

Towards a Secure Internet of Services: An Architectural View

Volkmar Lotz
SAP Research

February 10th, 2010

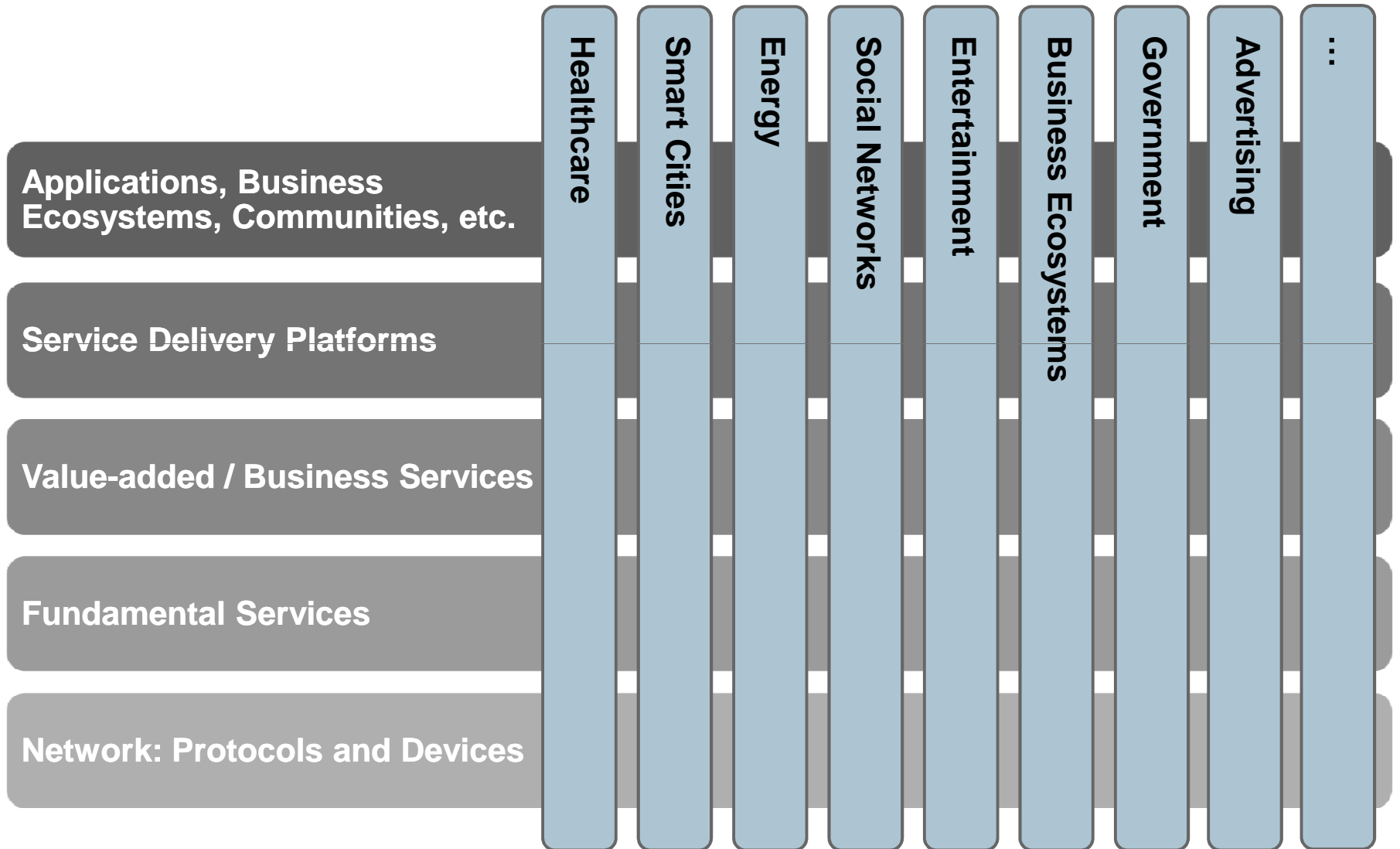
THE BEST-RUN BUSINESSES RUN SAP



Butler Lampson in Nov. 2009 issue of CACM:

- Security is not about perfection
- “If you want security, you must be prepared for inconvenience” (words of General B. Chidlaw, 1954)
- Security is about economics

Future Internet Applications and Services are highly diverse



Impact of diversity on Security & Trust



The FI is not expected to be generally secure and trusted (i.e., always and everywhere)

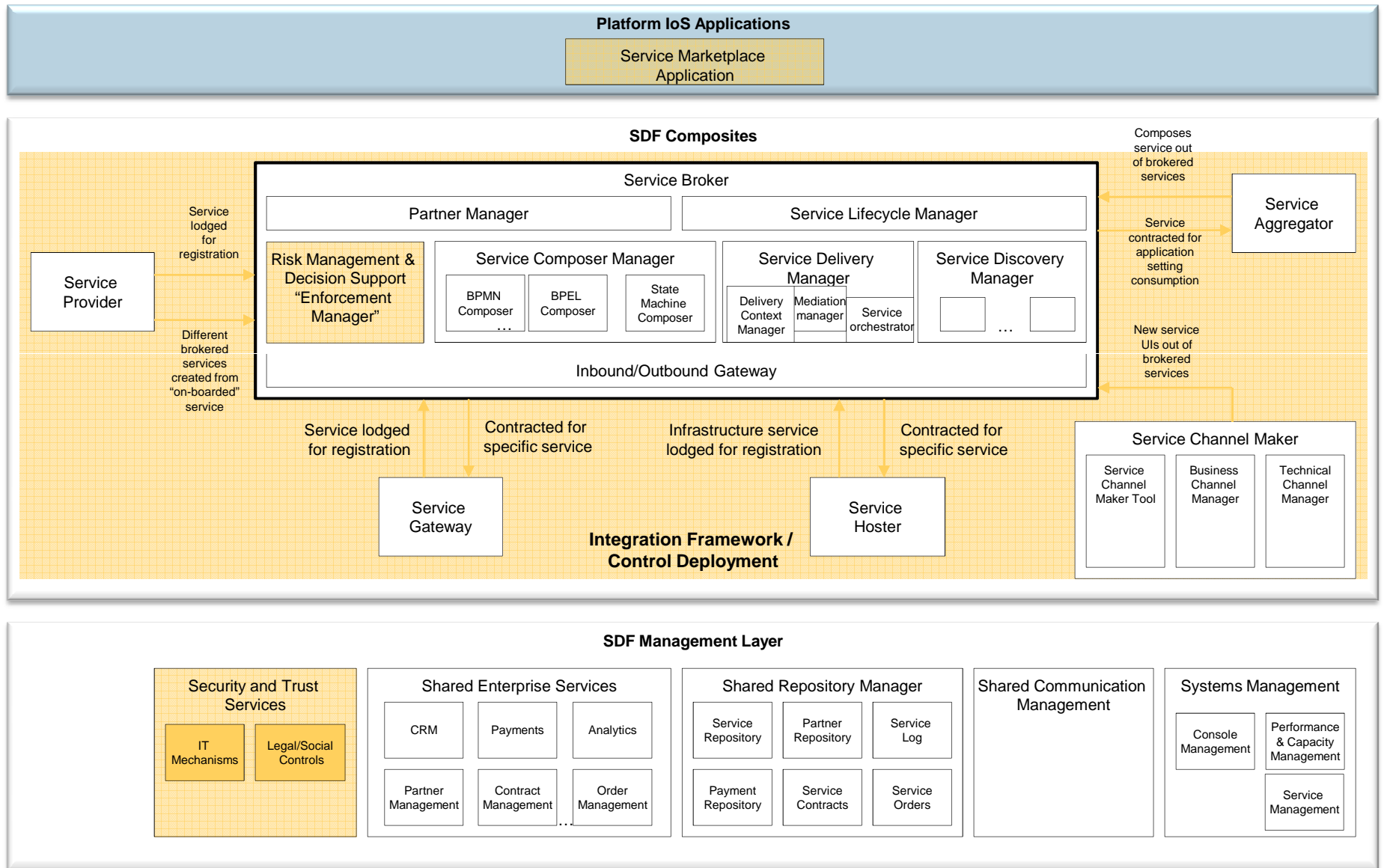
Different applications and stakeholders have differing protection needs

Paradigm shift in attack models: malicious service providers and consumers

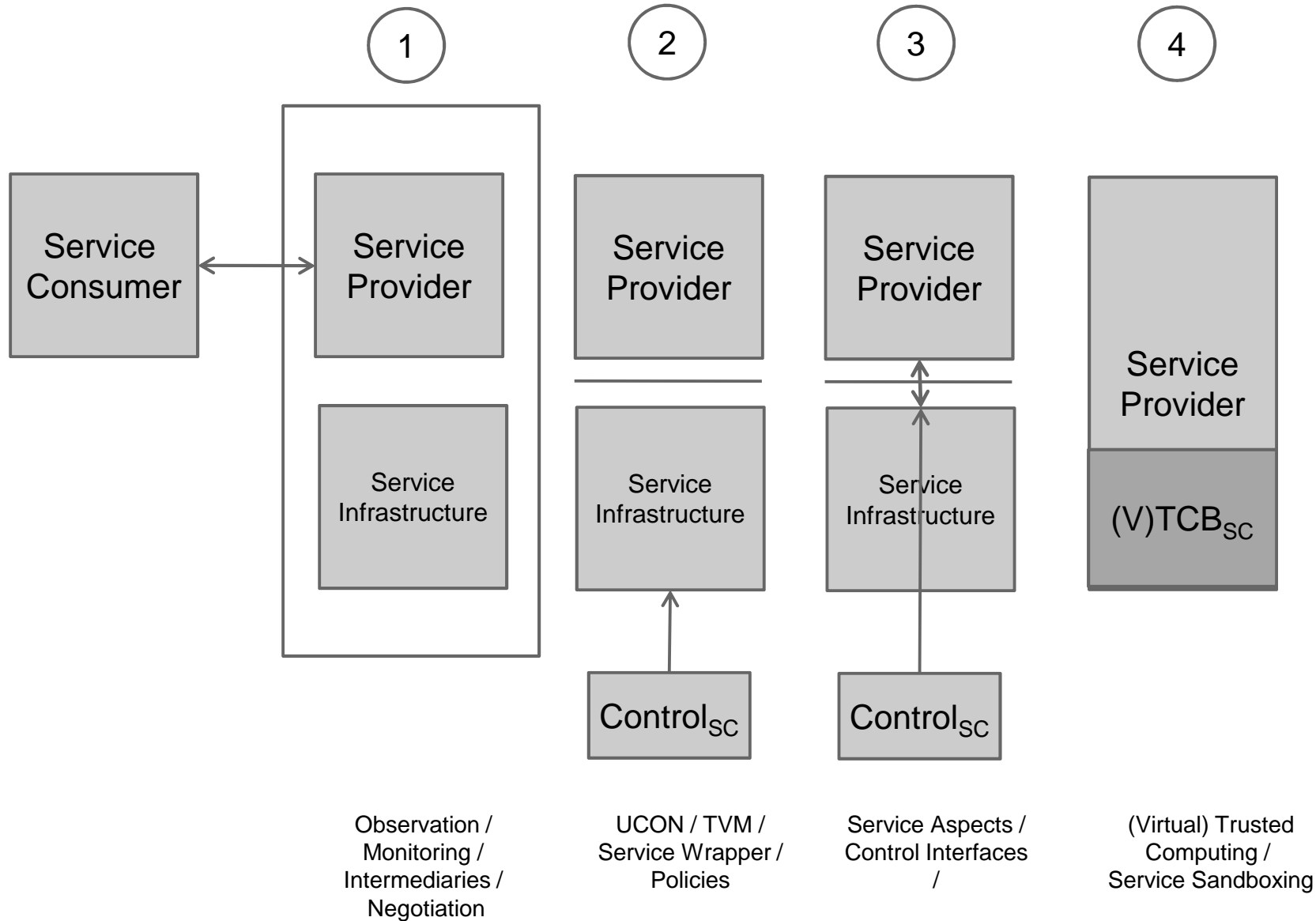
- Build trusted environments on-demand based on risk analysis and a spontaneously deployable set of mechanisms (“toolbox”)
- The toolbox needs to serve different “deployment” models, taking ownership, trust relations and technology into account
- Mechanisms range from the provision of incentives (e.g., social control) to enforcement of security properties (e.g., privacy preserving computing)
- Guidance through risk assessment and management methodology and tools
- Mechanisms as well as guidance and deployment support need to be available through all layers (“framework”)
- Design the architecture such that this model is supported (and, most important, usable)

→ We talk about a unified architectural view designed to be instantiated to meet context specific security needs

Integration of security services in a service delivery framework



Scalability to Service Deployment Models in Case of Control / Incentives





Technical environment

Business environment

Service specification: “Control APIs” → invasive access

Service description

Non-functional properties: performance, reliability, usability

“Feature Interaction”

<http://www.internet-of-services.com>