Information Society
Technologies

ReTrust

FET
Future and Emerging
Technologies

# Panel Discussion on:
# "What Do/Shall We Trust in Networking and Computing?"

## First International Workshop on Remote Entrusting
## October 15-16, 2008
## *Villa Madruzzo* - Trento - Italy

Chair: Yoram OFEK (University of Trento - Italy)

Panelists:

Mikhail ATALLAH (Purdue University – USA)
Christian COLLBERG (University of Arizona - USA)
Antonio MAÑA (Universidad de Málaga - Spain)
Paolo TONELLA (FBK, Trento - Italy)

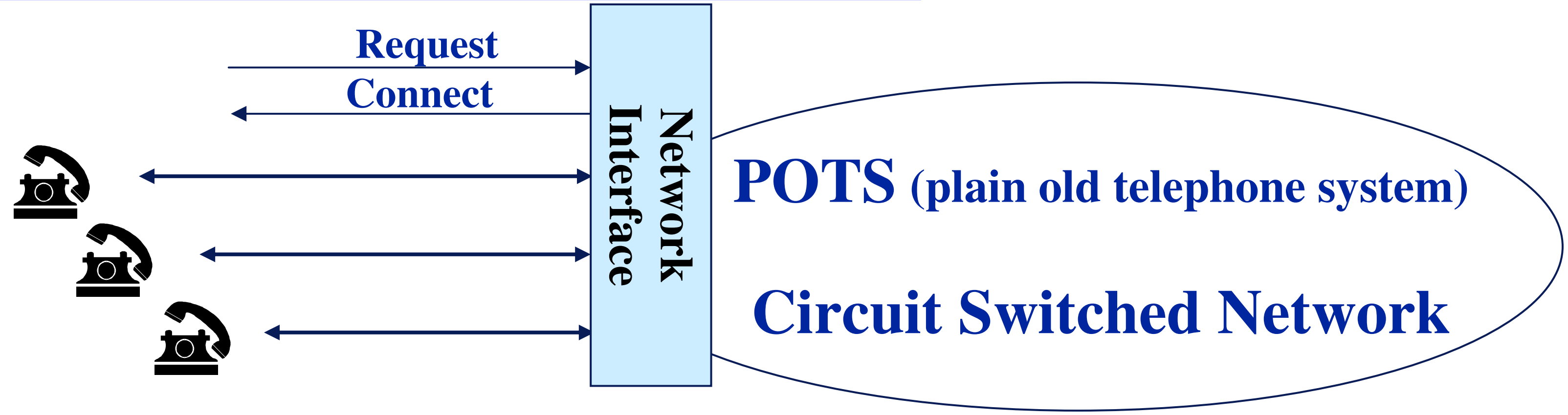
ReTrust

# Once Upon a Time …

- **POTS solution:**

  **(Hard) Wires NO Security and Trust Problems**

**Well-Defined Network Interface for:**
(1) **Isolation** of user from one another
(2) **Protection** of the network from malicious users



Request

Connect

Network Interface

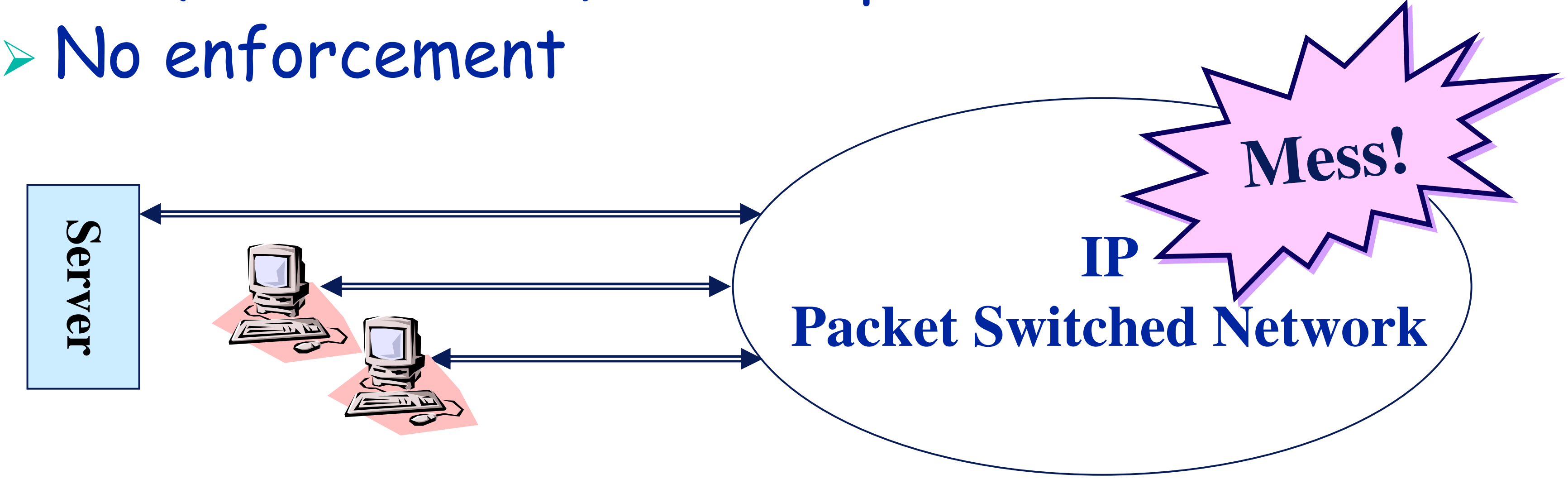
POTS (plain old telephone system)

Circuit Switched Network

**“Well-behaved” User = Telephone**
**(I.e., user cannot modify/control the program”**
**used to control and send data across the network)**

# Internet Basic Problems

- Initially, under naïve secure trust assumptions:
  - No (well-defined) network interface
  - No (well-defined) access protocol
  - No (well-defined) user expected behavior
  - No enforcement



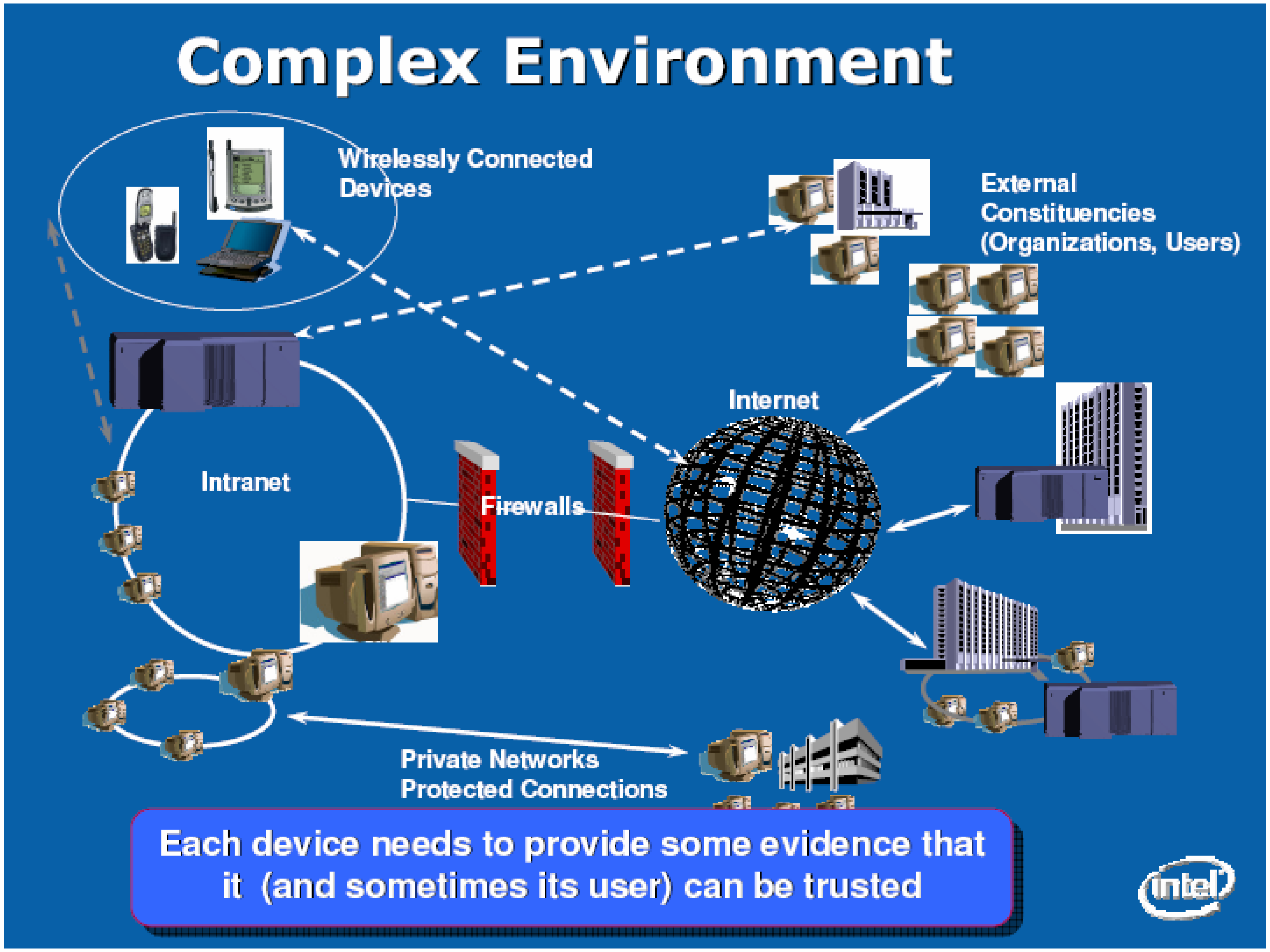
Users = Computers are often NOT "Well-behaved"

# Computing/Networking Convergence

- Exponential growth in **computing/networking**
- Leads to unifying: **computing/networking**
- **All machines/gadgets are interconnected**
- **Ensuring that applications are TRUSTED is critical [Operating as specified]**

- Avoiding manipulation of programs/protocols
  - STEALING content and information
  - DENIAL of service – TCP example
  - FAIR on-line bidding/trading/gaming
  - …
  - … …
  - … … …

# Very High Complexity

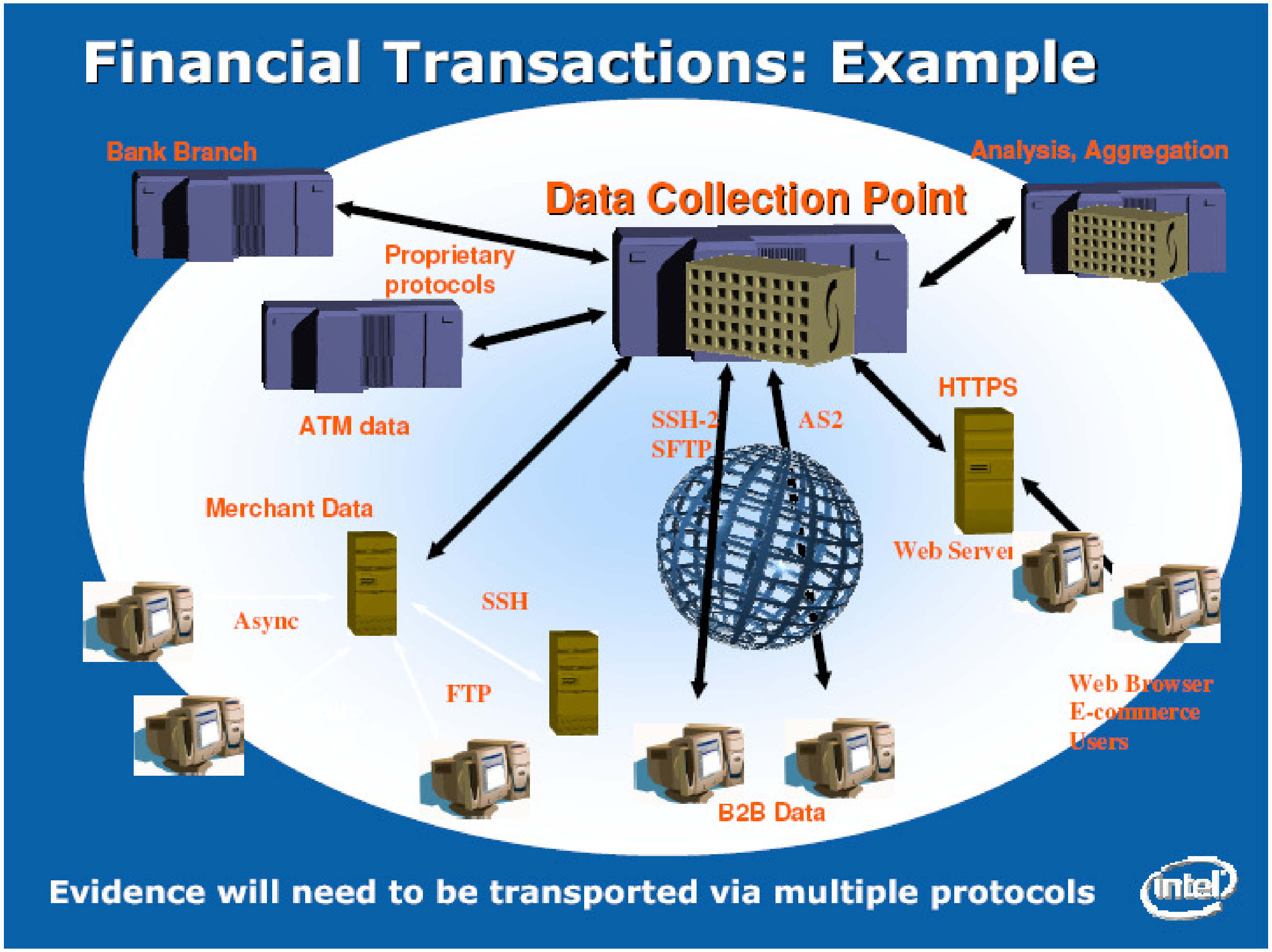


## Complex Environment

Wirelessly Connected Devices
External Constituencies (Organizations, Users)
Internet
Intranet
Firewalls
Private Networks Protected Connections
intel

Each device needs to provide some evidence that it (and sometimes its user) can be trusted

# Very High Complexity



## Financial Transactions: Example

Evidence will need to be transported via multiple protocols

# So …

- What is trust, trustworthy-ness, … ?

- What Can be Trusted?
  - Which network elements can be trusted?
    - Such as: firewall, gateways, server?

- Identity and trust:
  - How to use identity?
    - Signatures/attestation of SW & HW?

# So … (2)

- What is trust and what is security?
  - How shall we distinguish between the two?

# So … (3)

- In remote entrusting we assume that selected networking/computing components can be trusted
  - Trust: "behaves as expected"?
    - Is it realistic?
  - How shall identify and characterized TRUSTWORTHY COMPONENTS

# So … (4)

- Trust and Privacy Dilema
- Identity: user vs. machine
- Authentication: user vs. machine

- Trust and DRM
- Distributed (multi-party) trust
  - Mutual trust