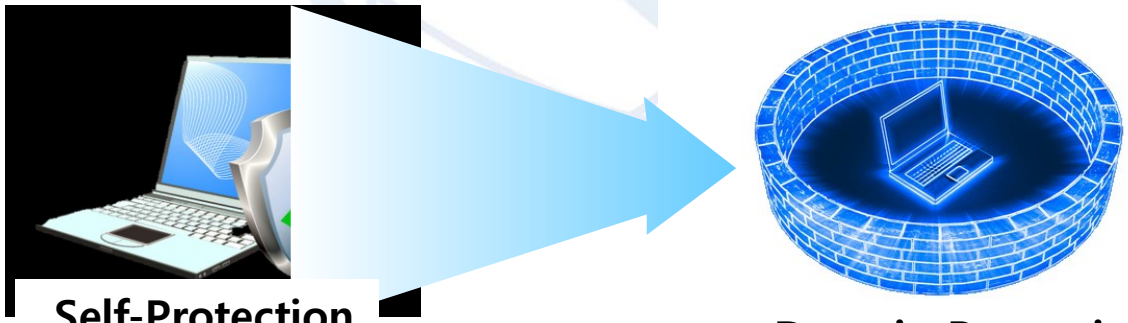
Principle: Trust Domain



- **An Autonomous Domain w.r.t Trust**
  - A group of entities in Trust Equivalence Class
    - All members within the group trust each other
    - The relation is Reflexive, Symmetric, and Transitive
  - Accepts only trusted entities/domains as members
    - Well-defined registration procedures are enforced
  - Provides safe enough intra-domain communications
    - Communication inside of the domain without security
    - Communication is protected from external attacks
  - Provides insulated external communications
    - Allows access to the domain by one of the gateways
    - Accepts only trusted inbound traffics (trust evaluation)
    - Forwards only accountable outbound traffics (with signature)

Principle: Accountability and Autonomy

- **Accountability with Autonomy (self-governance)**
  - Instead of Responsibility with Surveillance
- **Domain can select a mechanism to fulfill the intent of entities**
  - For confidentiality, the domain may use “safe wired links” or “unsafe wireless links with encryption”
- **Domain is accountable to the consequence of communications**
  - The domain administrator (or gateways) has responsibility for keeping the domain trustworthy ***(Delegated Security)***



Trustworthy Communication Framework

- **Goal**
  - Go back to **trustworthy environment** as the early Internet
  - Allow **global connectivity** as the current Internet
- **Trustworthy Communication Framework**
  - Based on the trust model
  - Starts with a trust domain where all members trust each other
  - Expend the trust domain by make trust relation with individual entity and/or other domains to achieve global connectivity

Framework : Major Technical Issues

1. How to build Insulated Domains
2. How to manage members within a domain
3. How to expand trust domains
4. How to manage trust relation with others

Framework: Issue – 1. Building an Insulated Domain

- **Domains as basic building blocks**
  - A protected, restricted region of the network
  - A single unified administration to keep the domain trustworthy
  - All members in the domain trust each other
  - Communication environment is safe enough for that trust level
- **How to build Insulated Trust Domains**
  - Determine a region of network

    *Ex: **physical domain** : host, enterprise, IDC, campus, radio access*

    ***logical domain** : VPN, Social Net, Spontaneous networks*
  - All devices and hosts in the domain must be disinfected
  - All communication links within the domain are insulated
    - By selecting reliable channels or enhancing security
  - Establish well-defined interfaces (gateways) for external access

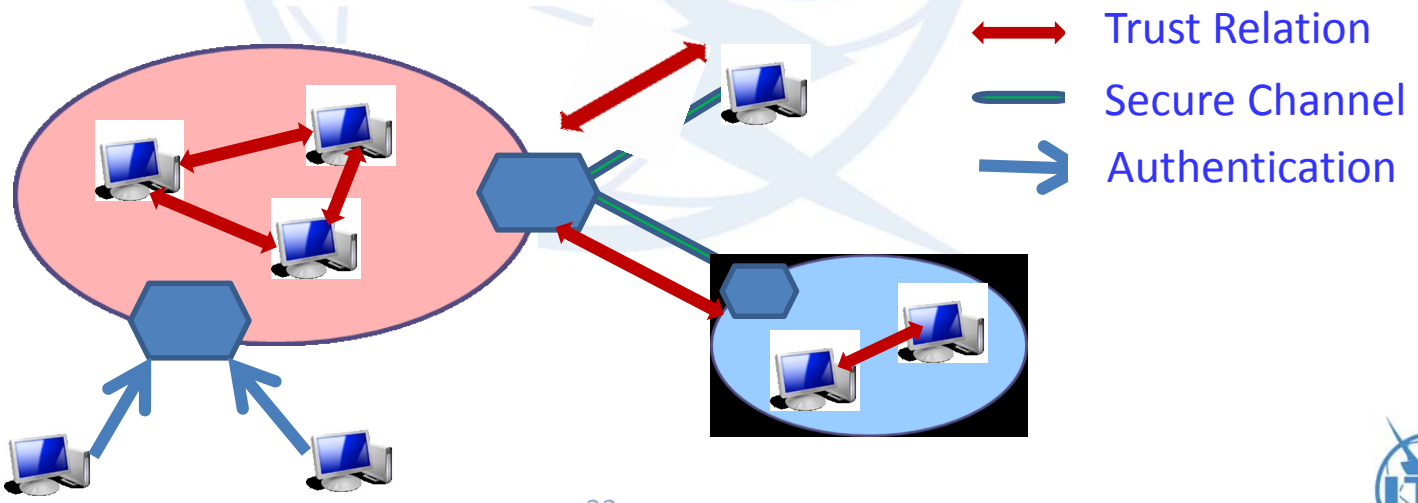
Framework: Issue – 2. Managing Trust Domains

- **How to keep Trust Domains Trustworthy**
  - Accept a new entity after verification
    - Identification
    - Trust Evaluation or Trust Contract
  - Keep the domain trustworthy
    - Periodic auditing
    - Periodic disinfection
    - Remove misbehaving entities
  - Provide safe intra-domain communication
    - Share a certain level of trust among members within the domain

- **Delegated Security**
  - Gateways enforce well-defined procedures for external communication

Framework: Issue – 3. Expanding the Trust Domain

- **Accessed from outside of the domain**
  - Via gateways through reliable Channels
  - Gateways keep “white list” of trusted IDs (of entities and domains)
    - Based on entity-level and domain-level trust relations
- **How to setup reliable channels**
  - Selecting only secure paths (ex: SCION)
  - Enforcing security functions at the channel endpoints (ex: IPsec)



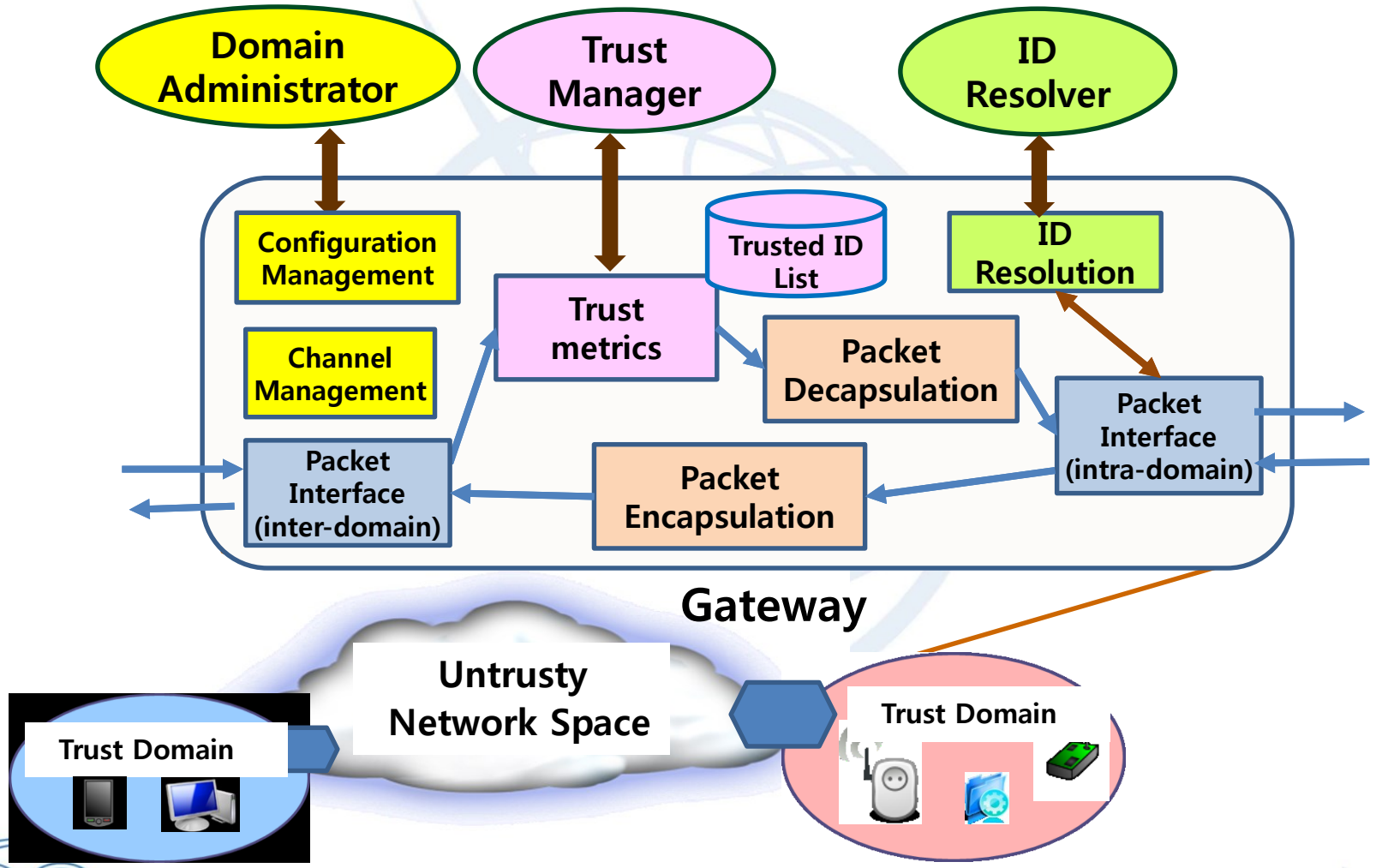
Framework: Issue – 4. Managing Trust Relations

- **Characteristics of Trust**
  - Trust is relative to some context
  - Trust is a measurable belief (***trust level***)
  - Trust is directed (normally asymmetric or sometimes symmetric)
  - Trust can be built and evolves in time.
- **Types of trust management model**
  - Policy based : Built by contracts and credential verification
  - Social Network based : Based on social relationships between peers
  - Reputation based : Evaluated by behaviors observed directly or indirectly
- **Trust management approaches**
  - Individual Initiative : each entity is responsible for its own fate
  - Global Trust : assumes centralized trust management authorities
  - Federated Trust : strategies for managing other trust domains

Framework: Major Building Blocks

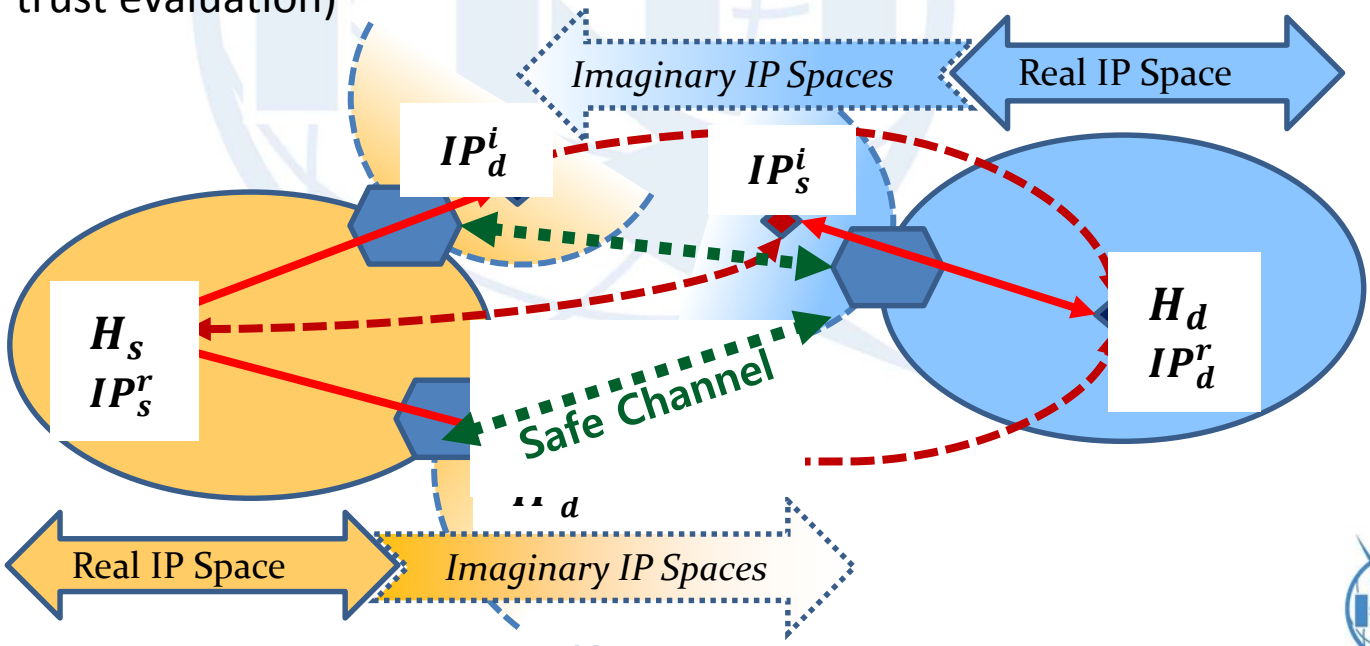
- **Domain Administrator**
  - Domain Configuration
  - Registration and Revocation of members of domain
- **ID resolver**
  - Mapping ID to Domain Specific Locator
- **Trust Manager**
  - Trust Evaluation on Entities and Domains (with ID)
- **Gateway** (of Insulated Domain)
  - Traffics across a domain boundary must pass the gateway
  - Only trusted packets are accepted
  - Only accountable traffics are forwarded
- **Channels**
  - Provide communication channel with acceptable risk level

Framework: Building Blocks- Overall



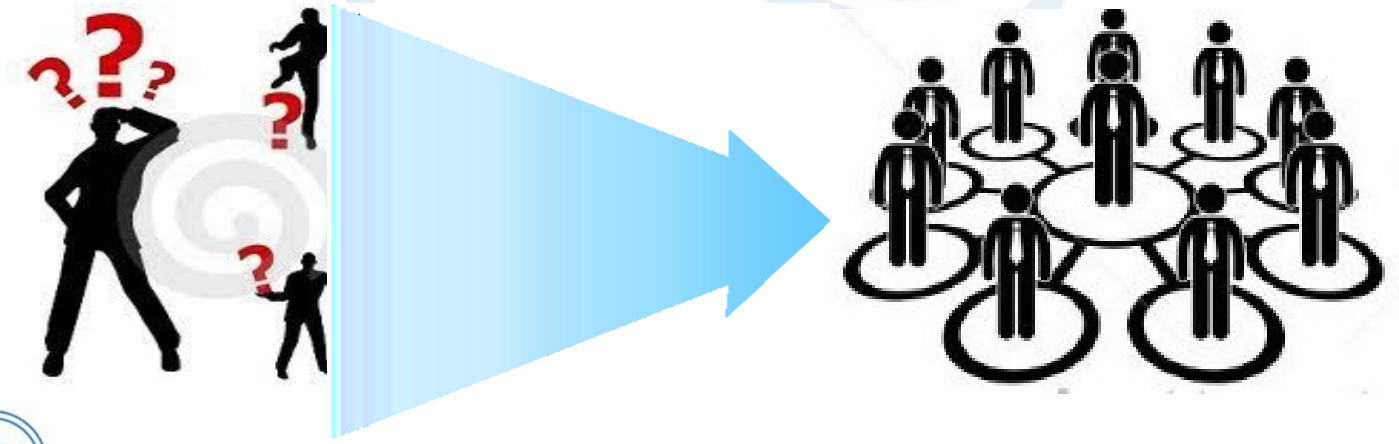
Framework: A Practical Scenario

- **Trust Domains with local IP address spaces**
  - Legacy hosts communicate with local IP addresses without security
- **Real & Imaginary IP address space**
  - **real IP addresses** are assigned to hosts in the domain IP^r_{host}
  - **imaginary IP addresses** are reserved for external hosts IP^i_{host}
  - Gateway translates (ID ⇔ local IP address) when passing domain boundary (after trust evaluation)



Concluding Remarks: Summary

- Entity-Environment Decoupling
- Anonymous ID with Traceability
- Bounded Trust in contrast to Unbounded Security
- Abstraction of Polymorphic Network Spaces into Domains
- Autonomous Trust domains with Accountability
- Security Delegation to the Domain



Concluding Remarks: Further Studies

- **Trust Relation Managements**
  - Enumerate “trust indexes”, “trust metrics”, and “trust level”
  - Dynamic trust level adjustments for entities and domains
  - Trust Index Service Infrastructure
- **ID management**
  - ID generation and registration
  - ID lookup service (for finding trust indexes and/or locators)
- **Domain based routing**
  - Network topology reductions
  - Domain information advertisements and Domain-level path computation
  - Overlapped domains and Pathlets within domains
- **ID based packet forwarding**
  - Domain passing procedures
- **Application specific domains**
  - IP networks, IoT, Named Data Network, Service Oriented Network, ….

Appendix : ID-LOC separation

- **ID-Locator Separated**
  - **ID** denotes an entity unambiguously
  - **Locator** specifies the location in the space (Environment)
  - ID is bound to the locator when the entity exists in a space
- **Why should ID be separated from Locator?**
  - ID is the **identifiable name** of an entity
  - Locator is the **locatable address** in a specific space
  - An entity may exist in multiple spaces
  - The space of the locator determines the mechanism

ID : Identifying the Entity Unambiguously

Locator : Specifying the relative position in the space

Appendix: Yet Another Definitions on Name, Address, Identifier, and Locator (YaNAIL)

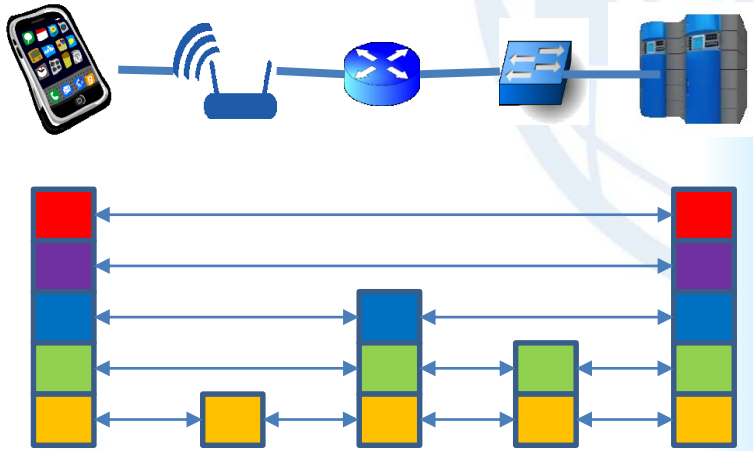
- **Definition by Role**
  - **Name** denotes an entity
  - **Address** denotes the position whe an entity can be placed
- **Definition by Property**
  - **An Identifier** is unique within a scope, i.e. ***<Set>***
    - **Identifiable name**
    - Location independent

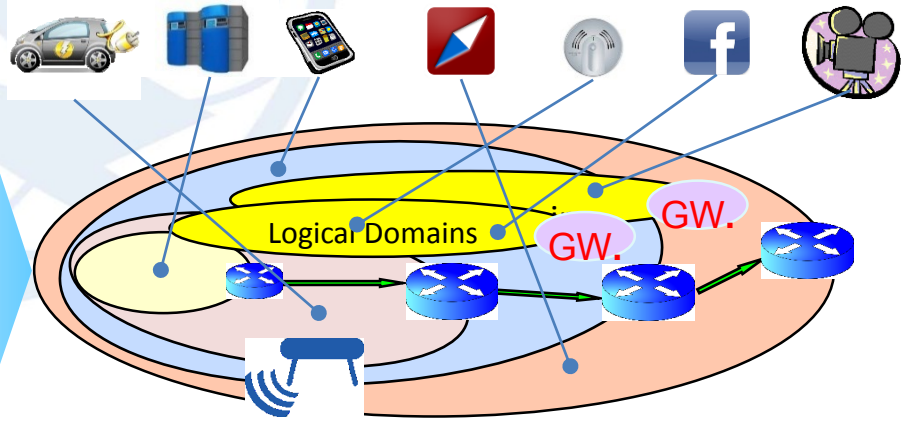
      ? Locatable name
  - **Locators** are inter-related on a given space, i.e. ***<Set, Relation>***
    - **Locatable address**
    - Mechanism dependent

      ? Identifiable address

Appendix: Views on Network

- **Vertical Functional View**
  - Network is viewed as a set of node and links
  - Functional decomposition within a node
  - Peer-to-peer protocols
  - System Engineer View
- **Horizontal Spatial View**
  - Network is viewed as collaborating spaces
  - Spatial decomposition of space (space structuring)
  - Procedures for passing spaces
  - Network Architect View

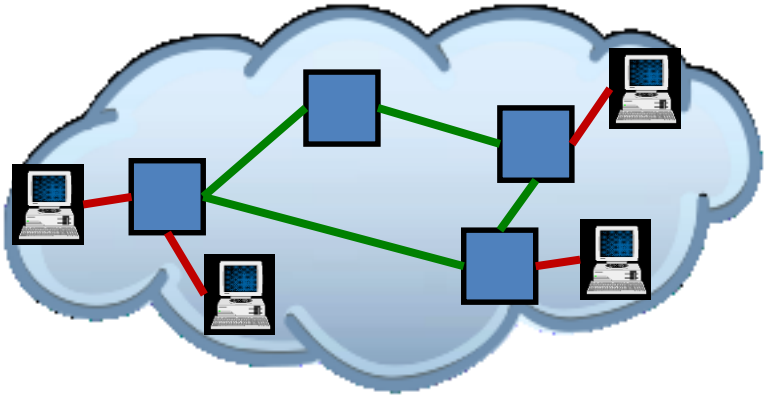




Appendix: Types of Network Spaces

- **Homomorphic Space**
  - All entities share the same mechanism (IP protocol)
  - Hard to evolve

➢ Making Entities IP-capable

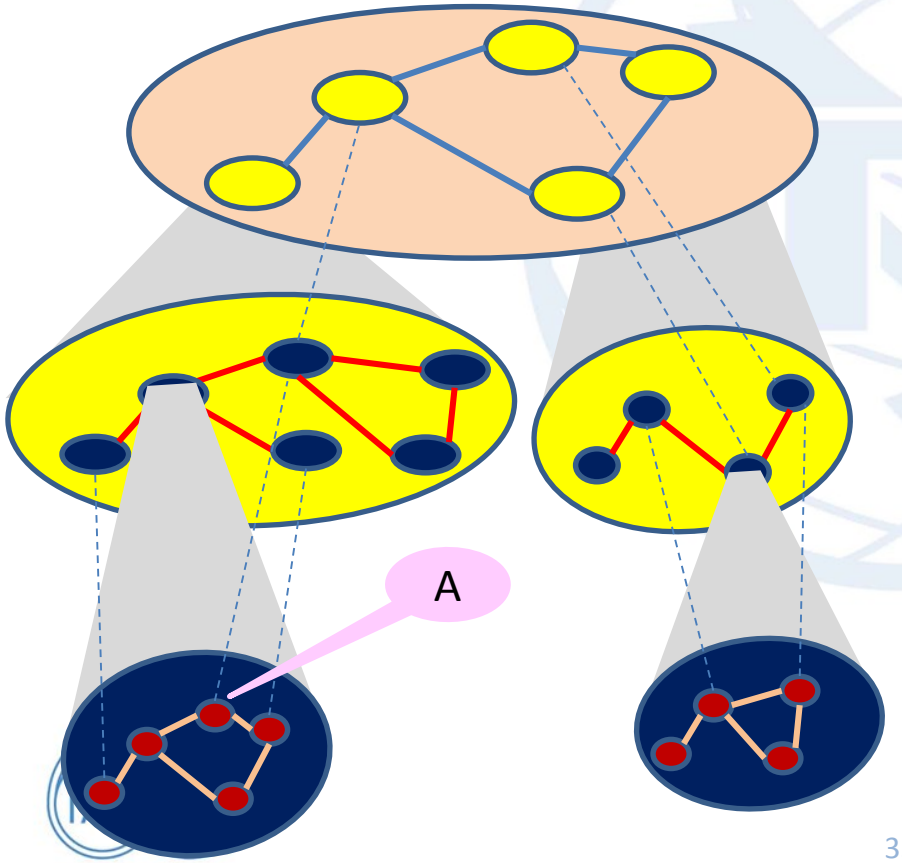


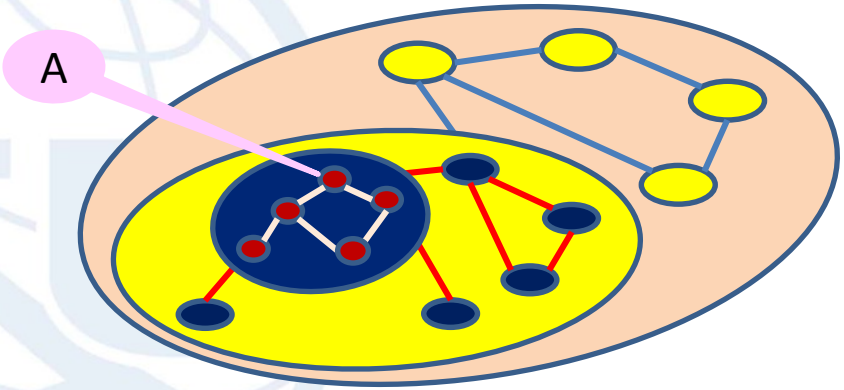
- **Polymorphic Space**
  - Enable different mechanisms in parallel
  - Enable easy deployment of new mechanisms

➢ Making Networks for Entities

Appendix: Hierarchy of Domains

- **A Recursive Domain allows Hierarchy of Domains**
  - Allows domains in a domain
  - A solution to scalability by network topology reduction





Reduced Topology

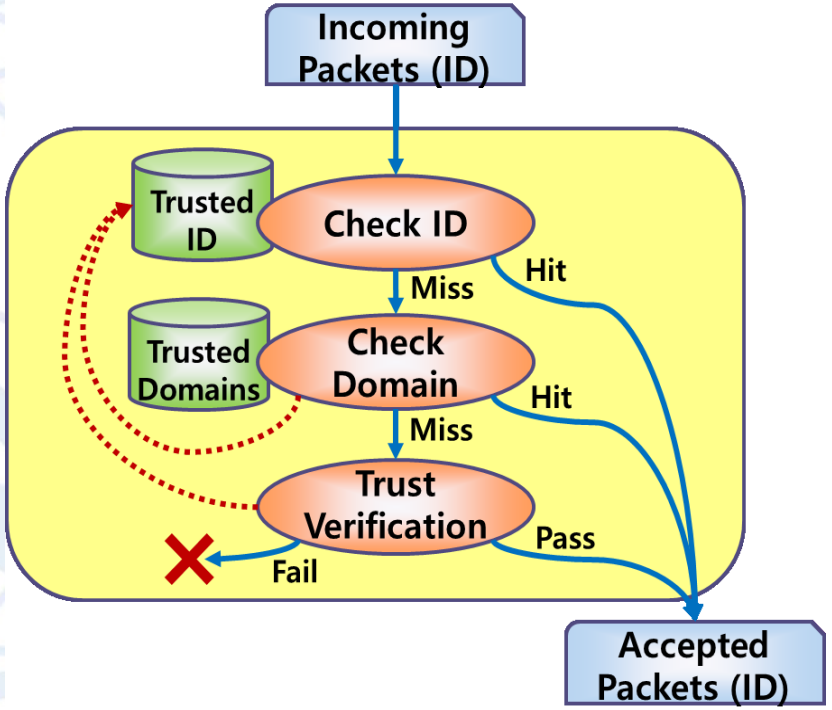
- the finer view on the nearer
- the coarser view on the further

For a network with N nodes, d elements per each domain

- Topology with $O(d \log_d N)$

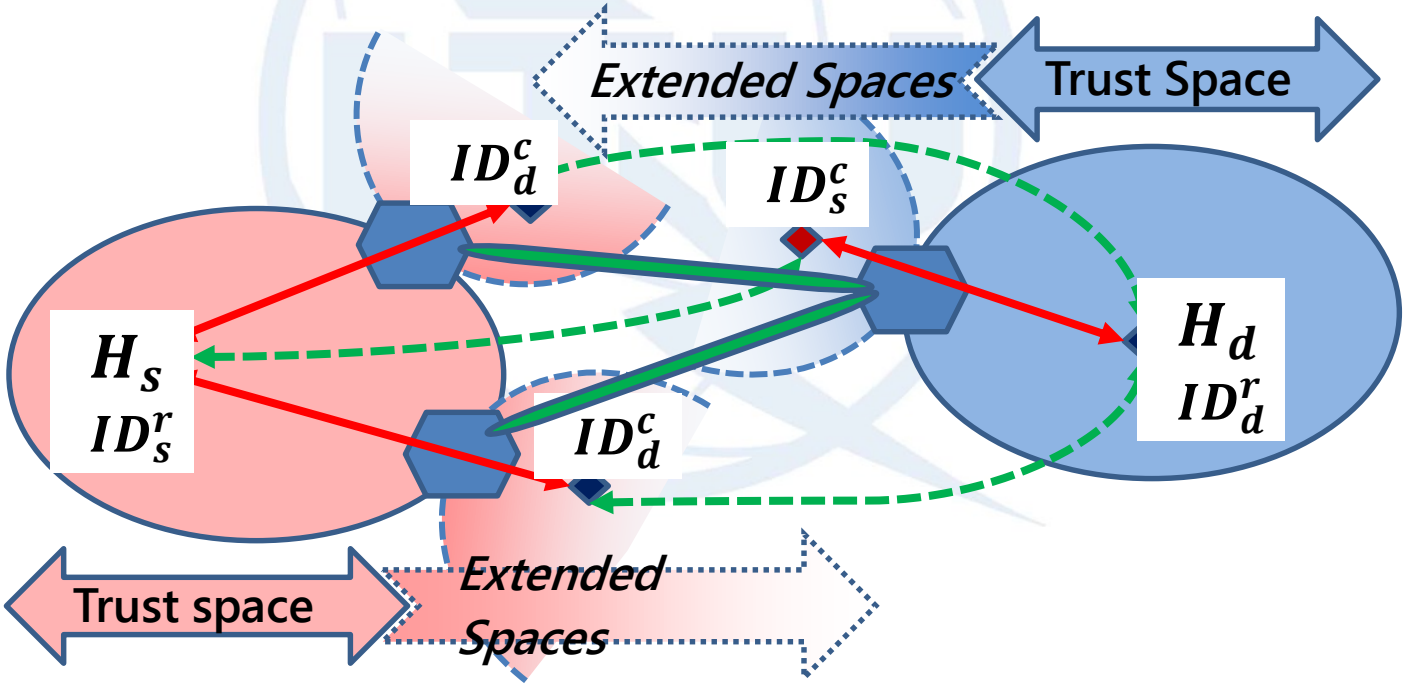
Appendix: Trusted Caches

- **Trusted ID Cache**
- **Trusted Domain Cache**
- **If not in the Cache**
  - Verification Procedure must be passed
  - Verified, then put the ID in the trusted cache for subsequent Packets



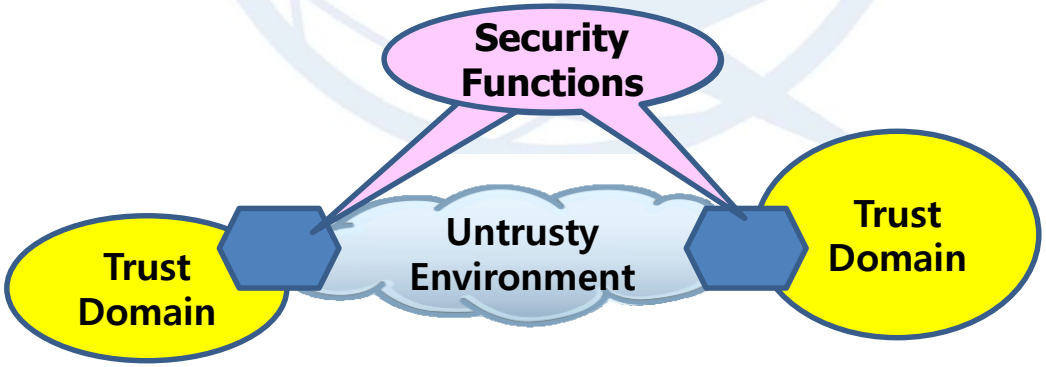
Appendix: Space Extension

- **Registered ID and Cached ID**
  - A trust space consists of registered IDs (ID_s^r, ID_d^r)
  - It is extended with cached IDs (ID_s^c, ID_d^c)
  - Channel between domains must be secure



Appendix: Channel Management

- **The channel between trust domains (entities)**
  - Guarantees the expected secure level,
    - Select secure paths (i.e. SCION)
    - Perform additional security functions (i.e. IPsec)
- **security functions for channels**
  - Content level: encryption, signature, etc.
  - Packet level: nonce, sequence, timestamp, reservation, etc.
  - Packet bundling : the functions can be applied to a set of packets



Appendix: Internet Governance

Authoritarian
- Centralized control
- Hierarchical Authorities
- Responsibility and Surveillance

Autonomy
- Distributed control
- Autonomous domains
- Accountability and Self-governance

Anarchy
- No control
- Selfish individuals
- No responsibility and Self-protection

Internet Governance

Appendix: Domains for IoT

- **Internet vs. IoT**
  - Hosts (Internet) are addressable and have processing power
  - Devices(IoT) are named and have no or limited processing power
  - Security becomes more critical
    - Stronger security needs more processing power
- **IoT Domain**
  - A domain specific to devices (ex. RFID reader)
  - Devices can delegate security to the domain
  - Devices can be kept secure within the Insulated trust domain

CCITT / ITU-T