Five years of emerging security

Sam Hartman

JANET Networkshop 39

April 13, 2011

Goals

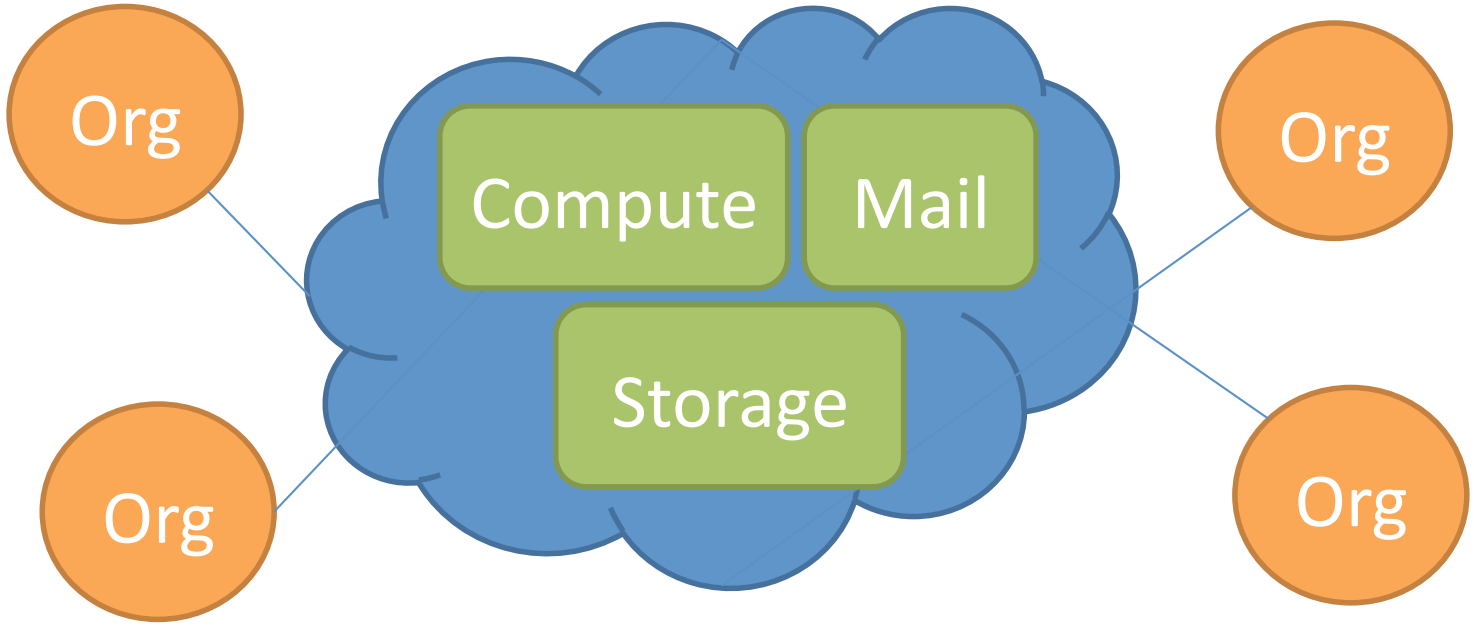
- What changes to the network should we expect over the next five years?
- What challenges do these pose to network security?
- How should we meet these challenges?

Today's network

- Firewalls and access authentication establish the network perimeter.
- VPNs, partner networks and collaborations create well-defined holes in the perimeter.

- Characteristics:
  - Static configuration of security.
  - Important distinction between *Inside* and *Outside*.

The Cloud

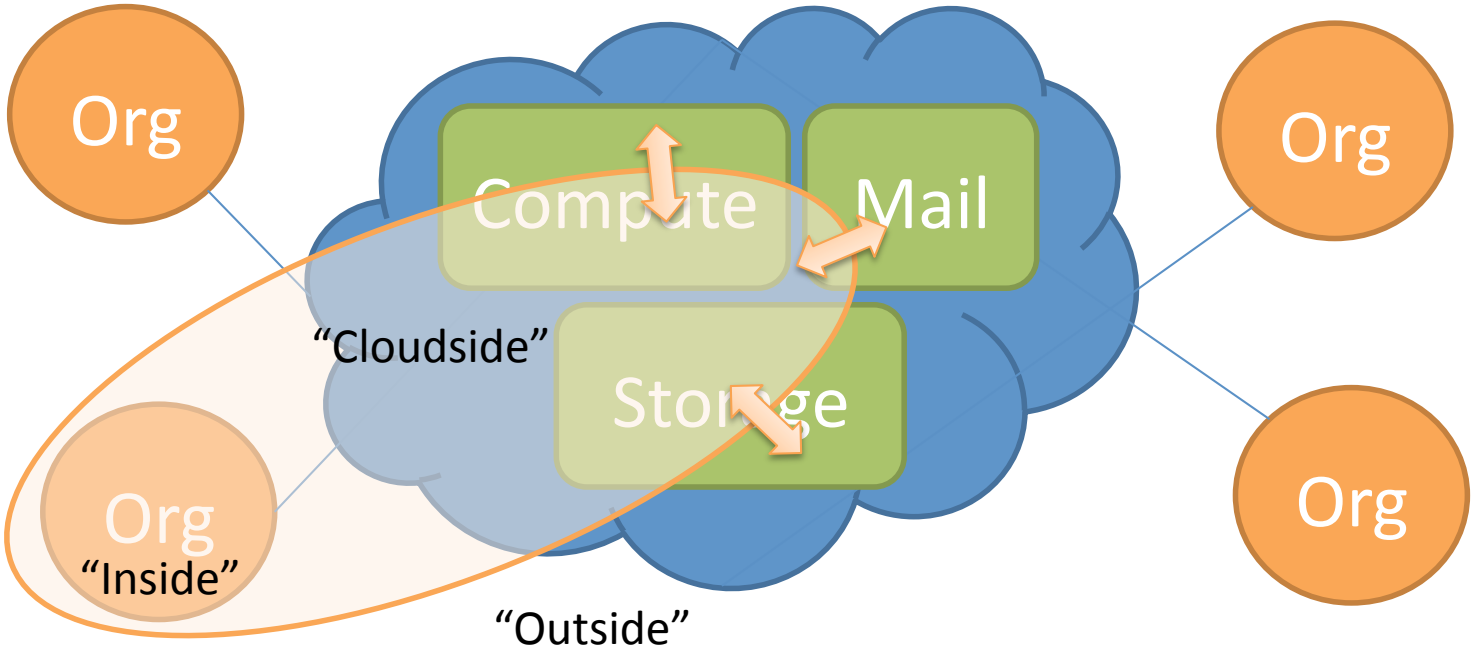


- The cloud promises economies of scale; the ability to re-use components to construct more composite services; as well as complete services such as mail and calendar.

Effects of the Cloud

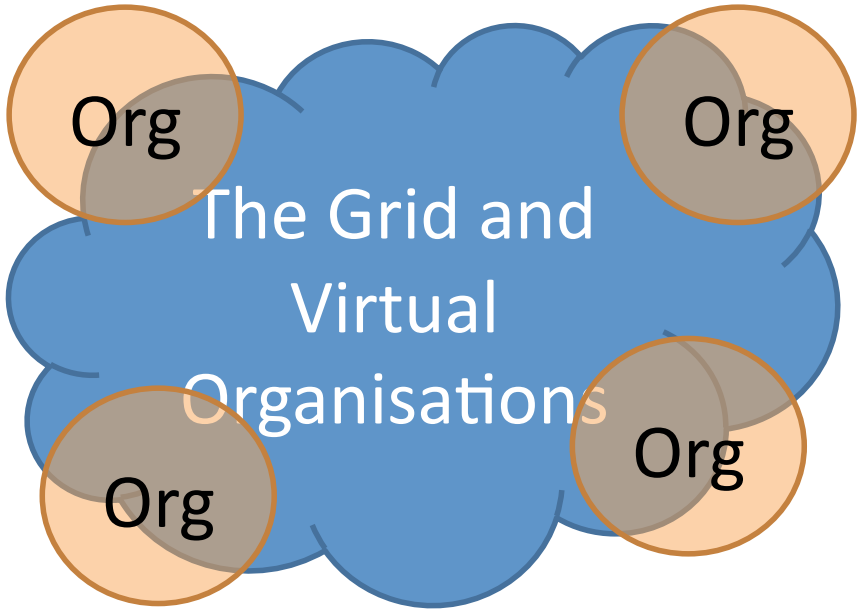
- Data housed outside of the organisation.
- Challenge: what data must remain within the organisation?
- External services benefit from connecting to internal infrastructure.
- Leading to connections across security boundaries.

Inside, Outside and the Cloud



- Today, "Inside" and "Outside" are defined by security policy acting on network topology.
- Soon, "Cloudside" will be defined by business relationships, and controlled by policy acting on identities of users, applications and organisations.

Grid computing



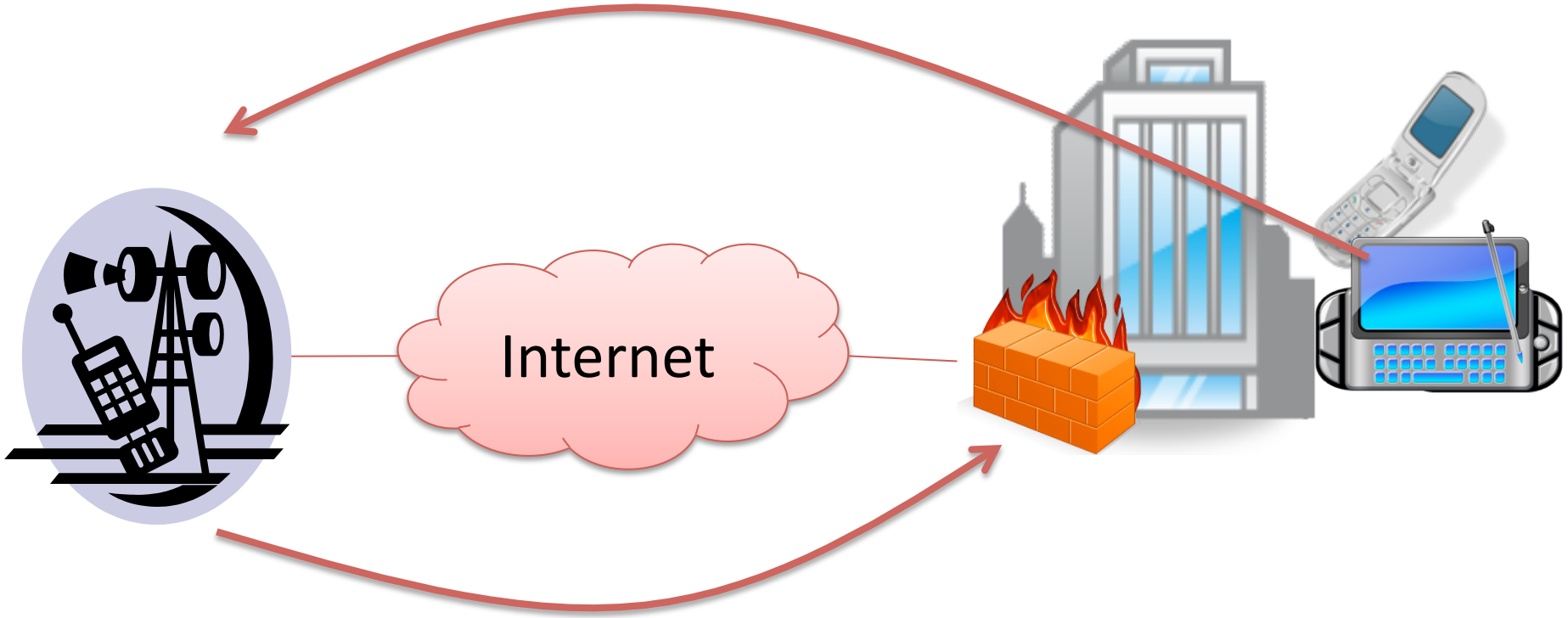
- In addition to the challenges of the Cloud, the Grid brings others' data and code into a network.

Collaborations continue

- Visitors to your organisation will continue to expect more and better:
  - Access to home services.
  - Access to visited services for collaboration.

- Greater requirements on identity management.
- More extensive federation so your affiliates gets these benefits when visiting elsewhere.

Mobile devices



Mobile devices appear to be outside the network, even when physically present. Users do not know, and cannot easily control, what connection is used.

Invasion of the Internet of Things

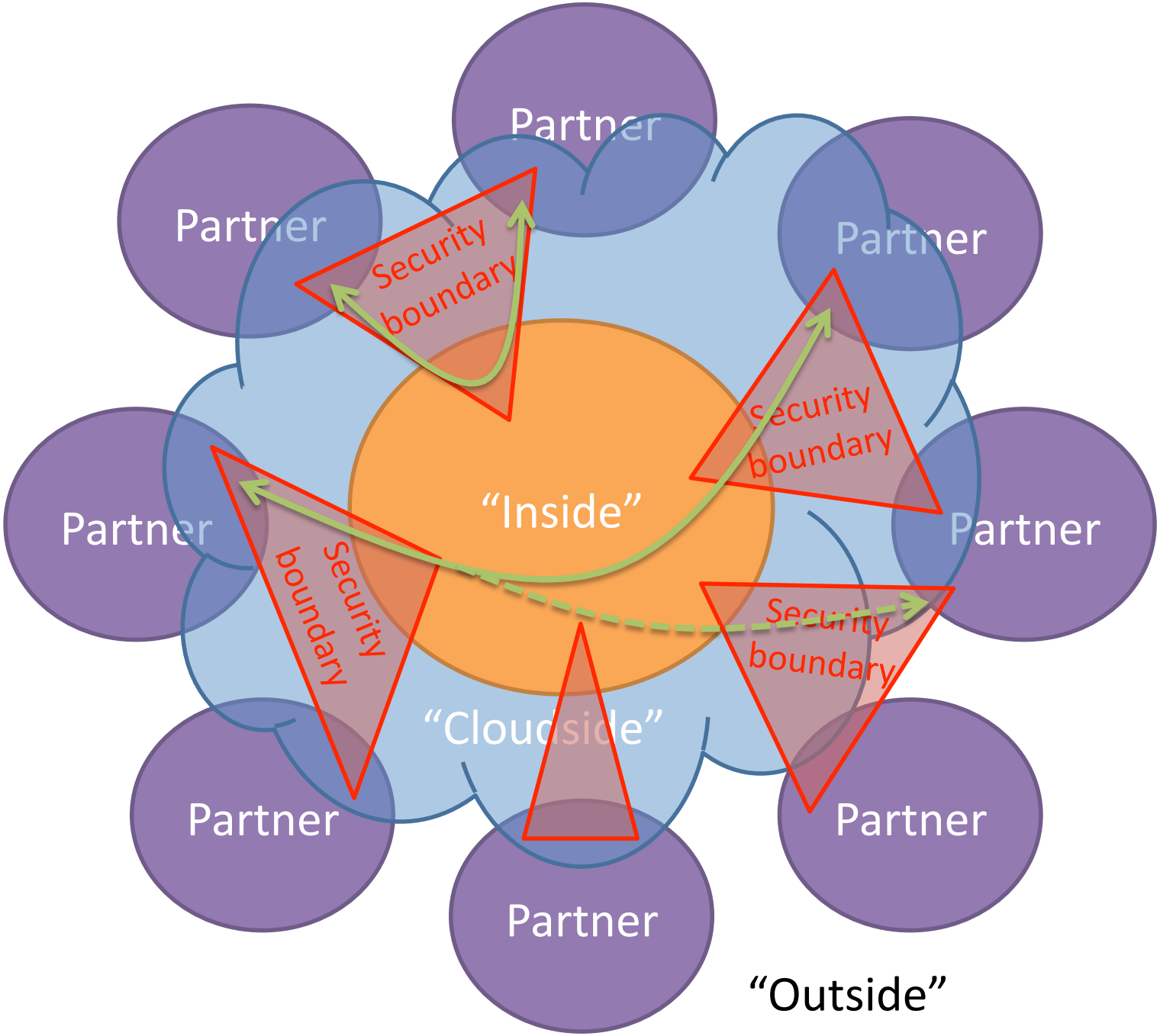
- Media appliances and projectors now…
- …smart energy, sensors, automation and consumer devices soon.
- Segregating these devices will not work: they want to interact with other computers and devices on the network.
- Estimate three devices per room in new construction.

Virtualisation

- Goals
  - Rapid response to changes in demand.
  - Economies of scale.
- Network, storage and disk are decoupled from physical resources.
- Requirement: dynamic configuration of virtual networks that interact with the physical network.
- Challenge: accounting and auditing that can keep pace.

Summary of security impacts

1. A small number of security boundaries will be insufficient.
2. Boundaries surround projects, applications and groups: not large networks.
3. Data, services, individuals and devices will regularly traverse organisational and network boundaries.
4. Resource access requirements will change rapidly and dynamically.


Partner
Partner
Partner
Partner
Partner
Partner
Partner
Partner
Security boundary
Security boundary
Security boundary
Security boundary
"Inside"
"Cloudside"
"Outside"

Developing policy

- *Inside* versus *Outside* no longer makes sense as a policy focus.
- What data and services need to be shared, and what must remain private?
- When is location an appropriate access-control factor? When not, what should stand in its place?
- What measures are appropriate for accountability and audit?

Strategies for security boundaries

- Move firewalls very close to the services.
- Application security, such as Web SSO, to reach across that boundary; irrespective of whether the user or service is internal or external.
- Small dynamic virtual networks with their own security boundary independent of physical topology.

Federation and Identity Management

- Strong authentication of machines and users is essential for fine-grained security boundaries.
- Authentication provides attributes for authorisation.
- Many organisations – both internal and external – will contribute identity information.
- Federation technology combines these into a coherent access management strategy.

Moonshot

- Moonshot is a JANET(UK) led initiative to develop a state-of-the-art federated access management technology.
- Goal: make federated access management the norm, not the special case.
- Meets emerging security challenges, and learns from existing federation technologies.
- Technology being standardised within IETF.
- Open-source implementation.

Combining security data

- Many sources of security information combined give a reasonable picture
  - Network information
  - Authenticated attributes about user or application
  - Information exchanged with home organisation
- Together, these can form the basis of a dynamic access control decision.

Conclusions

- Policy focused around the dynamic nature of tomorrow's networks gives administrators the tools needed to make decisions.
- Virtualisation, application authentication, and small security boundaries provide tools to enforce policy.
- Federation and identity management carry needed information across organisational boundaries
- Integrating multiple sources of information enhances access control and trend analysis.