Trust and Security Implications related to Adoption of Emerging Technologies and Internet Economy

Hafedh Gharbi Yahmadi.
ICT Professor at TBS

Which Approach ?

Answer:

We approach it on how it should be managed,

Less Technical with more "Social and economical"

The 4th fourth industrial revolution (human)

- Approximately 12 billion networked "things" worldwide

- By Cisco Analysis : There will be more than 50 billion devices connected to the Internet by 2020

Three 3 main axes to abort the subject of "Cyber risk in an IOT, AI, Cloud...world"

1. Trust, Privacy & Security implications related of emerging technologies
2. Corporate management in digital transformation and risk management.
3. Corporate Governance (Institute the data Governance)

- **Whenever we communicate, we will leave traces of ourselves behind.**

- **Privacy and trust expectations will change**

OLD INTERNET :
FLAT ARCHITECTURE

FUTURE WEB :
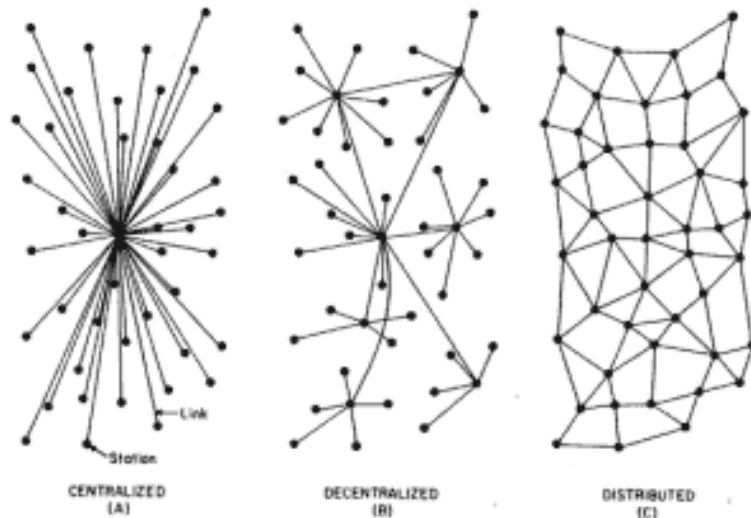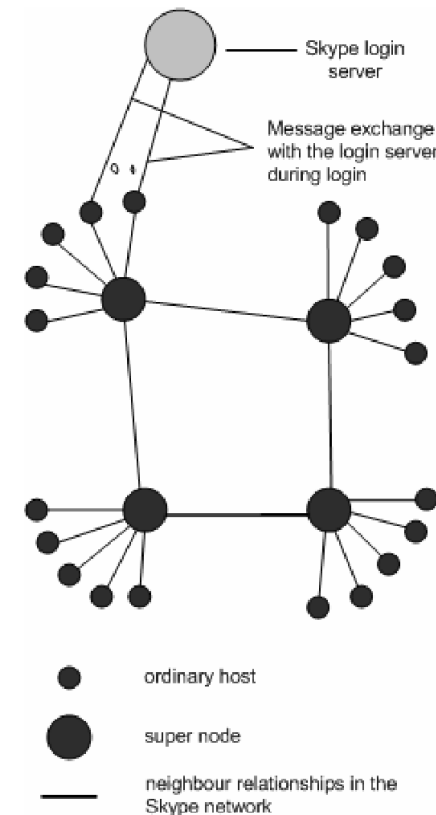**DISTRIBUTED "AGGRESSIVE" SERVICES**

FIG. I — Centralized, Decentralized and Distributed Networks

Emerging technologies don't rely on human intervention to function?
Emerging Tech are increasingly creating entirely new businesses and revenue streams.

Are we ready for the change?

Example : Skype architecture

4

The new landscape in security

ONS

Trans-continent Virtual Organizat

Domino effects

New standard bodies

Quantum Crypto for distribution of secrets

Illicit computations

Spontaneous massive attacks

identification IP addresses

Zetta bytes of data

Physical attacks on individuals,

Overlay, P2P, Grids

XML, Message, document

Intrusion, Malware

DDoS

Asymmetric cryptography

Illicit content

Computer virus

top ten security issues with emerging technologies

1. **Insecure Web Interface**
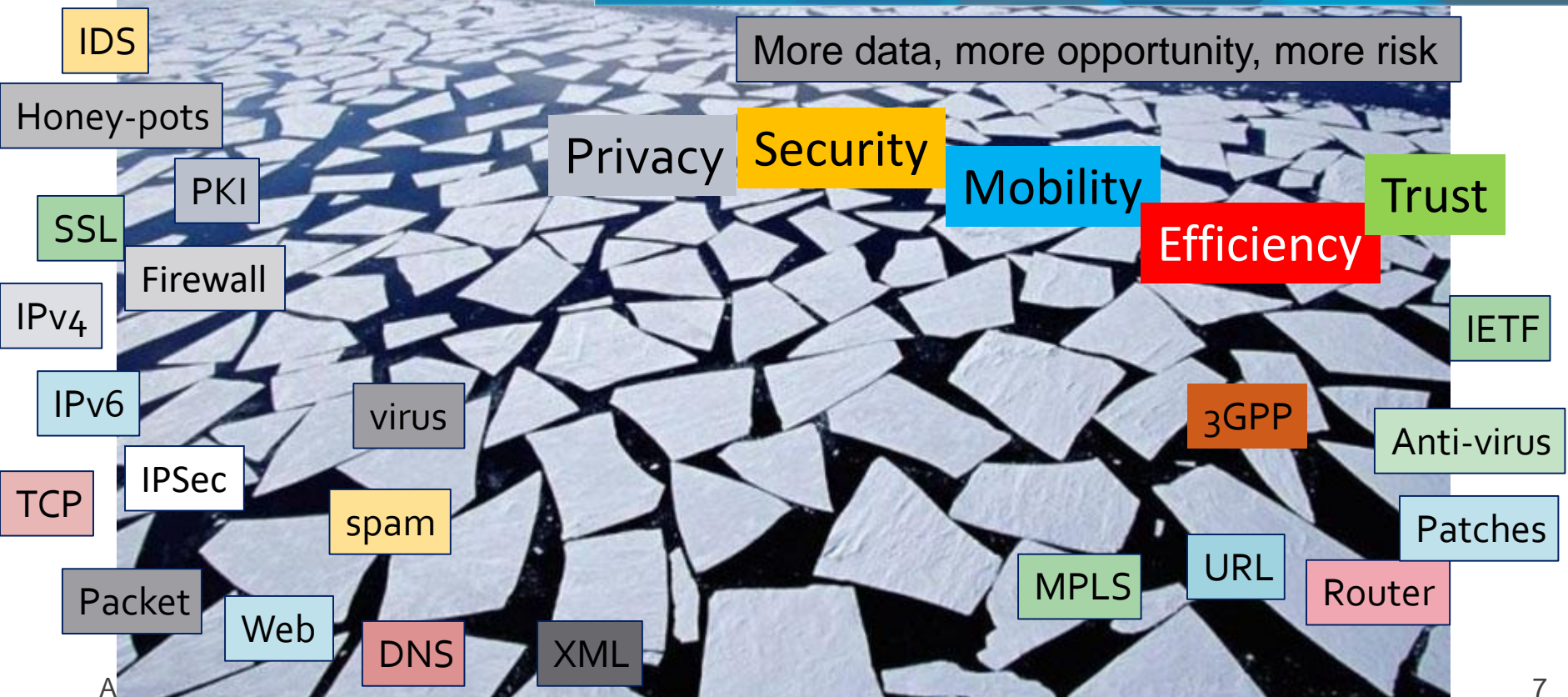2. **Insufficient Authentication/Authorisation** 'poorly protected credentials'
3. **Insecure Network Services**
4. **Lack of uniform standards**
5. **Privacy Concerns**
6. **Insecure cloud interface**
7. **Insecure mobile interface**
8. **Insufficient Security Configurability**
9. **Insecure Software/Firmware**
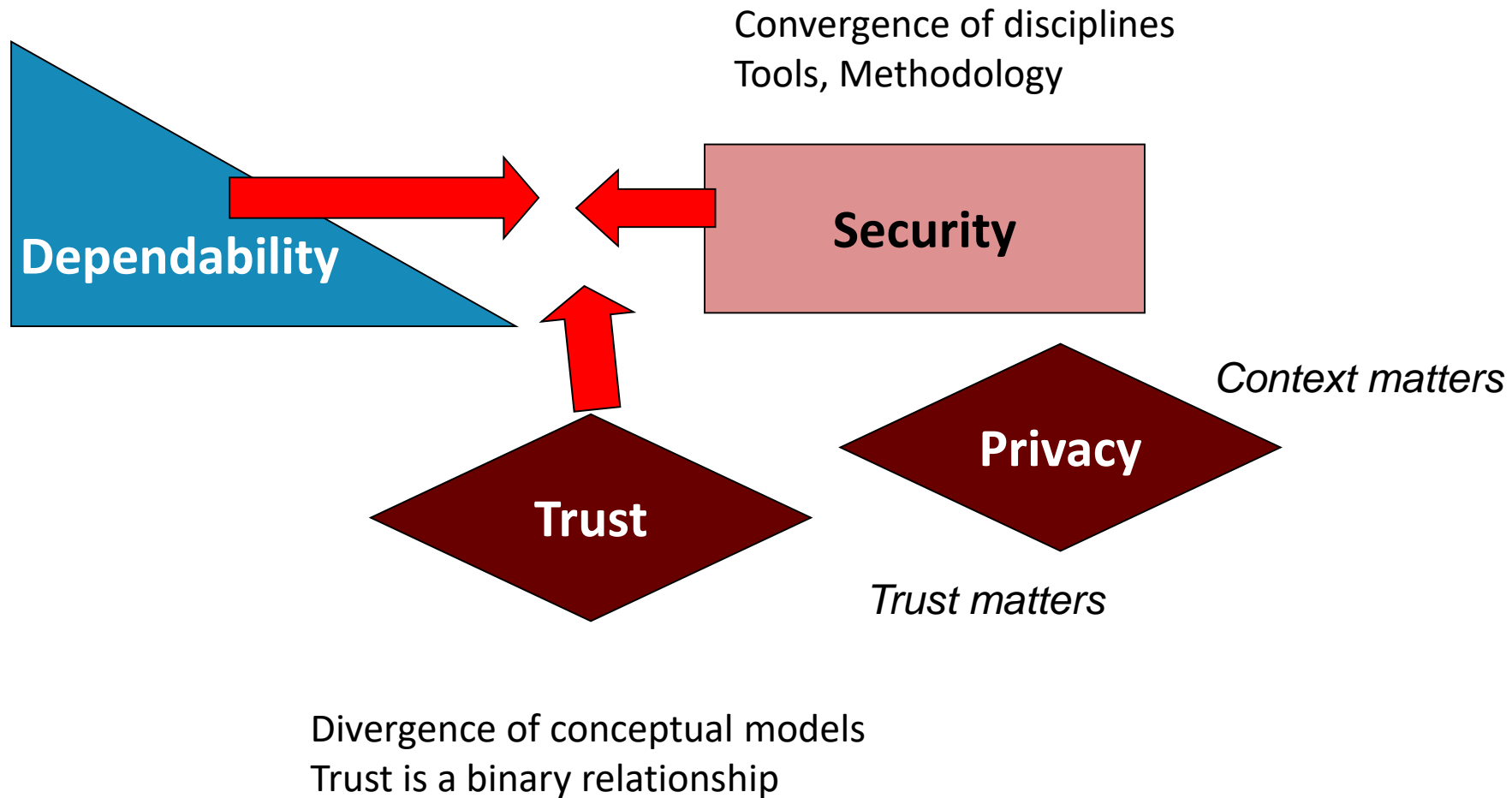10. **Poor Physical Security**

Internet is broken : how to heal the future fragile communications ?

Cyber threat landscape

IoT verticals

Health care | Life sciences	Smart home | Consumer	Infrastructure | Cities	Transport | Urban mobility	Industrial systems | Sensors	
Patient care	Wearables	HVAC	Traffic routing	Speed	Pressure
Remote diagnostics	Smart thermostat	Smart city	Telematics	Temperature	Light
Bio wearables	Pet feeding	Smart building	Smart parking	Flow	Position
Food sensors	Smoke alarm	Waste management	Public transport		
Equipment monitoring	Refrigerator	Temperature control		Motor	Fan
Elderly monitoring	Washer	Electric vehicle		Heat/cool	Lam/laser
	Home security			Valve	Robot arm

IDS

Honey-pots

PKI

SSL

Firewall

IPv4

IPv6

virus

IPSec

TCP

spam

Packet

Web

DNS

XML

More data, more opportunity, more risk

Privacy **Security** **Mobility** **Trust**

Efficiency

IETF

3GPP

Anti-virus

Patches

MPLS URL Router

1- Trust, Privacy vs Security implications of emerging technologies

Convergence of disciplines
Tools, Methodology

Dependability → ← **Security**

Context matters

↑ **Trust**

Privacy

Trust matters

Divergence of conceptual models
Trust is a binary relationship

1- Trust, Privacy vs Security implications of emerging technologies

What's the difference between security and privacy?

In fact both can be difficult to define, and can mean different things to different stakeholders.
Should be debated over and developed by society

What's privacy vs Security and trust, emerging technologies are reshaping the privacy definition, many new interpretation of what privacy really mean to individuals while using this emerging technologies.

Practical examples

- **Jordan case: e-banking survey**
In January 2016 ، the Journal of Engineering and Applied Sciences

- **Does user control options, would actually enhance privacy or security?**

- **Several emerging privacy concerns about connected vehicles.**

In reference that privacy is a social product, privacy is something that people create over time, based upon experiences, with the resources available

- Leaders of big enterprises are proactive to the impact
- They talk about Cyber-governance In technologies,
  - Emerging technologies are forcing many business leaders to reassess their decentralized approaches to cyber risk management (INTEROPERABILITY)
  - Cyber risk management and innovation must be also on equal footing
- Best practices (Standards project mngt, Change mnt and data governance)

91% of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders

53% include proactive management of cyber and privacy risks by design in the project plan and budget "fully from the start"

Source: Fall 2018 Digital Trust Inisghts, PwC
Base: 3,000 respondents

2- Corporate Security Risk Management

- In most large organizations, the approach to cyber risk may differ by region, product, or business unit.

- Ex: Microsoft case

3- Corporate Governance (Institute the data Governance)

- The world is changing We have to accept some other models
- Metadata
- Enforce the data governance model
- Institute the concept
  - Effective structure
  - Effective legislation

Recommendations

- **"PPP" Public Private Partnership is one solution;**

- **Multistakholder collaboration is required for managing effectively the change**

- **GDPR as best practices**

- **Institute the data governance**

- **Engage Academia, Engage private sector in this debate….**