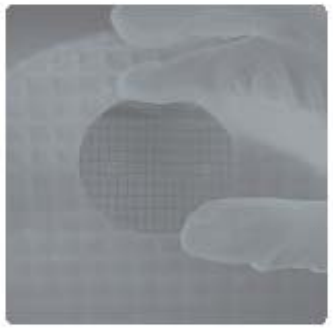
Security Considerations for the Future Internet



우리나라를 세계 속의 정보통신 일등국가로 만드는 사람들

2010.02.23.

Dong il Seo (*bluesea@etri.re.kr*)

IT R&D Global Leader

ETRI

Contents outline

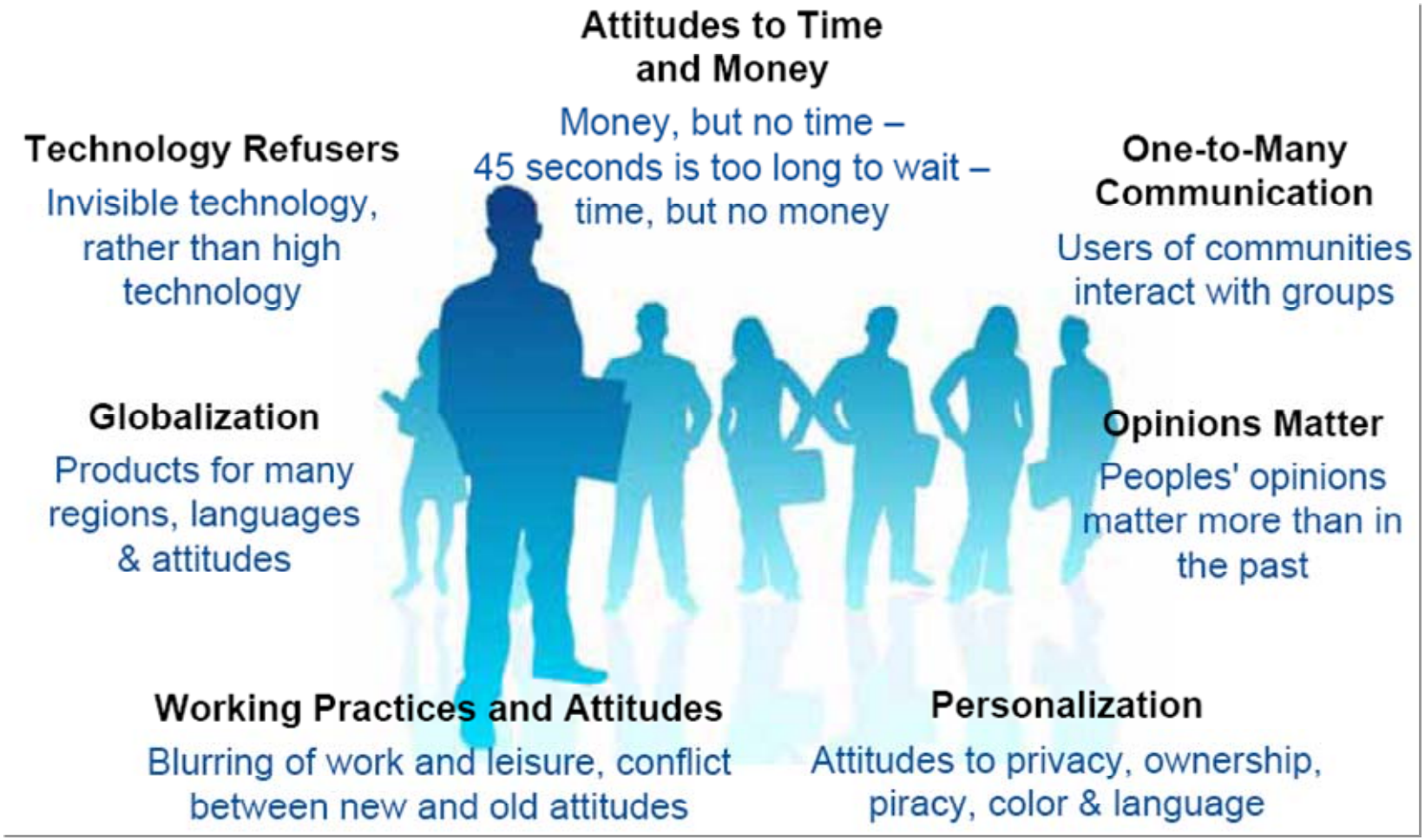
Technologies Trends

Security for Future Internet

Considerations

Worldwide Social Trend

❑ Social Trends, New Behaviors and Expectations – the "Pull" to Innovate (Gartner, '08.11)



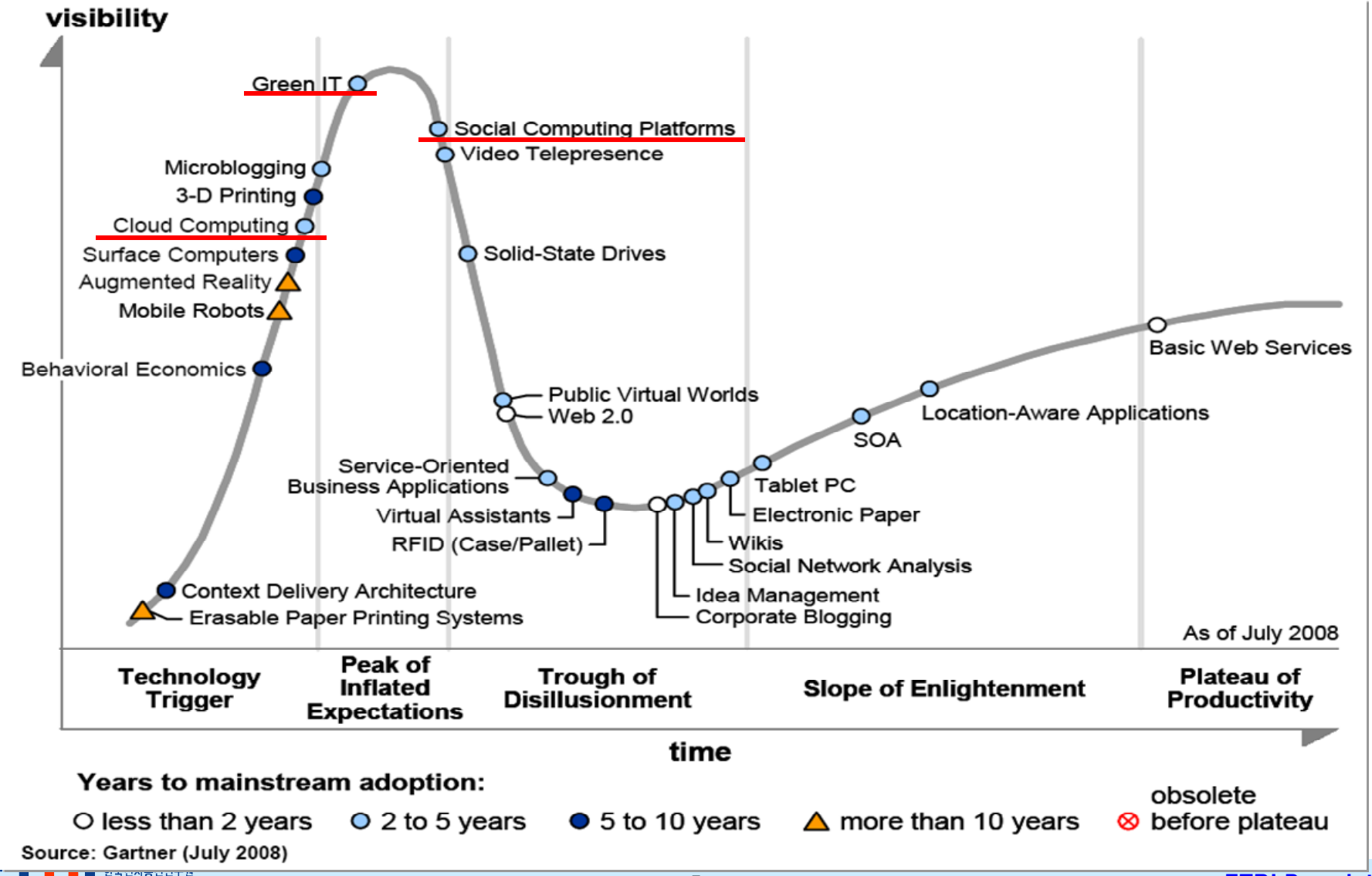
Top 10 Strategic Technologies

❑ Top 10 Strategic Technologies for 2010 (Gartner, 2009.10)

Rank	2008	2009	2010
1	Green IT	Virtualization	Cloud Computing
2	Unified Communications	Business Intelligence	Advanced Analytics
3	Business Process Management	Cloud Computing	Client Computing
4	Metadata Management	Green IT	IT for Green
5	Virtualization	Unified Communications	Reshaping the Data Center
6	Mashup	Social Software and Social Networking	Social Computing
7	Web Platform	Web Oriented Architecture	Security-Activity Monitoring
8	Computing Fabric	Enterprise Mashups	Flash Memory
9	Real World Web	Specialized Systems	Virtualization for Availability
10	Social Software	Servers-Beyond Blades	Mobile Applications

Emerging Technologies, 2008

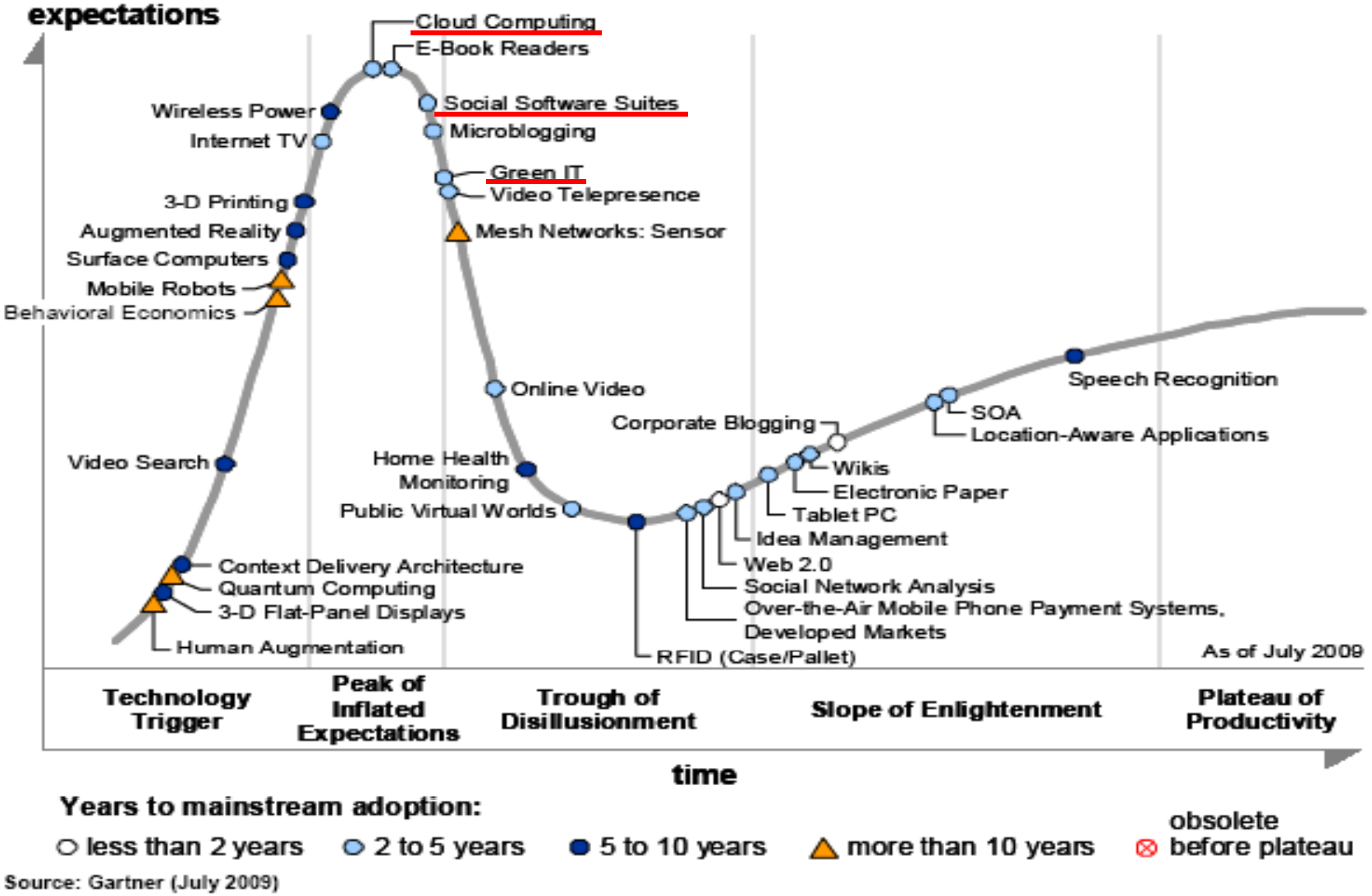
❖ Hype Cycle for Emerging Technologies, 2008



Source: Gartner (July 2008)

Emerging Technologies, 2009

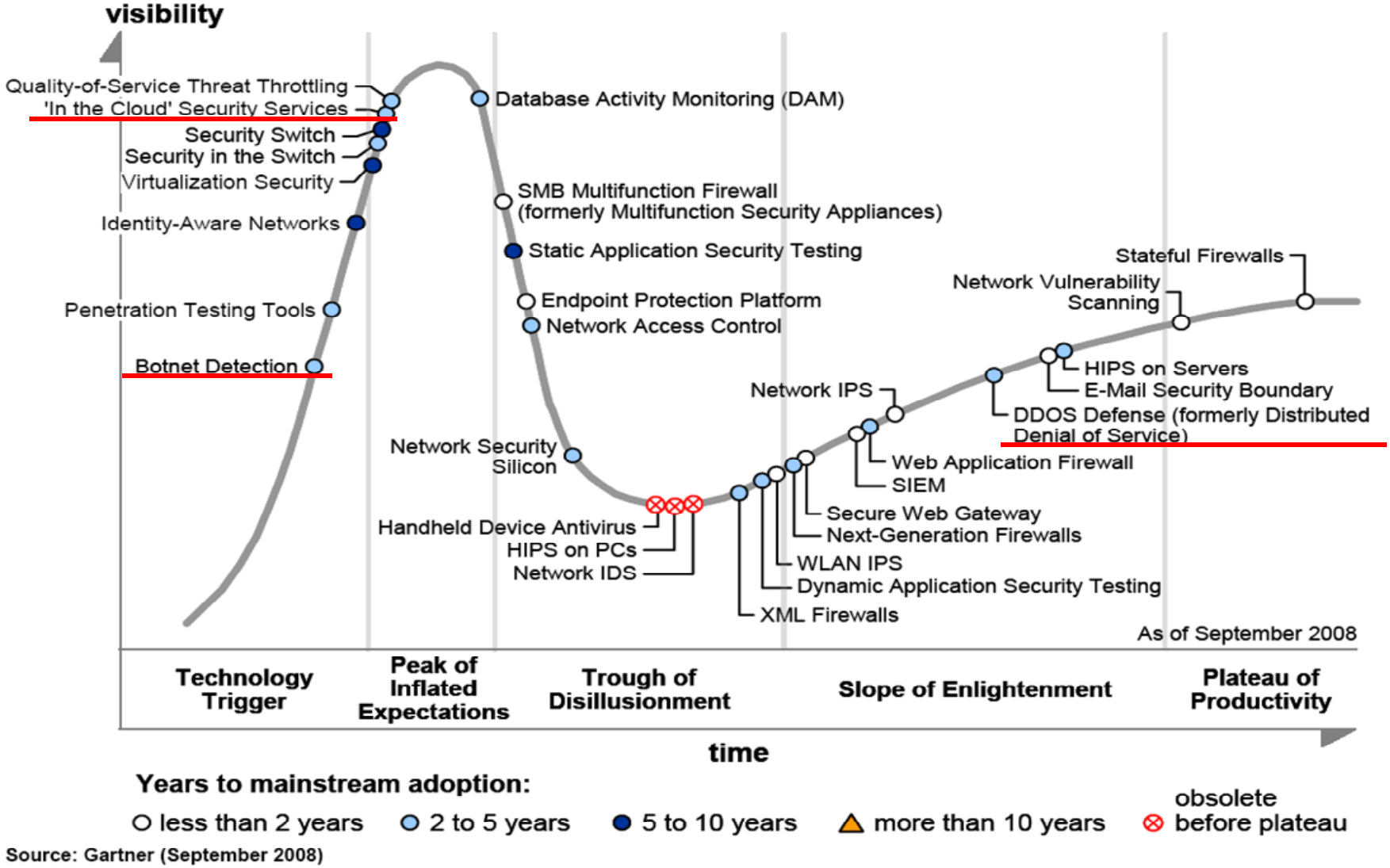
❖ Hype Cycle for Emerging Technologies, 2009



Source: Gartner (July 2009)

Infrastructure Protection, 2008

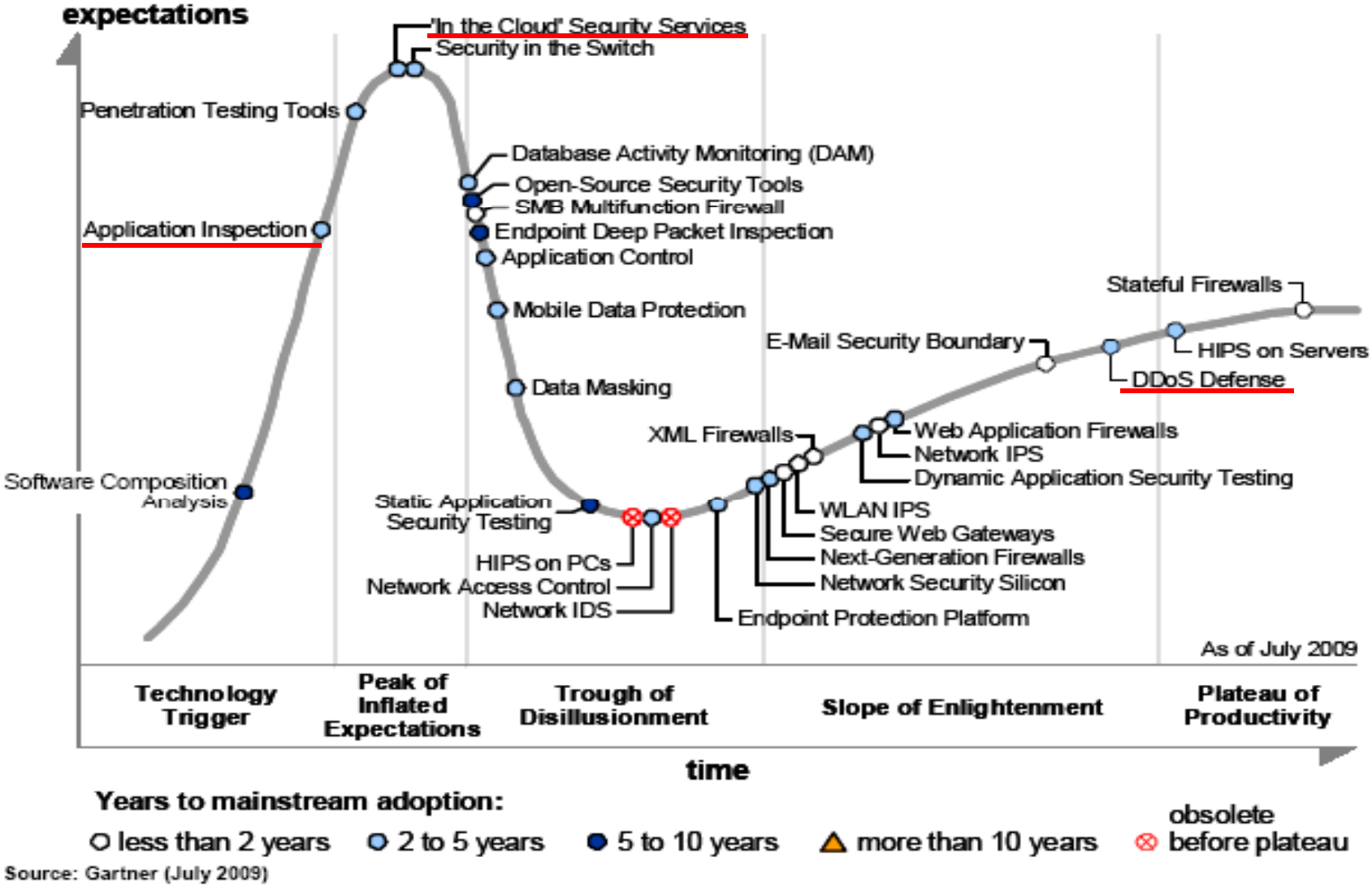
- Hype Cycle for Infrastructure Protection, 2008



Source: Gartner (September 2008)

Infrastructure Protection, 2009

- Hype Cycle for Infrastructure Protection, 2009



Source: Gartner (July 2009)

Cyber Attack Trends

- Targeted vs. broad
  - targeted attacks
- Changes in motivation
  - prior to 2006 : Hactivism (Politically motivated attacks)
  - Current : Financially motivated attacks
- Changes in targets
  - not looking for vulnerable PCs
  - looking for vulnerable web sites and vulnerable users
- Technologies
  - Applying STEALTH techniques to attacks hiding
  - Zero-day attack trial increased
  - Attacks using web vulnerability increased
  - Attacks on mobile vulnerability increased

The requirement of future internet

- ✓Scalability/Ubiquity
- ✓Security/Robustness
- ✓Mobility
- ✓Heterogeneity
- ✓Quality of Service
- ✓Re-configurability
- ✓Context-awareness
- ✓Manageability
- ✓Data-centric or Content-centric
- ✓Economics

※ the requirement of future internet = the problems with current internet

FP7 Security Project

- FP7 - 14 Security Projects

  “Security, Privacy and Trust in the Future Internet”

Integrated projects

- MASTER
- PRIMELIFE
- TAS3
- TECOM

Specific targeted research projects

- AVANTSSAR
- AWISSENET
- INTERSECTION
- PICOS
- PRISM
- SWIFT
- WOMBAT

Networks of Excellence Co-ordination Actions

- eCRYPT II
- FORWARD
- THINK-TRUST

FP7 Security Project

✓MASTER

: Managing Assurance, Security and Trust for Services

- This project aims at providing manageable assurance of the security and trust levels and regulatory compliance of highly dynamic Service Oriented Architectures that deal with business process

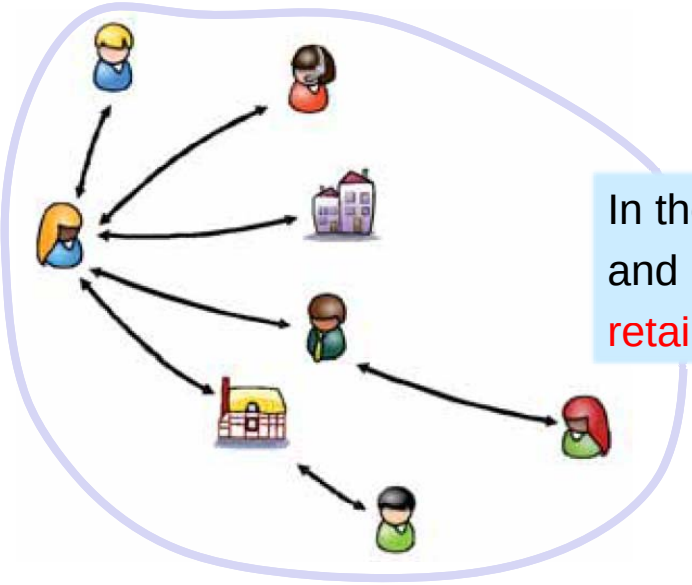
- It defines an overall infrastructure that facilitate the monitoring, enforcement and audit of quantifiable indicators on the security of a business process

FP7 Security Project

✓PRIMELIFE

: Bring Life-Long Privacy to the Internet

- This project aims at bringing sustainable Privacy and Identity Management to future networks and services, with users retaining control of their own personal data



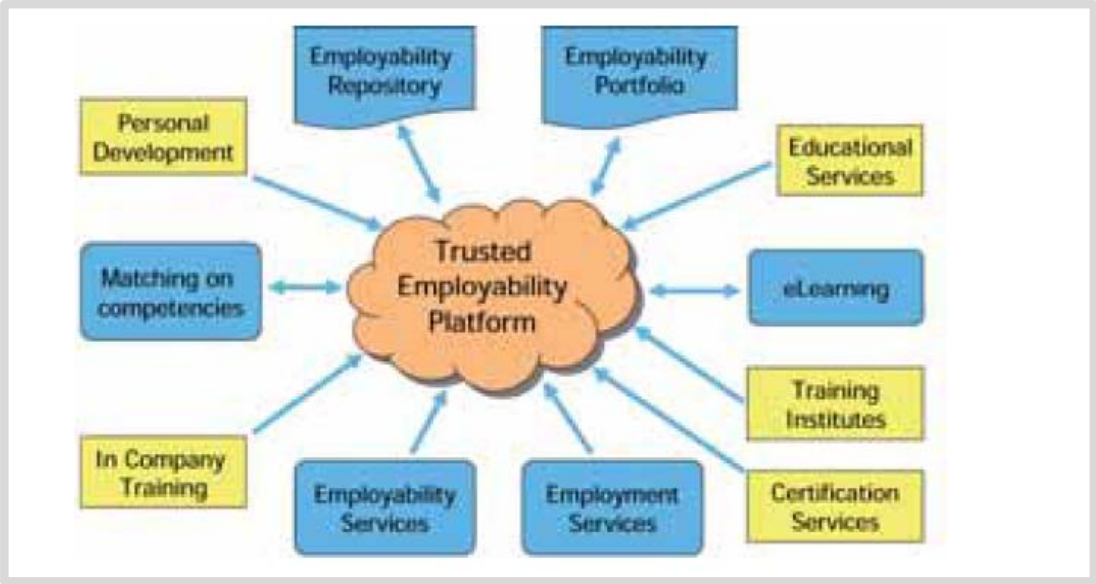
In the Information Society, users can act and interact in a safe and secure way while retaining control of their private sphere

FP7 Security Project

✓TAS3

: Trusted Architecture for Securely Shared Services

- This project aims at developing a generic architecture with trusted services to manage personal information and substantiating it into two concrete healthcare and employability platforms

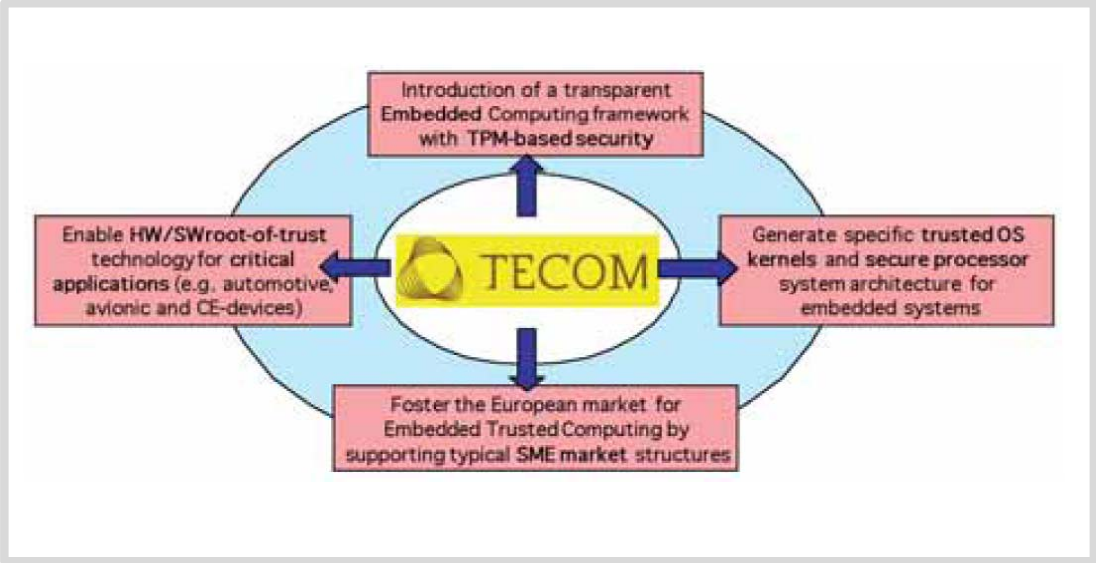


FP7 Security Project

✓TECOM

: Trusted Embedded Computing

- This project will adapt a systematic approach to the development of trusted embedded systems, consisting of hardware platforms with integrated trust components
- It includes following issues in the figure



FP7 Security Project

✓AVANTSSAR

: Validating Security Properties of Software Services

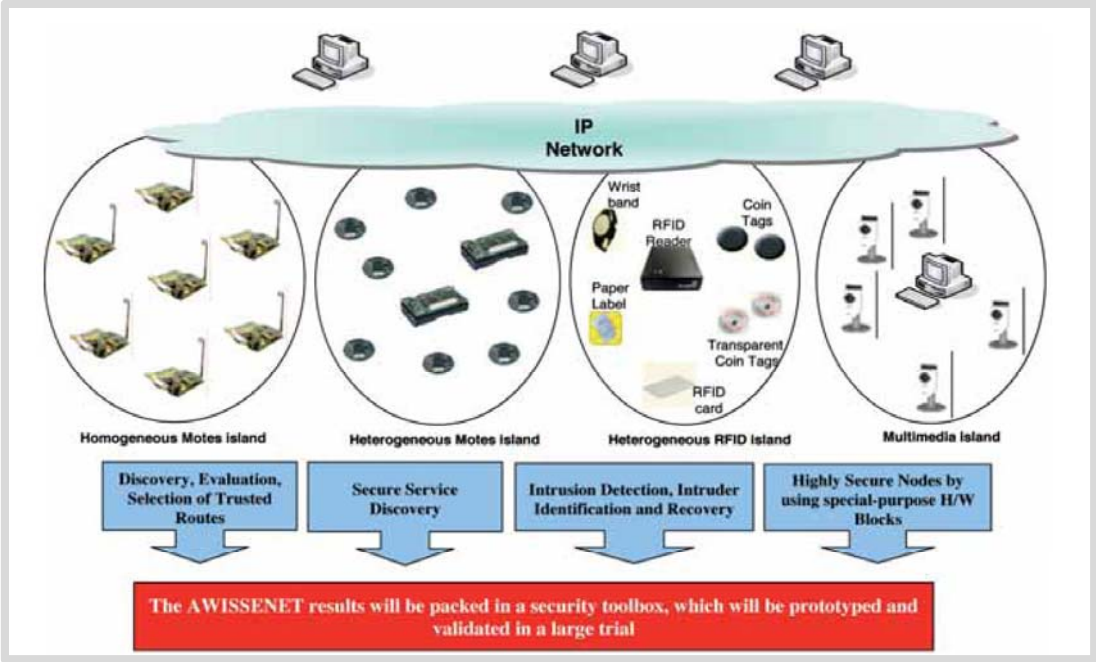
- This project will develop the first computer language for specifying trust and security properties of services and their dynamic composition into secure service architectures
- The language will be integrated in a new software platform with algorithms and tools to validate those properties

FP7 Security Project

✓AWISSENET

: Ad-hoc personal area network and WIreless Sensor Secure NETwork

- This project focuses on security and resilience across ad-hoc Personal Area Networks (PANs) and wireless sensor networks



FP7 Security Project

✓INTERSECTION

: Infrastructure for heTErogeneous, Resilient, Secure, Complex, Tightly Inter-Operating Networks

- This project focuses on vulnerabilities at the intersection points between interoperating network providers

✓PICOS

: Privacy and Identity Management for Community Services

- This project will develop and build a state-of-the-art platform for providing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks

FP7 Security Project

✓PRISM

: Privacy-aware Secure Monitoring

- This project aims at setting a new de-facto standard for privacy-preserving traffic monitoring and deliver a tool that is guaranteed for legal compliance

✓SWIFT

: Secure Widespread Identities for Federated Telecommunications

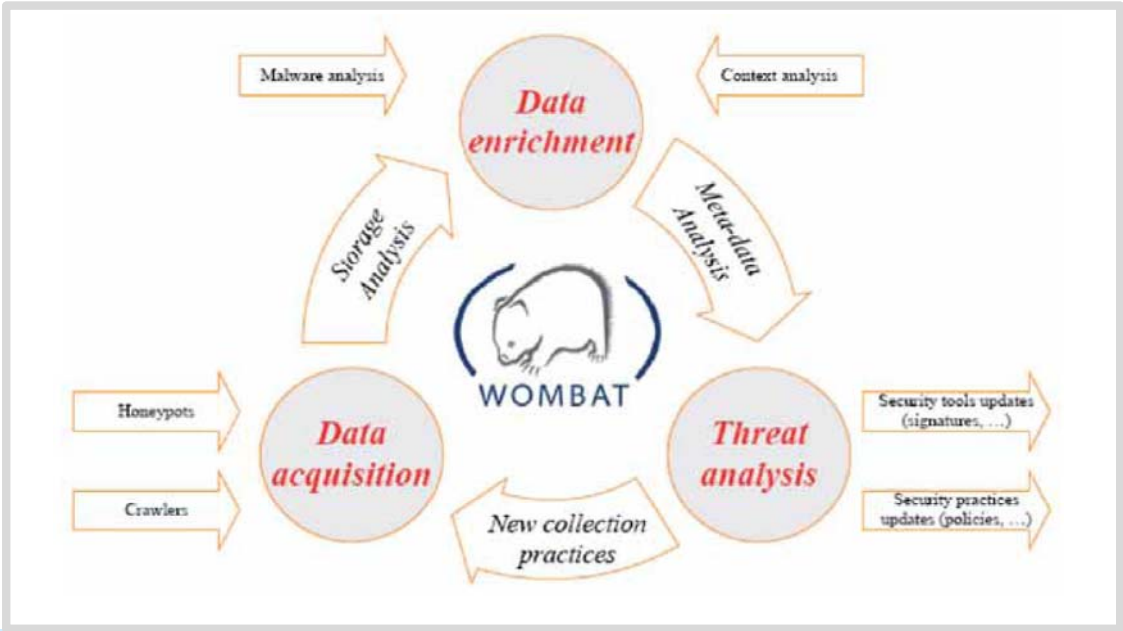
- Identity Management (IdM) are currently confined to the web services domain. SWIFT extends IdM by including user centricity and network operators as additional interdependent domains with IdM at the core

FP7 Security Project

✓WOMBAT

: Worldwide Observatory of Malicious Behaviors and Attack Threats

- This project aims at providing new means to understand the existing and emerging threats that are targeting the Internet economy and the net citizens



FP7 Security Project

✓eCRYPT II

: Fundamental enabler for secure, dependable and trusted infrastructures

- … Outstanding and on-Going Challenges for European Cryptology !

✓FORWARD

: Managing Emerging Threats in ICT Infrastructures

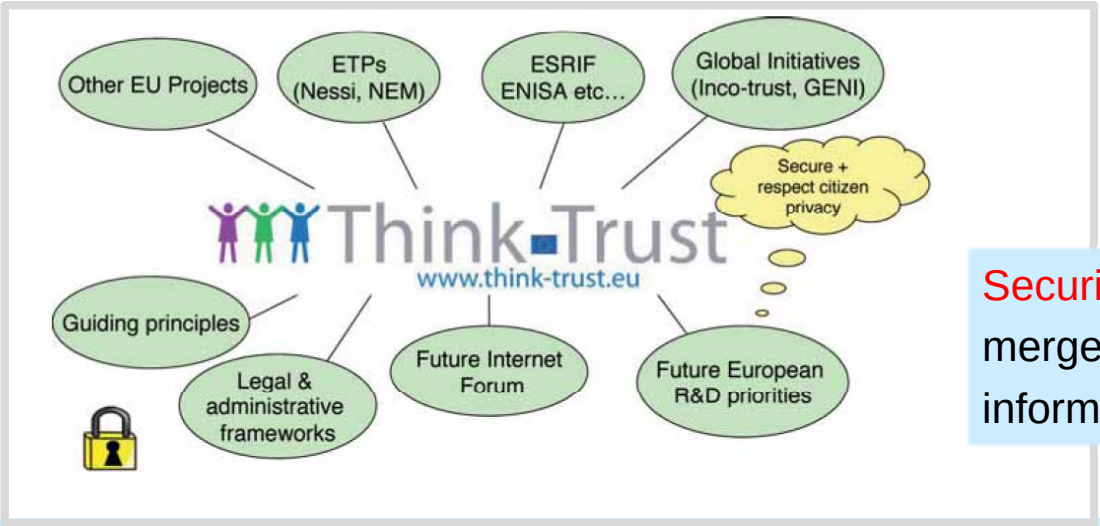
- This project aims at promoting collaboration and partnership between researchers from academia and industry involved in the projection of ICT infrastructures against cyber threats such as malicious code, spam and phishing

FP7 Security Project

✓THINK-TRUST

: Think Tank for Converging Consumer Needs in ICT Trust, Security and Dependability

- This project is a Coordination Action that will set up an ICT Security Research Advisory Board that will bring together the opinions and requirements of a comprehensive range of stakeholders with regard to trust, security and dependability issues in emerging ICT environments



Security is the solution to the mergence of a new dynamic information society

USA, FIND project

- ✓ FIND (Future Internet Design) is a major new long-term initiative of the NSF NeTS research program
- ✓ NSF NeTS research program
  - ➢ Future INternet Design (FIND)
  - ➢ Networking of Sensor System (NOSS)
  - ➢ Wireless Networks (WN)
  - ➢ Networking Broadly Defined (NBD)
- ✓ Total of 48 projects (By February 2010)
  - ➢ FIND research might address questions
    - How can we design a network that is fundamentally more secure and available than today's Internet? How would we conceive the security problem if we could start from scratch?
    - How might such functions as information dissemination, location management or identity management best fit into a new network architecture?
    - What will be the long-term impact of new technologies such as advanced wireless and optics?
    - How will economics and technology interact to shape the overall design of a future network?
    - How do we design a network that preserves a free and open society?

USA, FIND project

- ✓ Architectural Support for Network Trouble-Shooting
- ✓ Keyword
  - ➢ Identity
  - ➢ Tracking
  - ➢ Privacy
- ✓ Outline
  - ➢ This project aims to fundamentally change the nature and quality of network troubleshooting.
  - ➢ Research themes
    - Identifying Responsibility
    - Beyond Modularity
    - Tracking Causality
    - Privacy
    - Troubleshooting and Robustness

USA, FIND project

- ✓ Designing Secure Networks From the Ground-Up
- ✓ Keyword
  - ➢ Security
  - ➢ Privacy
- ✓ Outline
  - ➢ This project aims to develop a clean-slate Internet architecture where protection from malicious network-based attacks is a fundamental design goal and build, deploy and operate a prototype SANE(Security Architecture for Private Network Settings) network
  - ➢ Research themes
    - Designing SANE Switches
    - SANE's Service Model
    - Protection and Communication in SANE
    - End-to-End Communication
    - Revoking Access

USA, FIND project

- ✓ Enabling Defense and Deterrence through Private Attribution
- ✓ Keyword
  - ➢ Security
  - ➢ Packet Attribution
  - ➢ Group Signature
- ✓ Outline
  - ➢ This project is developing a novel architectural primitive---private attribution---based on group signatures that allows any network element to verify that a packet was sent by a member of a given group
  - ➢ Research themes
    - Privacy-preserving per-packet attribution
    - Content-based privacy assurance

USA, FIND project

- ✓ Enabling Future Internet innovations through Transitwire (eFIT)
- ✓ Keyword
  - ➢ Addressing
  - ➢ Routing
- ✓ Outline
  - ➢ This project is a new Internet architecture design, eFIT, to achieve the objective of enabling future innovations by ensuring strong universal connectivity at the architectural level
  - ➢ Research themes
    - Mobility
    - Security
    - Path Diversity and User Selection
    - Network Diagnosis
    - Explicit Network Feedback
    - Quality of Service

USA, FIND project

- ✓ Postmodern Internetwork Architecture
- ✓ Keyword
  - ➢ Internetwork
  - ➢ Network-layer innovation
  - ➢ Security
- ✓ Outline
  - ➢ This project aims to design, implement, and evaluate through daily use a minimalist internetwork layer and auxiliary functionality that anticipates tussles and allows them to be played out in policy space, as opposed to in the packet-forwarding path
  - ➢ Research themes
    - Support for any foreseeable policy requirement via explicit mechanism. This forces tussles to play out explicitly, under the control of the mechanism, as opposed to "under the covers."
    - Complete isolation of routing and forwarding. Routing (path selection) may be in-band, out-of-band, or some of both. This provides maximum flexibility with respect to the amount and type of resources devoted to path selection.
    - User control over inter-realm paths, within the constraints imposed by provider-specified policies. This allows forusers to select paths to achieve quality or other policy objectives.
    - Isolation of the basic forwarding mechanism from any kind of endpoint identifier. This makes it possible to use different forms of endpoint ID without modifying the fast forwarding path.

USA, FIND project

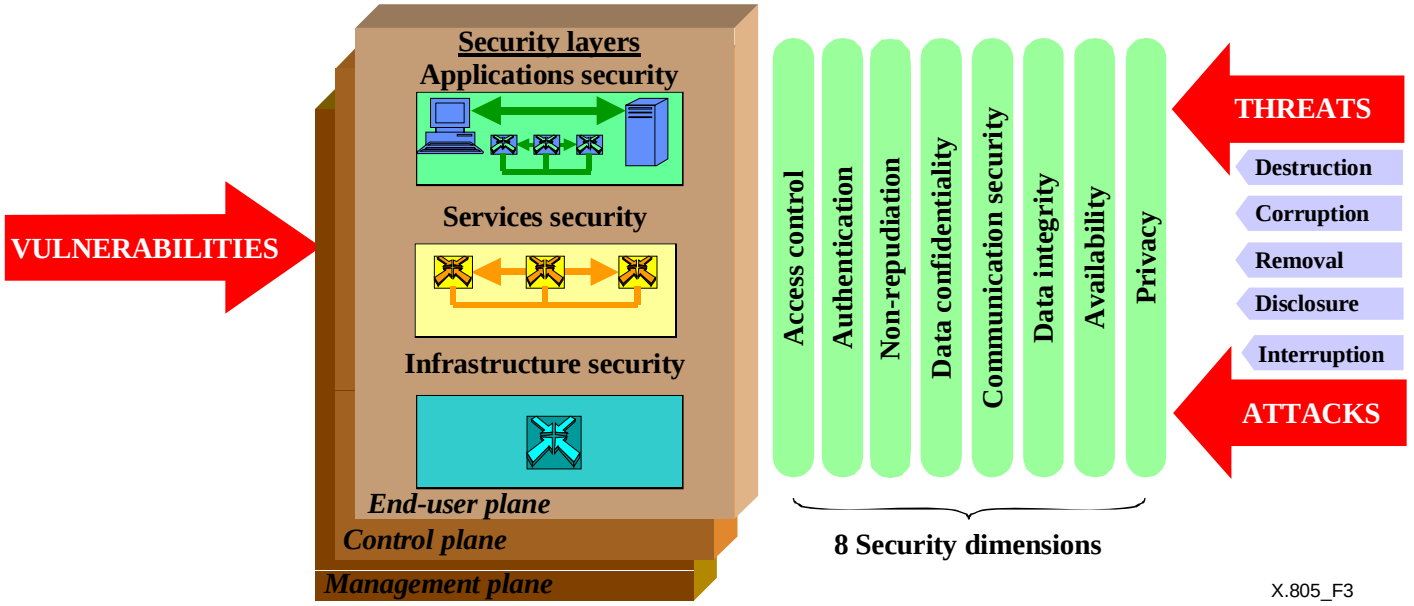
- ✓ Privacy-Preserving Attribution and provenance
- ✓ Keyword
  - ➢ Security
  - ➢ Attribution
  - ➢ Provenance
  - ➢ Group signature
  - ➢ Data Exfiltration
- ✓ Outline
  - ➢ This project is developing two key architectural capabilities---host attribution (which physical machine sent a packet) and data provenance (what is the ``origin'' of the data contained within a packet)---to enable the direct expression of a wide-range of security policies
  - ➢ Research themes
    - Key architectural components to improve the level of security and assurance available to network services
    - PIs are initiating a dialogue among both researchers and network operators about critical policy aspects of network security

USA, FIND project

- ✓ Protecting User Privacy in a network with Ubiquitous computing devices
- ✓ Keyword
  - ➢ Privacy
  - ➢ Implicit identifier
  - ➢ Wireless network security
- ✓ Outline
  - ➢ This project is to study existing systems such as 802.11 to characterize privacy threats and design improved network and link protocols that provide stronger privacy guarantees
  - ➢ Research themes
    - This includes names that conceal identity without compromising network functions, such as routing, that rely on them; name discovery
    - resolution protocols that do not reveal information across system layers.; techniques to detect implicit names exposed by end-points

Standardization Activity in ITU-T (1)

- ✓ **X.805 Security Architecture (conventional view on security in common)**
- ➔ [X.805] defines the following security dimensions. These security dimensions and security threats stated above are considered as the base of this Recommendation.
- ➔ However, This Recommendation does not further define or distinguish the use of the X.805 security layers (Applications, Services, or Infrastructure)
- ➔ Thus, It need to infer completeness for use as a security assessment for NGN networks which are not compliant with this standard.



Security architecture for end-to-end network security

Standardization Activity in ITU-T (2)

✓ 8 Security Dimensions of Y.2701 (Security Requirements for NGN Release 1)

1) Access Control

Wikipedia Definition.

Access control *is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.*

Cryptography and Network Security Principles and Practice 3rd Ed.

In the context of network security, ***access control*** *is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.*

- NGN providers are required to restrict access to authorized subscribers.
- The NGN is required to prevent unauthorized access, such as by intruders masquerading as authorized users.

Standardization Activity in ITU-T (3)

2) Authentication

Wikipedia Definition.

Authorization *is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define access policy.*

- NGN providers are required to support capabilities to authenticate subscriber, equipment, network elements , and other providers. This includes support of, but is not limited to, the following:
  a. Capabilities to authenticate users for transport network access
  b. Capabilities to authenticate user for access to services at the start of, and during, service delivery
  c. Capabilities for a NGN user to authenticate the NGN provider on each stratum
  d. Capabilities to allow user peer-to-peer authentication
  e. Capabilities to allow mutual authentication between two NGN providers on each stratum for exchange of signaling, management and media/bearer traffic
  f. Capabilities to allow authentication of other service providers across ANI interfaces. SIMbased and/or non-SIM-based approaches are to be supported

Standardization Activity in ITU-T (4)

3) Non-reputation

Webopedia Definition.

In reference to digital security, ***non-repudiation*** *means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.*

- This Recommendation does not specify any non-repudiation security requirements.
- *So, additional concerns of non-reputation are specified and needed for the future Internet environments.*

Standardization Activity in ITU-T (5)

4) Data Confidentiality

[X.800 in ITU-T]
The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Hitachi ID Systems, Inc.
Data Confidentiality is whether the information stored on a system is protected against unintended or unauthorized access. Since systems are sometimes used to manage sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data. Accordingly, this is an integral component of Security.

- NGN providers are required to protect the confidentiality of subscriber traffic by cryptographic or other means.
- NGN providers are required to protect confidentiality of control messages by cryptographic or other means if security policy requests.
- NGN providers are required to protect the confidentiality of management traffic by cryptographic or other means.

Standardization Activity in ITU-T (6)

5) Communication Security

Wikipedia Definition.

Communications security (COMSEC)*: Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, traffic-flow security. and physical security of COMSEC equipment.*

- NGN providers are required to provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

Standardization Activity in ITU-T (7)

6) Data Integrity

PC Magazine Encyclopedia

The quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data. It is achieved by preventing accidental or deliberate but unauthorized insertion, modification or destruction of data in a database. Data integrity is one of the six fundamental components of information security.

Cryptography and Network Security Principles and Practice 3rd Ed.

*As with confidentiality, **integrity** can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straight-forward approach is total stream protection.*

- NGN providers are required to protect the integrity of subscriber traffic by cryptographic or other means.
- NGN providers are required to protect integrity of control messages by cryptographic or other means if security policy requests.
- NGN providers are required to protect the integrity of management traffic by cryptographic or other means.

Standardization Activity in ITU-T (8)

7) Availability

[X.800] and RFC 2828

*Both standards define **availability** to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).*

- NGN is required to provide security capabilities to enable NGN providers to prevent or terminate communications with the non-compliant end-user equipment; e.g. to mitigate DoS attacks, spreading of viruses or worms and other attacks. These capabilities may be suspended to allow emergency communications.
- NGN internal network elements may also be susceptible to viruses, worms, and other attacks. Similar measures to quarantine network components are also required.
- An NGN should provide provision of security capabilities to enable a NGN provider to filter out packets and traffic that is considered harmful by the respective security policy.
- NGN is required to provide capabilities for the support of disaster recovery functions and procedures. The specific requirements are outside the scope of this Recommendation.

Standardization Activity in ITU-T (9)

8) Privacy

Wikipedia Definition.

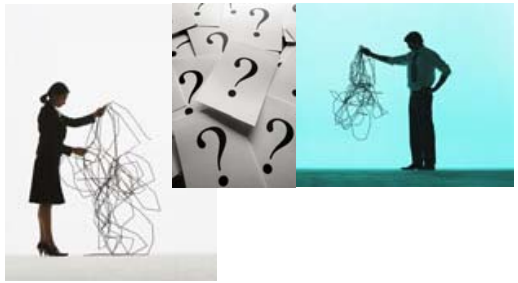
Privacy *is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes.*

- NGN is required to provide capabilities to protect the subscriber's private information such as location data, identities, phone numbers, network addresses or call-accounting data according to national regulations and laws.
- Specific requirements for privacy are national matter and are out of scope.

Towards a New Way of Future Internet Security

✓ A Complicated Problem (Nobody goes that way)

A pile of cable,
totally mixed up! ☹



Sorting through
a pile of cable

Holding one end first!

Holding opposite ends of a long cable

Long way… but, a better approach

Holding ends of a cable
and putting them together ☺

***Possible?
… might be impractical***

The Next Step might be… (1)

✓ **Openness VS. Security**

➔ One good strategy is fairly tuning two objectives for achieving a balanced performance

Preparing for expected benefits

Functionality, Sharing, Transparency, Convenience, Compatibility, Anonymity, Performance, Operability, and so forth

Coping with potential risks

Confidentiality, Integrity, Availability, Concealment, Protection, Privacy, Identification, Trustworthiness, etc.

Emerging technologies and services, and one-to-one communications come us with unpredictable threats and attacks

Risky-ignored Internet

Security costs too much

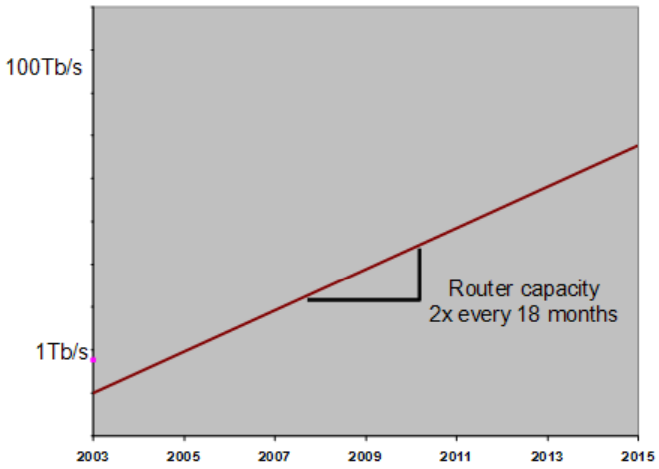
Should be equally fair??

We're going the same way together

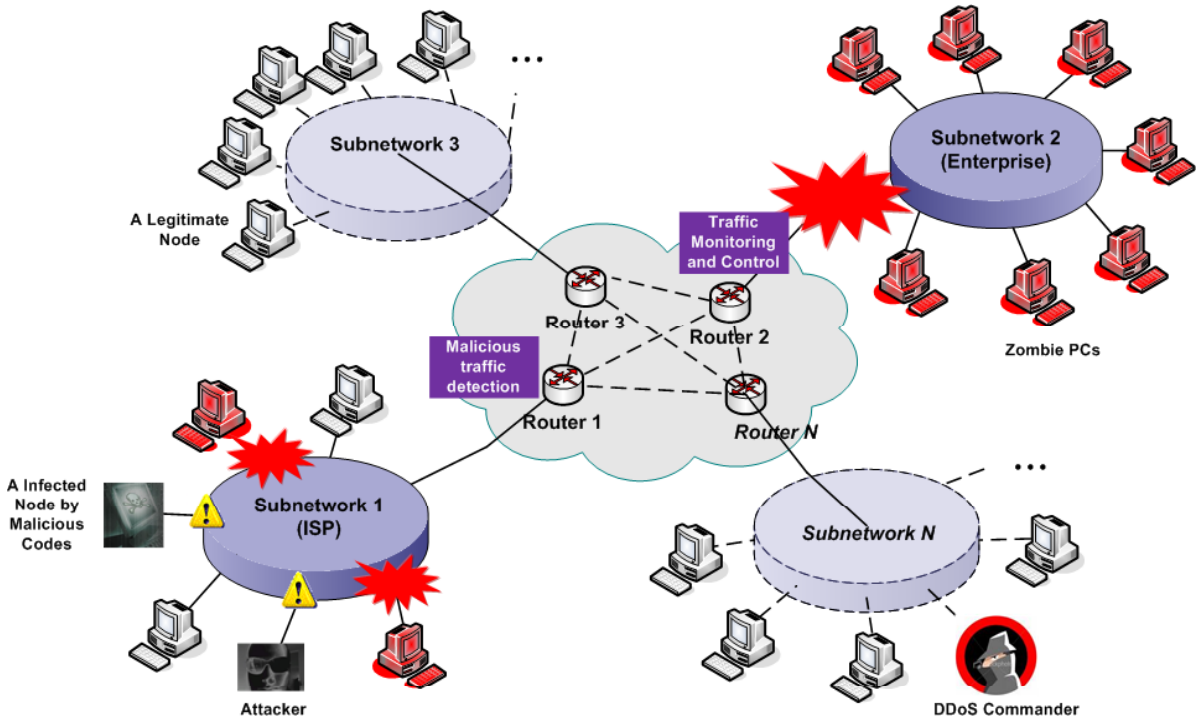
The Next Step might be… (2)

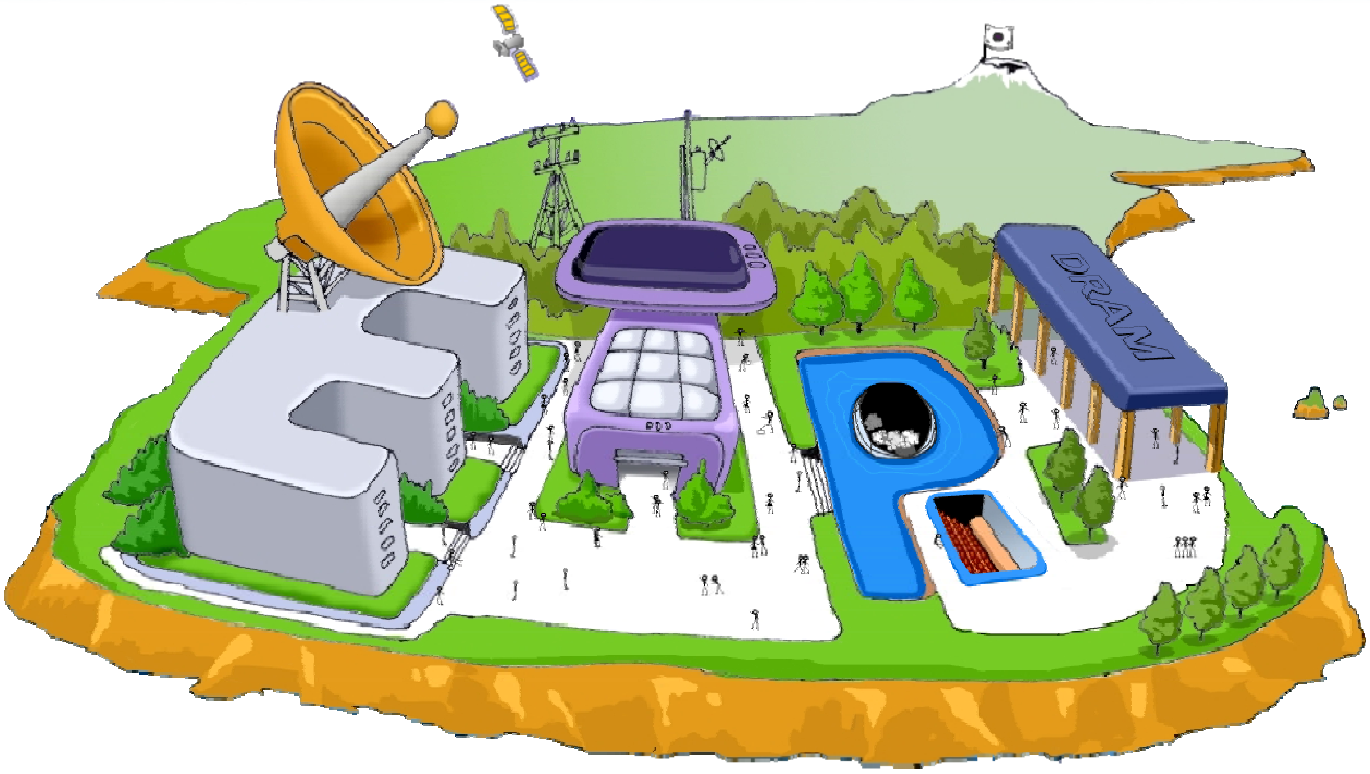
- ✓ **Building free networks from malicious codes and DDoS attacks**
- ➔ One suggestion is that individual routers could be equipped with detection, blocking, and other relevant functions coping with serious threats and attacks.
- ➔ This cooperative network is able to play a role of the global sensorium for the future Internet.

A Linear (Pessimistic) Expectation in the Router Capacity Growth



*Source from Stanford Univ.





Future is not to be predicted,
but to be created.