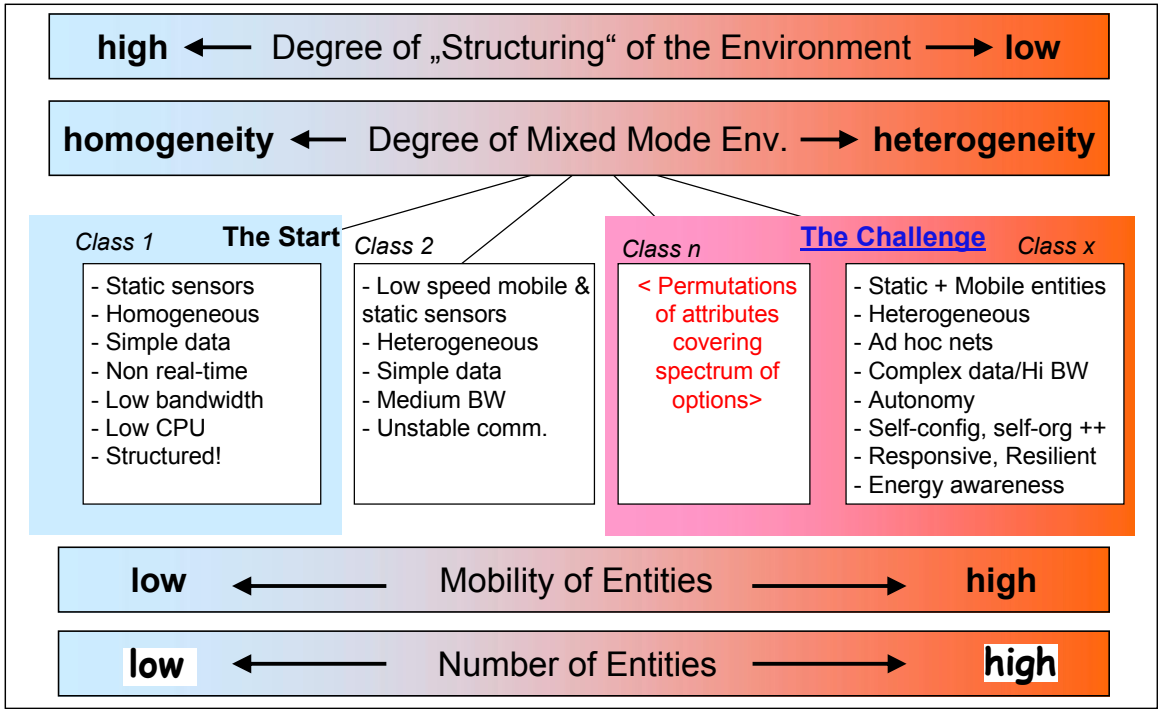
Trustworthiness in the Interconnected World

Neeraj Suri

Dept. of Computer Science
TU Darmstadt, Germany

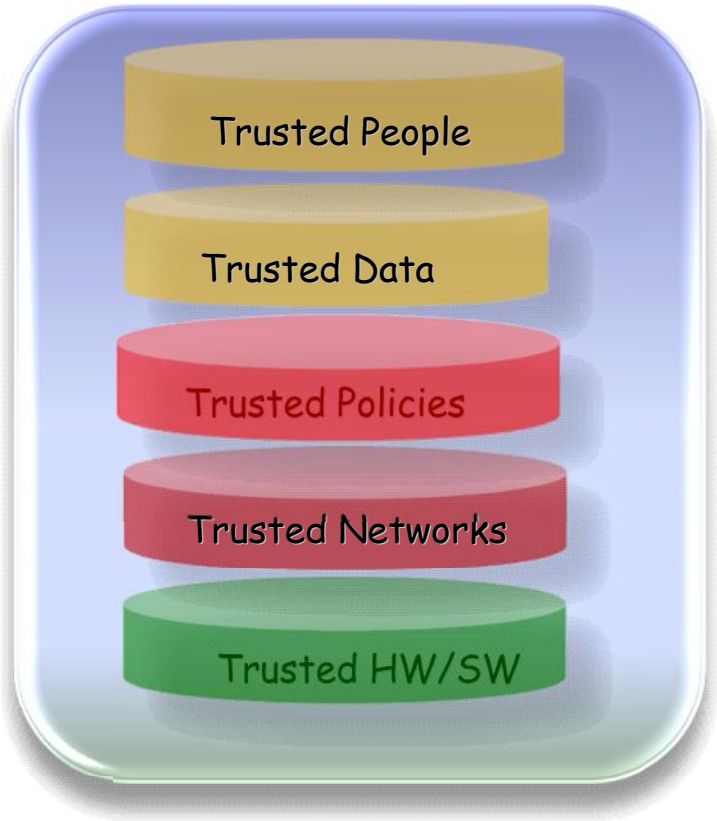
www.deeds.informatik.tu-darmstadt.de
suri@cs.tu-darmstadt.de

The Ecosystem: Networks, IoT & other Cloud-y Things



- Technologies & Systems (Internet, Cloud and the myriad spectrum of devices, infrastructures and services) get used when we are willing to trust them to deliver the services we expect from them irrespective of the disruptions (design, operational or deliberate) encountered by them. This basis of trustworthiness defines their value or the lack thereof!

The Trust Stack



- Trust is an end-to-end attribute.
- Trust is not a piecemeal property. Cyber attacks target the entire trust chain (the blocks, the interfaces and technology changes) for the "weakest link" vulnerability.
- Virtually all e-services are likely (and increasingly by design) networked in either obvious or non-obvious ways …

…and the blocks/infrastructures/services are international!

Google reports China-based attack, says pullout possible

By Jeanne Meserve and Mike M. Ahlers, CNN
January 12, 2010 10:56 p.m. EST

Google reported Tuesday an alleged attack on its US corporate infrastructure last month originating in China.

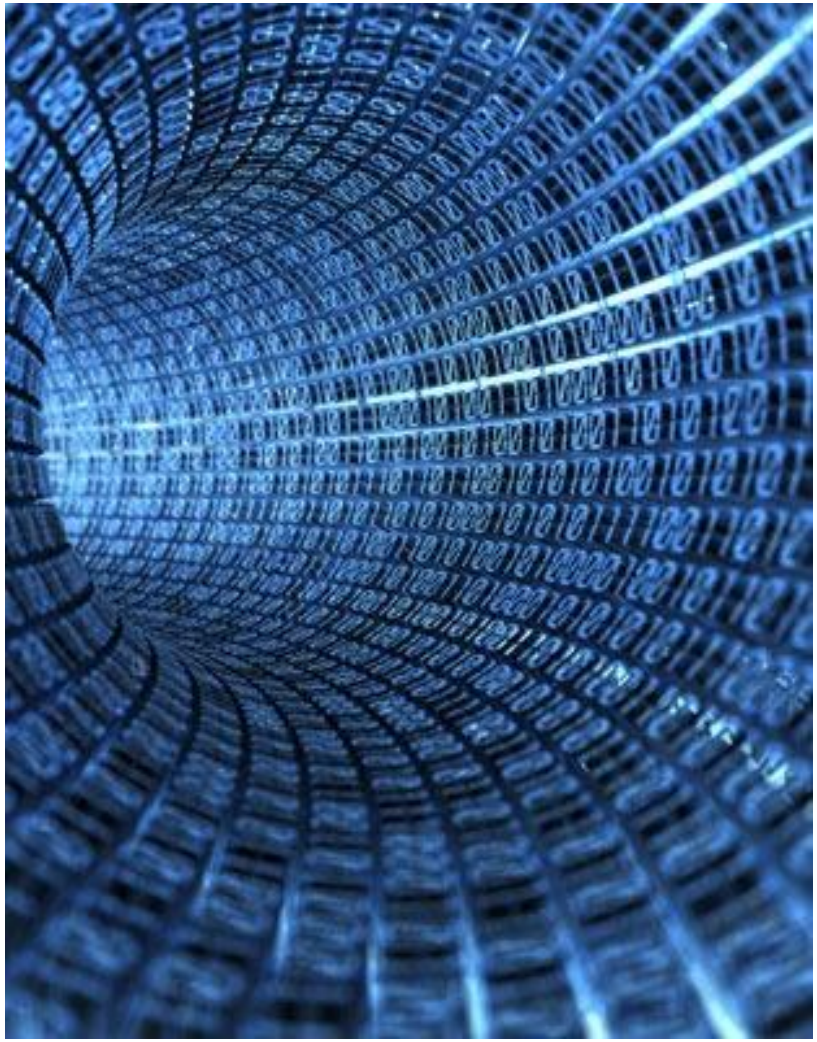
STORY HIGHLIGHTS

- Google says an attack originating from China targeted its US infrastructure
- The attack occurred last month and targeted Chinese human rights activists, the company said
- Google says 20 other companies were also targeted

WASHINGTON (CNN) -- Google said Tuesday the company and at least 20 others were victims of a "highly sophisticated and targeted attack" originating in China in mid-December, evidently to gain access to the e-mail accounts of Chinese human rights activists.

"Based on our investigation to date we believe their attack did not achieve that objective," according to a statement by David Drummond, senior vice president of corporate development and chief legal officer for Google, operator of the most popular Internet search engine.

The connected world runs on Data!



- The "Data" Elements
  - Data Acquisition
  - Data Dissemination
  - Data Storage
  - Data Management/Usage

Data Access, Dissemination, Storage & Legal/Social +++

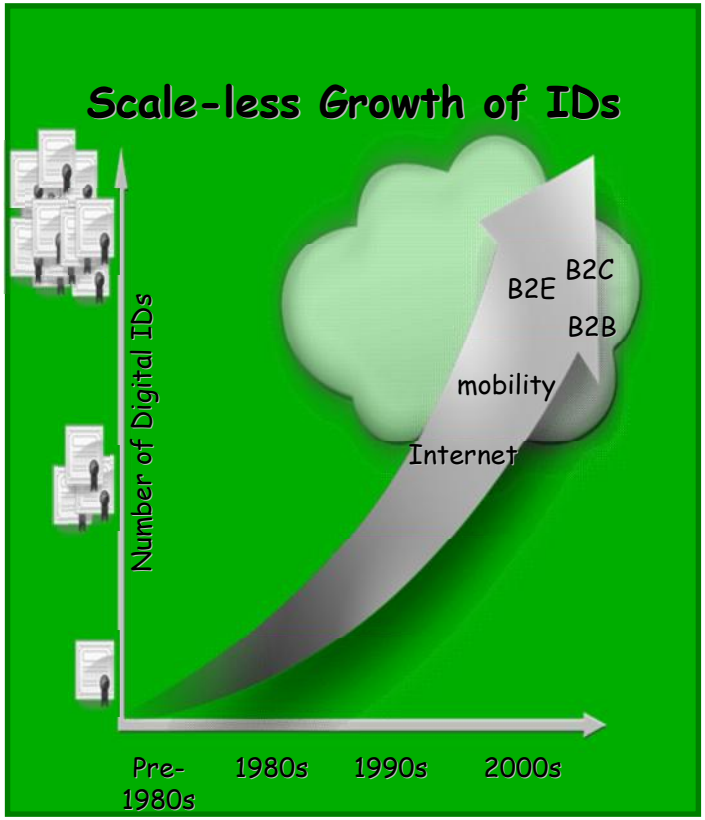
- Services and servers are no longer monolithic or local … global, collaborative computing, P2P, Cloud…
- Data Servers are located worldwide - Google Data Centers
  - For a security breach on the data, who is liable? The data center locale? The owner of the data center? The network?

The Big "Data" Issue: Accountability?

- At what level & by what "trusted" authority ?
- For networks? For services/apps?
- Data – ownership, digital rights
  - Traceability?
  - Browsing data?
  - Account data patterns for trend analysis?
  - Data longevity?
  - Legal ownership & rights?
  - Liability? Governance? Compliance?

- Data Acquisition
- Data Dissemination
- Data Storage
- Data Access

Data ➔ Identity: Provision & Management



- **Physical/Real ID, Virtual ID, Service-Device-Session ID …**
- **ID: Scope & Rights**
  - Individual/Collective/Business
  - Unique? Link to Physical ID?
  - Acquired, transferred…
  - Regulated
  - Authenticated
  - Hierarchical
  - Permanence
  - Scalable?

- Who manages the mgmt, & mgmt of what ID? Policies? How?
- What are the controls (and their accountability)?
- Is there any globally conformal and attributable identity?

The Data Perspective: Common Focus Areas

- While one can come up with many (many many) innovative technological solutions *"your favorite cloud-y approach here"*, do we have a handle on:
  - What constitutes (globally conformal) data ownership and data accountability – individual and institutional?
    - What to monitor, at what level and where – & by who in the intl. chain?
  - What constitutes globally conformal identity?
  - Do we know how to specify and assess trust for liability? quantitatively, reproducibly?
  - What are the quantifiers/metrics of trust (Security & Privacy) based on which one can develop solutions – that are technologically and internationally viable!
    - … and are also invariant to technology changes

The Privacy & Security Interplay

- Multi-cultural/national nuances! The role of technology in trust is also often cultural – what to monitor, how to monitor, who monitors, and issues of data retention…

- **Localized Approaches**: Smart spaces - ID's & authentication? Zero knowledge proofs?

- **E2E Trust-Privacy-Security Envelope:** Measures of privacy? Quantification of Trust-Privacy-Security? Tradeoffs?
  ** Liability and Governance on an international scale?

Social Requirements | **Economic Basis** | **Policies/Political**

The Elements of Cooperation?

- It is a "globally" connected world!
- The issues (access, storage, identity, accountability, liability…) are global (whether we like it or not ☺)
- The solutions necessarily need to be global as well…

…an opportunity for EC cooperation (Objective 1.4, Jan 12)

- … aims to contribute to a trustworthy Information Society based on an ecosystem of digital communication, data processing and service provisioning infrastructures, with trustworthiness in its design, as well as respect for human and societal values and cultures.

- Four main targets
  - Heterogeneous networked, service and computing environments
  - Trust, eIdentity and Privacy management infrastructures
  - Data policy, governance and socio-economic systems
  - Networking and coordination activities

- www.deeds.informatik.tu-darmstadt.de
- suri@cs.tu-darmstadt.de