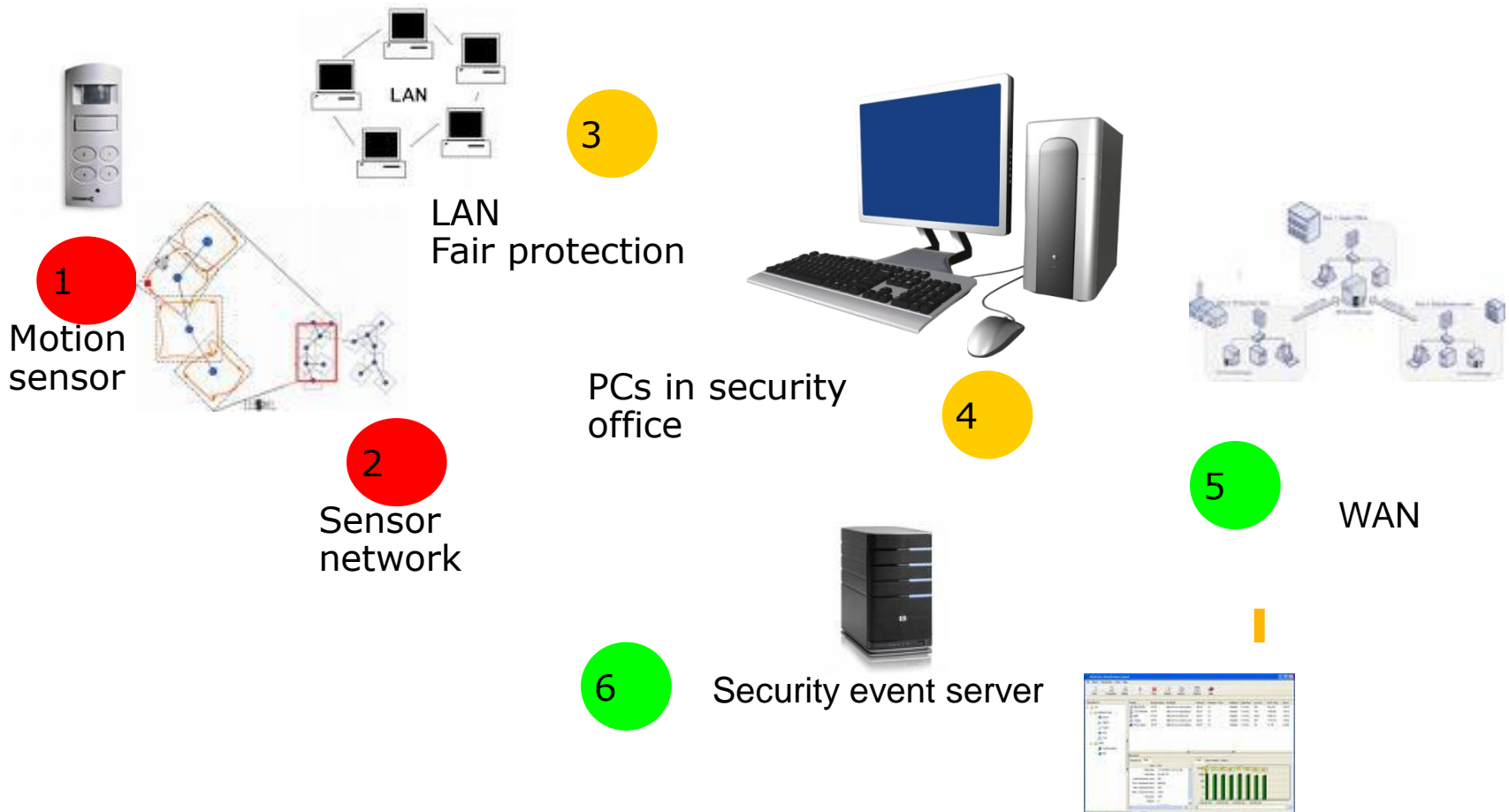# Solving the problem of trust "composition".

January 2011

Claire Vishik

Situations Requiring Trust: Examples

1. Access to mission critical systems

2. Social networking

3. Online banking and e-commerce

4. Using an ATM in a foreign country

5. Using medical services, accessing health records

6. Updating/synchronising your devices via your computer

7. Accessing premium content in a mobile setting

8. Setting up and updating PCs for enterprise employees

Variability of Levels of Protection

1 Motion sensor

2 Sensor network

3 LAN
Fair protection

PCs in security office

4

5 WAN

6 Security event server

Is the process secure if some components are secure?

Variability of Anonymity Options

2 Subscription settings

4 Comments on Web site
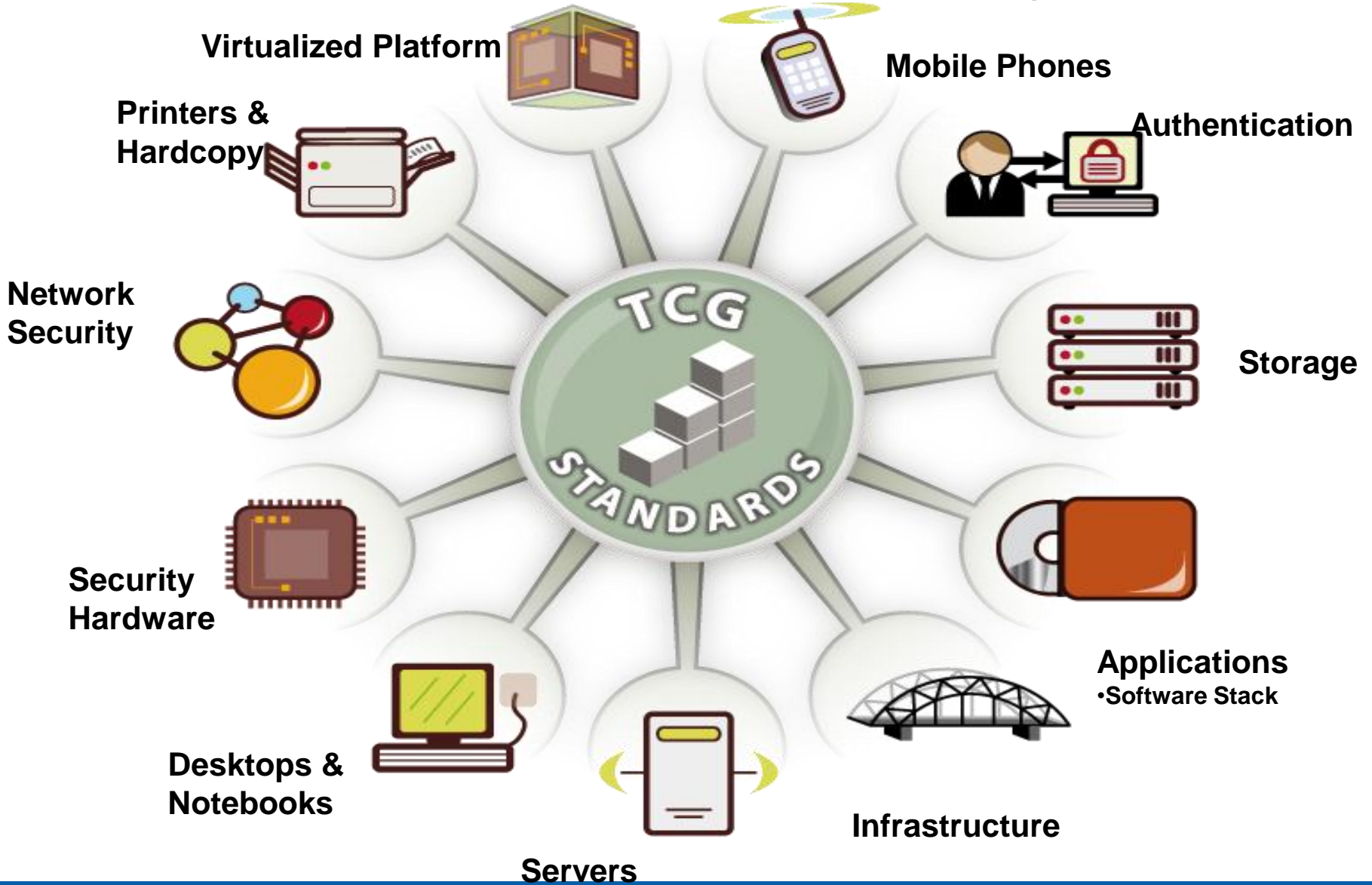
Payment for subscription

3

1

Web application on mobile phone

Activities: subscription, payment, and comments. When is a user anonymous?

Anonymity: matter of degree

TCG: Standards for Trusted Systems

Virtualized Platform

Mobile Phones

Authentication

Printers & Hardcopy

Network Security

Storage

Security Hardware

Applications
•Software Stack

Desktops & Notebooks

Infrastructure

Servers

Trust Definition and Enforcement: Some Approaches

1 Measurement (security, privacy)

2 Authentication

3 Reputation

4 Policy frameworks

5 IC Fingerprinting

6 Many other approaches

Gaps

Cross domain functionality

- Trust technologies are domain specific, but most processes reach across domains. Privacy domains? Cross-domain privacy?

Measurement techniques

- At the heart of today's TC approach
- Not designed to be top-to-bottom
- Not designed for privacy

Discovery and routing techniques

- How can we discover trustworthy devices, networks, and services? How can we be routed to them? How can we define privacy-friendly request routing?

Some Gaps (II)

Inventory of "trust features" is incomplete

- What about authenticity of a device or application or policy?
- What about data quality? Anonymity? Privacy?
- Evidence of a certain level of privacy?

Policy Frameworks

- User controlled trust policies? User perceptions of trust? User-driven definitions of trust? Privacy policy enforcement?

Dynamic trust

- Can we establish trust based on observation in a privacy-friendly way? Can we dynamically change trust parameters?

THANK YOU!