Panel:
Business Impact of Research on Policy for Distributed Systems and Networks

IEEE Policy Workshop 2007

Marco Casassa Mont
(marco.casassa-mont@hp.com)
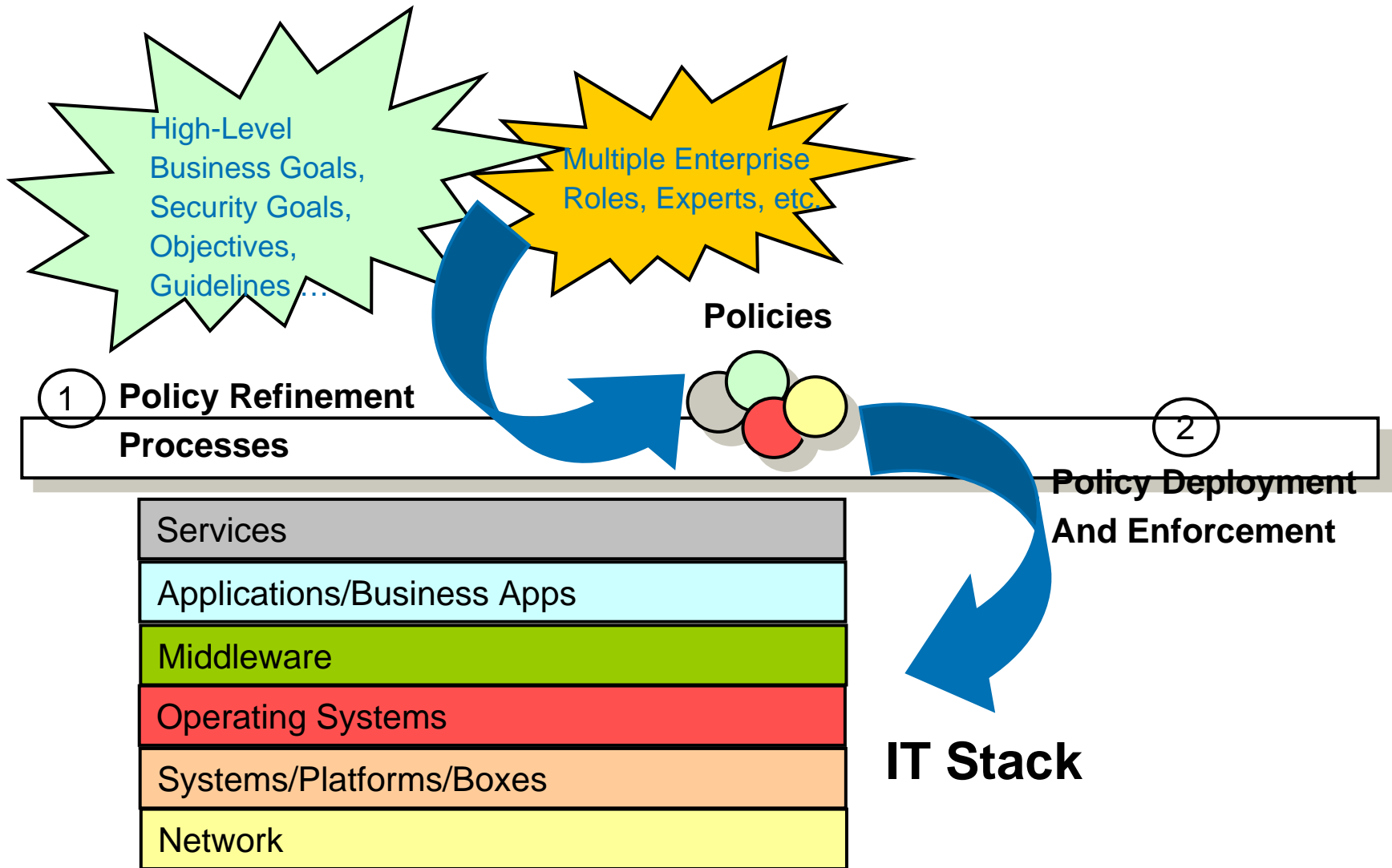
Hewlett-Packard Labs

Questions

- What success stories does the policy research community have to show for these ten years of research in terms of real business impact?

- What was envisaged ten years ago that did not materialize, and what are the reasons for that?

- Is the community still investigating these issues? What is the likelihood of success if so?

- New trends and links to business-driven IT management?
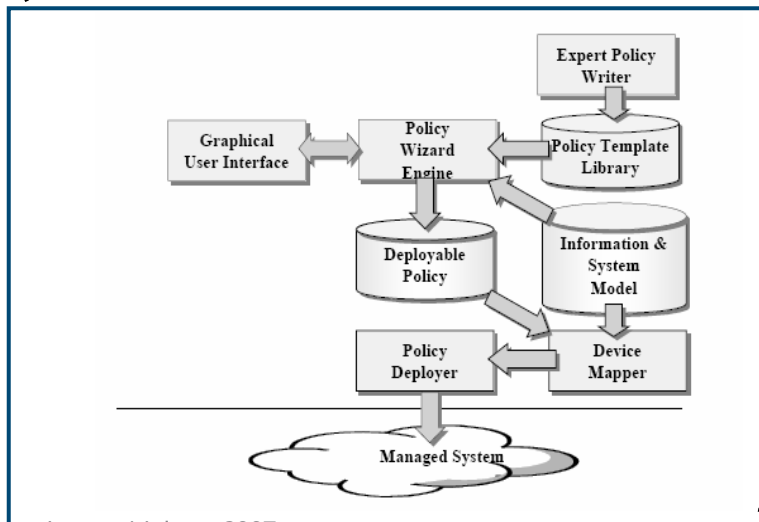
The Vision of 10 Years Ago

High-Level Business Goals, Security Goals, Objectives, Guidelines...

Multiple Enterprise Roles, Experts, etc.

Policies

1 **Policy Refinement Processes**

2 **Policy Deployment And Enforcement**

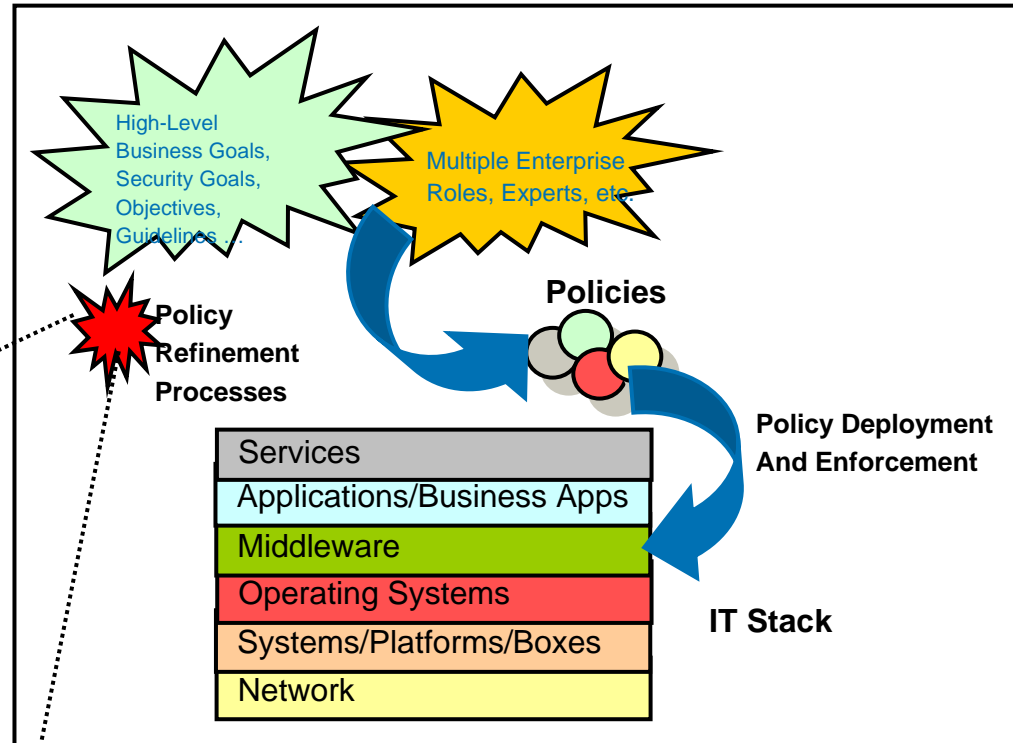| Services |
| Applications/Business Apps |
| Middleware |
| Operating Systems |
| Systems/Platforms/Boxes |
| Network |

IT Stack

Enterprises/Organisations

Policy Refinement: POWER Prototype

1998

- Understood the importance of "bridging" high-level goals & policies with policies at the IT level.
- Good "academic" success
- Got some attention from HP business units

High-Level Business Goals, Security Goals, Objectives, Guidelines…

Multiple Enterprise Roles, Experts, etc.

Policy Refinement Processes

Policies

Policy Deployment And Enforcement

Services
Applications/Business Apps
Middleware
Operating Systems
Systems/Platforms/Boxes
Network

IT Stack

Expert Policy Writer

Graphical User Interface

Policy Wizard Engine

Policy Template Library

Deployable Policy

Information & System Model
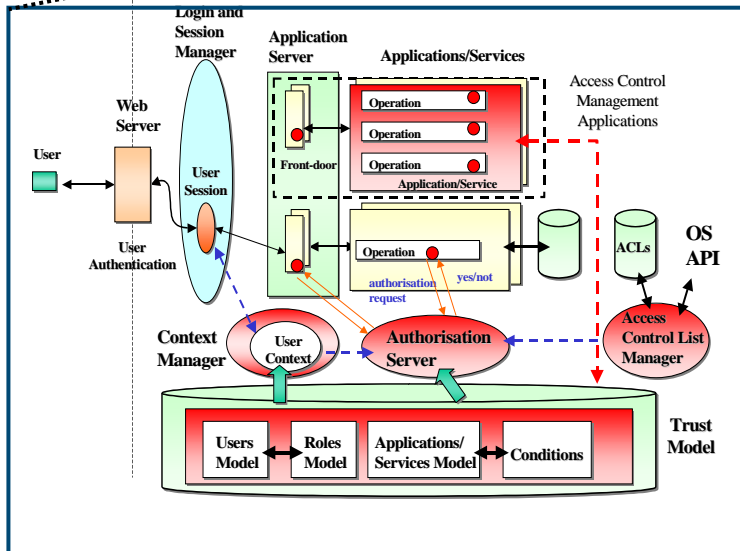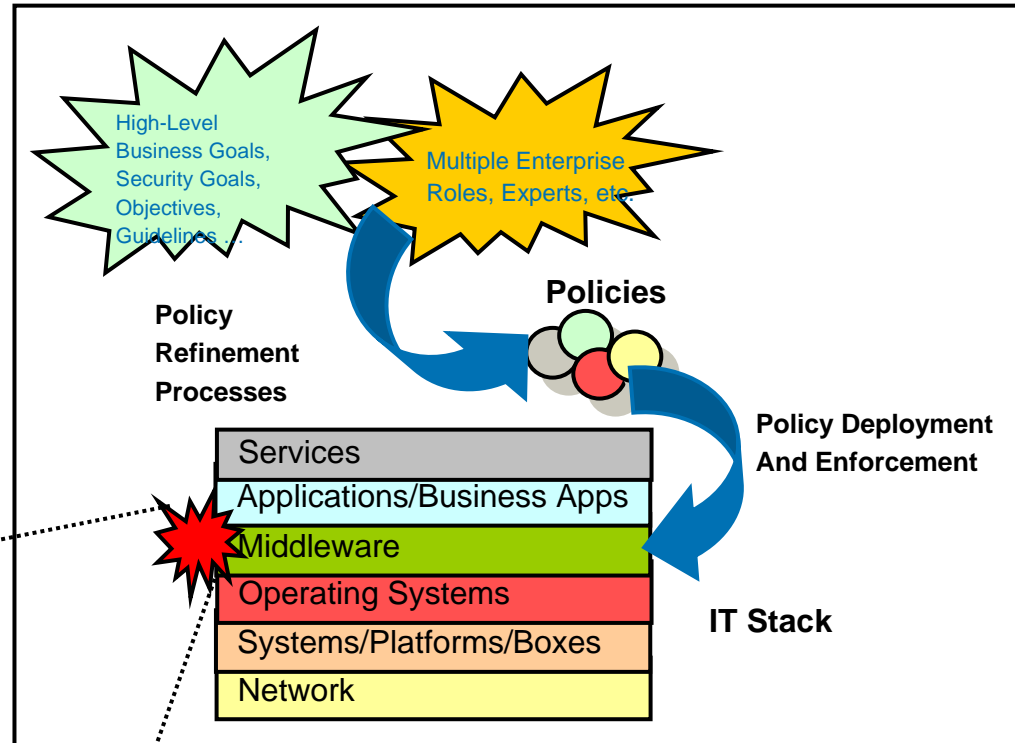
Policy Deployer

Device Mapper

Managed System

X
- Too early. Enterprises/Orgs not ready
- Too general-purpose approach …
- No clear definition of high-level processes
- Over-simplified understanding of high-level policy and guideline definition steps
  → seen them from an IT perspective, NOT a business perspective (involving risk/cost management, etc.)

ACSIS: "Rich", App-Level Authorization Policies

1999

- Focused on more pragmatic types of Policies at App/Service level
- Bet on B2B, App/Service-driven policies
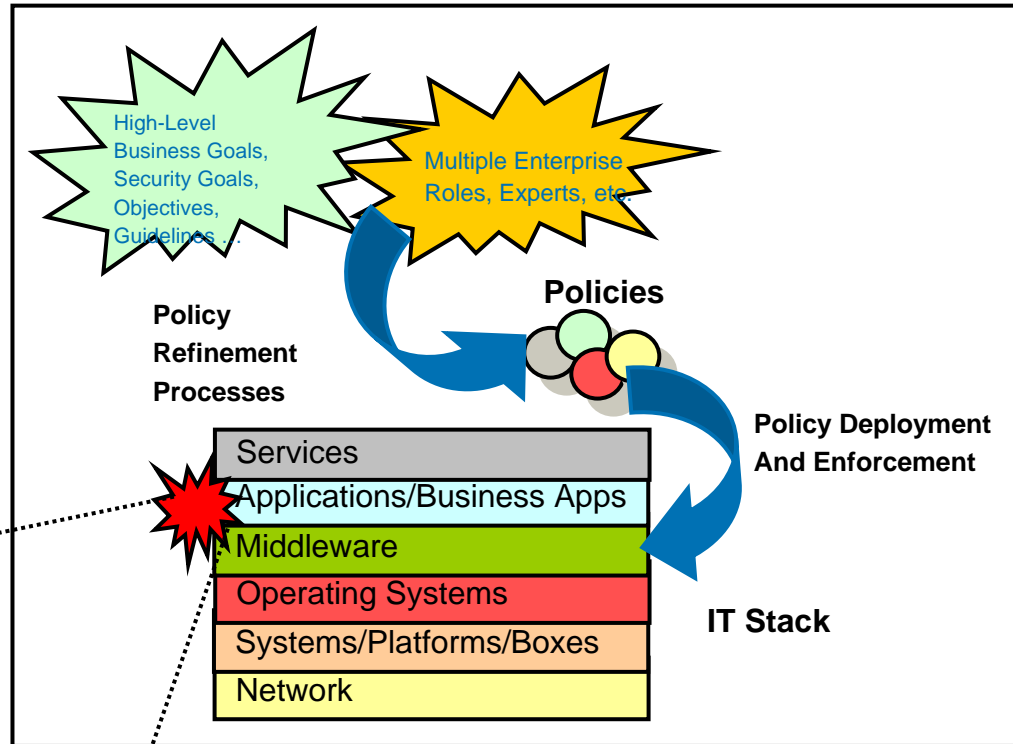- Got good attention from HP business units
- Helped by Internet-hype …

High-Level Business Goals, Security Goals, Objectives, Guidelines …

Multiple Enterprise Roles, Experts, etc.

Policies

Policy Refinement Processes

Policy Deployment And Enforcement

IT Stack
- Services
- Applications/Business Apps
- Middleware
- Operating Systems
- Systems/Platforms/Boxes
- Network

Login and Session Manager · **Application Server** · **Applications/Services** · Access Control Management Applications

Web Server · User · User Session · Front-door · Operation · Operation · Operation · Application/Service · Operation · yes/not · authorisation request · User Authentication · ACLs · OS API · Context Manager · User Context · Authorisation Server · Access Control List Manager · Users Model · Roles Model · Applications/ Services Model · Conditions · Trust Model

X
- A few AAA solutions were already deployed in enterprises → dealing with legacy …
- Despite the added-value, not worth changing legacy solutions
- Too IT focused …
- No transfer to HP divisions …

PASTELS: PKI + Trust Policies + Authorization Policies

2000-2002

✓ • Focused on "missing" policy aspects: trust policies, jointly with PKI infrastructure and authorization
• Bet on B2B and PKI adoption
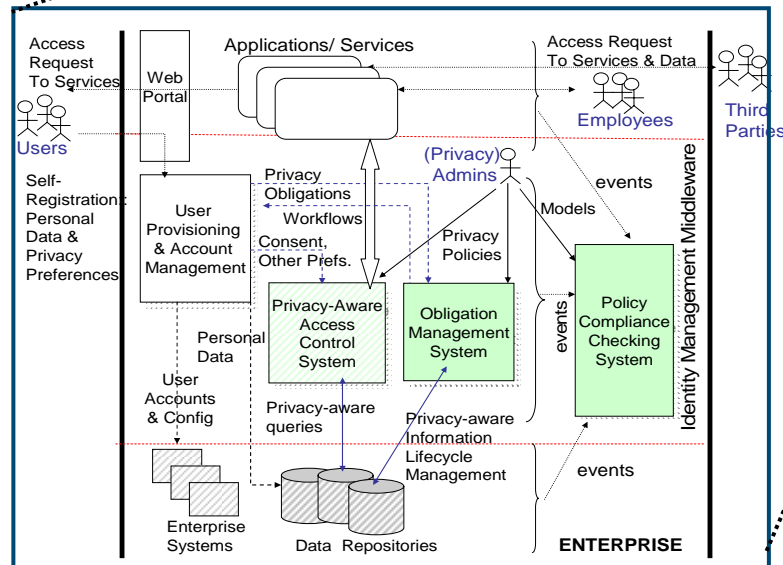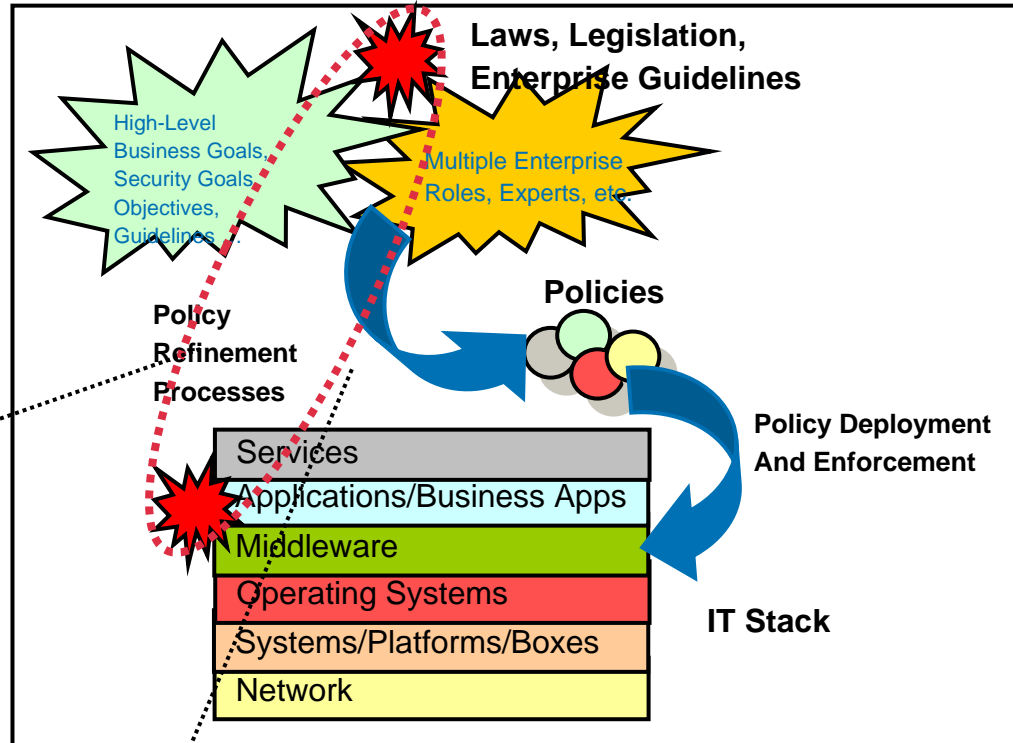• Got good attention from HP business units & Exhibitions
• Helped by PKI-hype

High-Level Business Goals, Security Goals, Objectives, Guidelines …

Multiple Enterprise Roles, Experts, etc.

Policies

Policy Refinement Processes

Policy Deployment And Enforcement

Services
Applications/Business Apps
Middleware
Operating Systems
Systems/Platforms/Boxes
Network

IT Stack

Remote Enterprise / E-Services / Enterprise diagram

X • PKI and trust management have not actually become a priority for enterprise. No widespread adoption
• Again, too IT focused …
• No dynamic B2B adoption …
• No transfer to HP divisions …
• Internet burst - end of a cycle …

hp invent
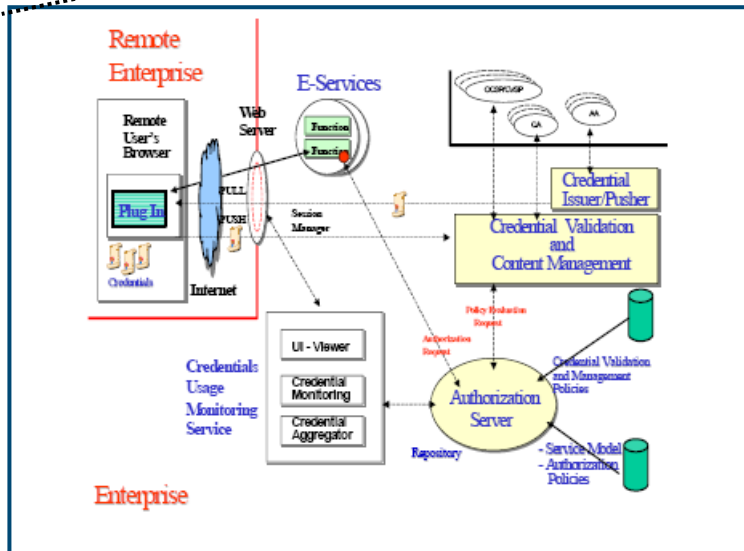
Privacy-aware Policy Management …

2004-2007 …

- Addressed Policy Management problem from Business, Legislative & Users perspective → real needs (compliance, data governance, etc.)
- Leveraged Existing Enterprise Identity Mgmt Solutions
- Got good "Academic" attention (conference papers, etc.)
- Technology and Knowledge transfer to HP business units

Laws, Legislation, Enterprise Guidelines

High-Level Business Goals, Security Goals Objectives, Guidelines …

Multiple Enterprise Roles, Experts, etc.

Policies

Policy Refinement Processes

Policy Deployment And Enforcement

Services
Applications/Business Apps
Middleware
Operating Systems
Systems/Platforms/Boxes
Network

IT Stack

X • Targeted area is still a "niche"-area
- Business priorities on other types of compliance (e.g. SOX compliance)
- Auditing as important as enforcement …
- Increasing relevance and importance of Business-driven IT management and focus on policies in this space …

What success stories does the policy research community have to show for these ten years of research in terms of real business impact?

- Academic "Successes" do not imply Industrial/Business Success

- We (as HP Labs) had success stories and business impact
  - in terms of Technology and Knowledge Transfers -
  when <u>Aligned</u> with Business (and Users) Needs:
    - → Example of Privacy-aware Policy Management
    - → Example of Policy Management in Federated
        Identity Management Context
    - → Example of "Sticky Policies" associated to Valuable/Confidential Data

- Clear perception of added value at the Business-level

- Importance of Leveraging Legacy and State-of-the-Art Solutions. No willingness of businesses to throw away past investments → conservative approach

What was envisaged ten years ago that did not materialize, and what are the reasons for that?
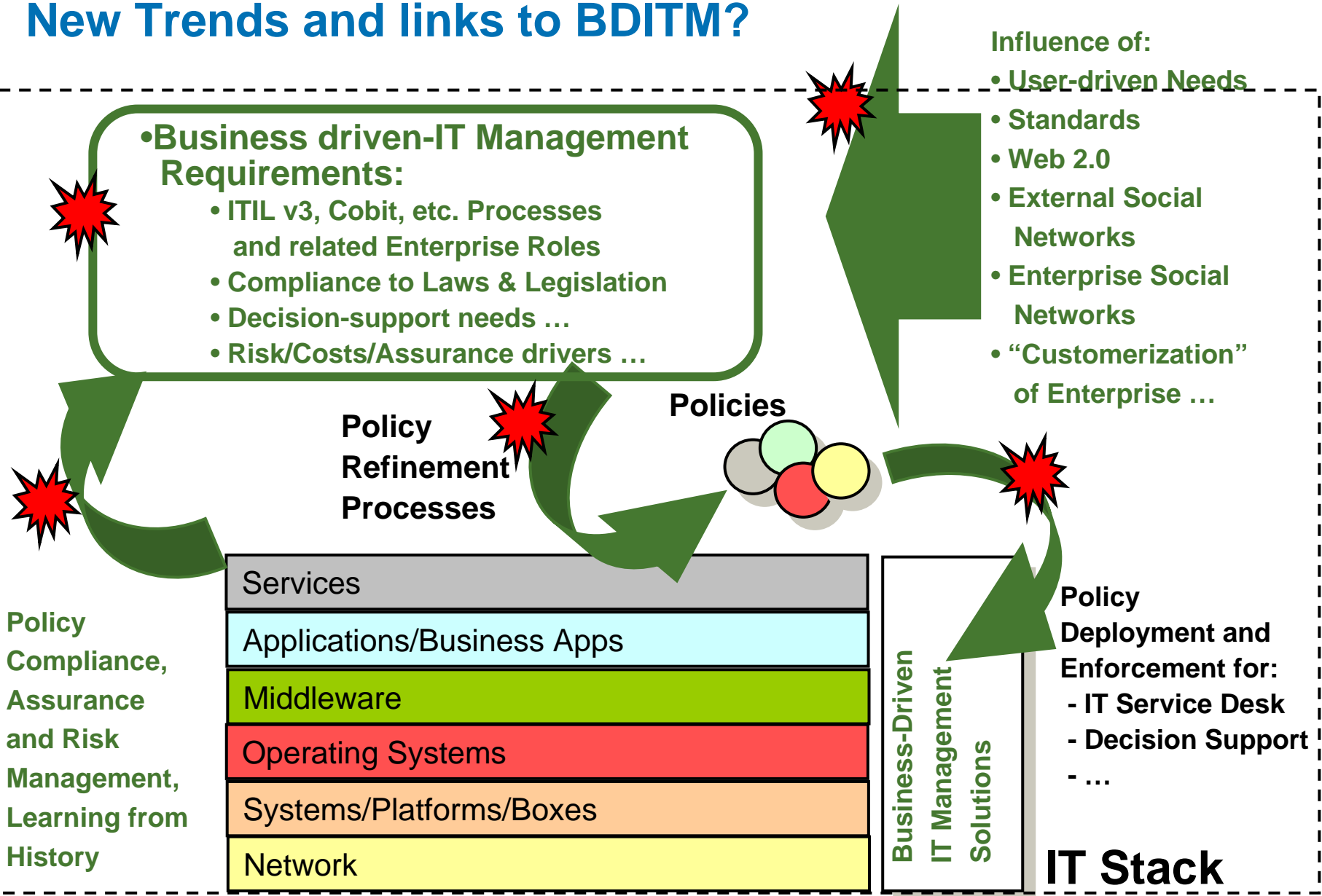
- General-purpose Approach to Policy Refinement & Management
  - Unrealistic: too many different IT Layers and related Requirements
  - Unrealistic: underestimated/lack-of-knowledge of processes and decision-making mechanisms at the business-level

- IT-focused Approach to Policy Management:
  - Unrealistic: first understand business needs and drivers
  - Often too much advanced technical functionalities - in terms of policy management – that are not really required by enterprises/organisations
  - Reality-check: Business-driven IT Management

- "Ideal" Approaches, based on "Starting from Scratch":
  - Unrealistic: first understand current legacy constraints and existing solutions. Consider cost/benefit of requiring to changes

Is the community still investigating these issues?
What is the likelihood of success if so?

Yes, but with a more Pragmatic and Business-driven Approach:

- Policy Refinement & Management for IT solutions:
  - <u>Driven by business: (involving risk/cost analysis, etc.)</u>
  - Based on business IT standards & processes, such as ITIL, COBIT, e
    - → How to Refine these types of Policies/Guidelines
    - → How to Deploy and Enforce these Policies
    - → How to Deal with Compliance and Governance aspects
  - <u>Focused on key areas</u>, such as IT Support, Help Desk, Quality of Service and SLA, Decision Support
    - → Very Important Areas subject to High Investments

- Reasonably High Likelihood of Success, if R&D work is <u>NOT Done in Isolation</u> but involving Industry and Business Units and <u>Continuously Cooperating</u> with them

New Trends and links to BDITM?

Influence of:
- User-driven Needs
- Standards
- Web 2.0
- External Social Networks
- Enterprise Social Networks
- "Customerization" of Enterprise …

- **Business driven-IT Management Requirements:**
  - ITIL v3, Cobit, etc. Processes and related Enterprise Roles
  - Compliance to Laws & Legislation
  - Decision-support needs …
  - Risk/Costs/Assurance drivers …

Policy Refinement Processes

Policies

Policy Compliance, Assurance and Risk Management, Learning from History

Policy Deployment and Enforcement for:
- IT Service Desk
- Decision Support
- …

IT Stack
Services
Applications/Business Apps
Middleware
Operating Systems
Systems/Platforms/Boxes
Network

Business-Driven IT Management Solutions

Towards Enterprise Web 2.0 …