Human Factors in Developing Trustworthy IT Systems and Applications

Stephen S. Yau

Information Assurance Center, and

School of Computing, Informatics, and Decision Systems Eng.
Arizona State University

Tempe, Arizona USA

yau@asu.edu

Outline

- Trustworthy IT Systems and Applications (ITSA)
- Challenges of Developing ITSA
- Human Factors in Developing ITSA
- Current State of Art
- Future Research

Evolution of IT Systems

- Mainframe (1950s)
- Personal Computer (early 1970s)
- Object-Oriented Computing (1980s)
-
- Grid Computing (1990s)
- Services Computing (2001)
- Cloud Computing (2005)
- Internet of Things (2009)

Internet

Virtualization

Wireless

Smart Device

Current Trends of ITSA

- Based on ***service-oriented and cloud computing, and IoT paradigms with smart devices, large computing power, internet and big data***
- ***Standard interfaces*** for accessing capabilities offered by various providers
- Applications can be ***quickly composed*** of ***services*** to form ***workflows (business processes)*** for applications on IT systems.

Current Trends of ITSA (cont.)

- Consisting of **various heterogeneous components and smart devices**
- Relying ***public and private networks***
- Depending more on ***outsourcing services***
- ***More information and resource sharing***
- ***Adaptation*** to dynamic application requirements of users or environments (functional and QoS)
- ***Interoperation of heterogeneous services, components, and devices***

Trustworthy ITSA

- ***Trustworthy ITSA (TITSA)*** are needed due to
  - Over public or private networks, as well as mobile networks – more open to ***attacks***
  - Interactions involving ***unknown entities***
  - ***Dynamic*** and ***pervasive environments***
  - Large-scale and cross-domain ***service collaborations***
  - ***Distributed intelligence*** and ***control***
  - ***Dynamic QoS expectations*** for multiple workflows

Trustworthy ITSA ***(cont.)***

- Major aspects
  - ***Human***
    - Users and collaborators
    - Service and infrastructure providers
    - Insiders and outsiders
  - ***Devices, software, hardware, networks,*** and ***systems***
  - ***Dynamic user requirements and environments***
  - ***Dynamic security policies*** and ***enforcement***
  - ***Effective techniques***
  - ***Cost, usability*** and ***efficiency***

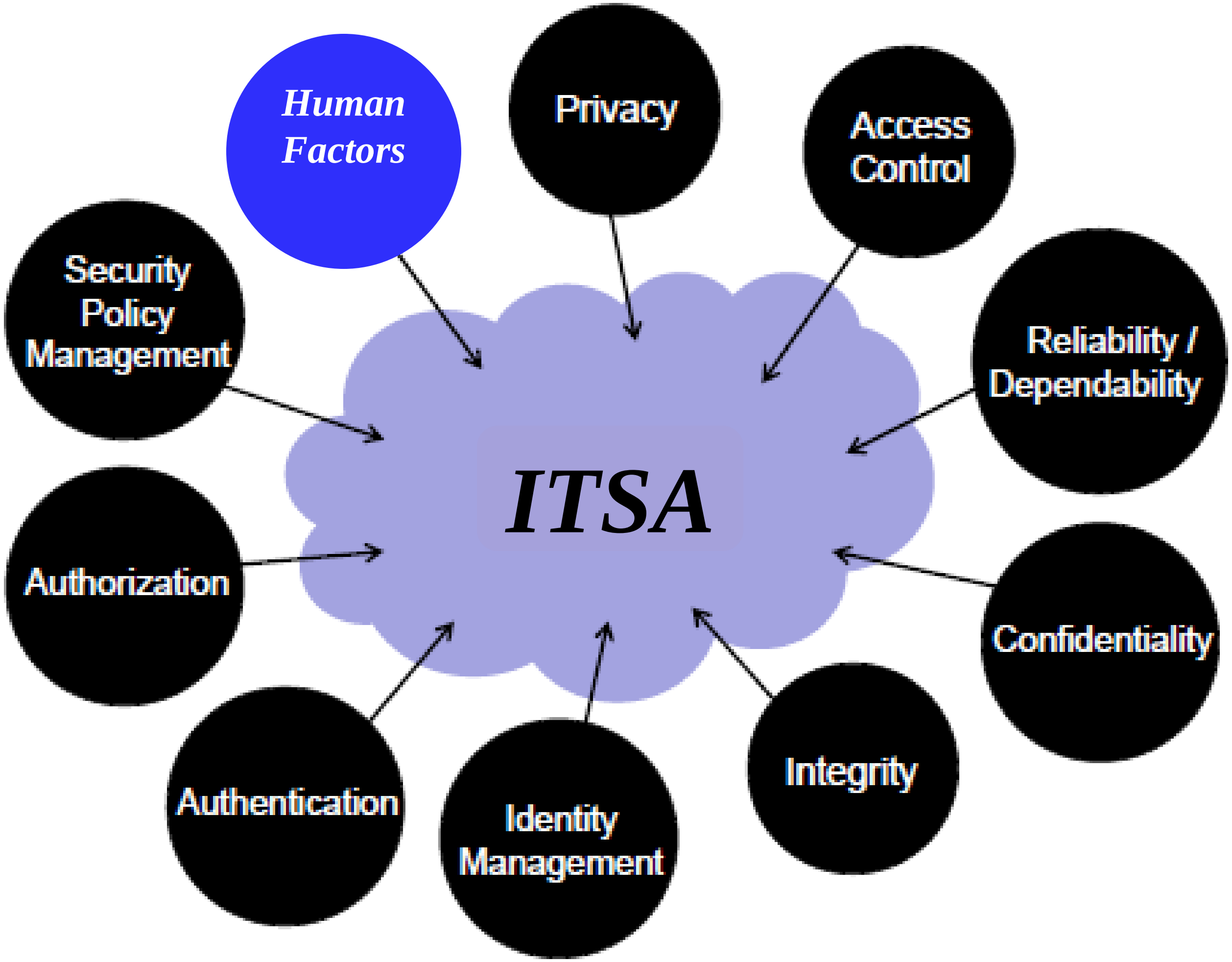
Trustworthy ITSA (cont.)

- Various system technologies needed for developing IITSA
  - Security
  - Trust management
  - Situation awareness
  - Runtime adaptation
    - QoS monitoring and analysis
    - QoS requirement trade-off
    - Resource allocation

Concerns of ITSA Users

- Most ITSA users are concerned with ***leakage of their sensitive data*** because their data is processed and stored on machines owned and operated by various service providers, not controlled by users.
- Due to severe limitation of resources available in mobile devices and characteristics of mobile networking, ***security*** issues is more severe for ITSA involving mobile devices and networking.

Challenges: Security for ITSA



Challenges of Developing TITSA

- ***Interactions among services*** in TITSA may have ***unforeseen consequence***s in trust, security, QoS, and risk
  - Untrusted/malicious services
  - Intermediate results generated during service interactions may reveal sensitive information
  - Trustworthiness of service providers, infrastructure providers and users

Challenges of Developing TITSA **(cont.)**

- ***Multiple QoS requirements*** from multiple users for various applications
- ***Runtime tradeoffs*** among expected QoS requirements
  - Example: Mechanisms providing ***security protection*** are often ***computationally intensive*** and require certain sacrifice in other QoS (e.g. service delay and throughput) with available resources
- ***Cost, usability*** and ***efficiency***

Challenges of Developing TITSA **(cont.)**

- ***Dynamically changing environment***
  - Make ***assessing trust and risk*** difficult
  - Need ***situation awareness*** due to dynamic trust and risk
  - Need ***adaptive enforcement*** of security policies
- ***Information needed*** for making decisions regarding trustworthiness usually ***distributed on multiple services and organizations.*** Need the following:
  - ***Cooperative decision making*** (e.g. delegation, policy composition with multiple organizations, collaborative QoS management, risk assessment, trust evaluation)
  - ***Pcient enforcement*** of ***distributed security policies***
  - ***Protection*** against various entities

Challenges of Developing TITSA ***(cont.)***

- ***Service selection*** and ***composition***
  - How to select ***more appropriate services*** and compose them to satisfy both functional and QoS requirements of various users, while ensure ***overall system trustworthiness*** and ***security***?
  - Need ***meaningful*** and ***quantitative metrics*** for ***trustworthiness, security*** and various attributes of overall TITSA
  - How to make ***service ranking*** to identify "better" services satisfying their requirements

Human Factors in TITSA

- In general, a ***human factor*** is a ***physical, psychological or cognitive property of an*** **individual or an individual in a community**, specific to humans and influencing technological systems as well as their applications.
- **Examples**: Influences, interests, relationships (collaboration/competition), opinions (positive/negative/neutral, support/against), knowledge (expertise), reputation, wisdom, physical and psychological factors (stress, fatigue, fear, happy).

Human Factors in TITSA (cont.)

- IT systems become more powerful, and their ***applications*** become more ***diverse*** and ***pervasive***
- ***Human factors*** are increasingly influential on the quality and efficiency of generating the results because
  - ITSA getting more ***embedded,*** increasingly involving ***multi-party collaborations*** and often more ***pervasive***
  - Applications must address multiple quality aspects expected by users, such as security, privacy, trustworthiness and performance

Three Levels of Human Factors

- Level 1. Direct Human-and-Human Relations
  - Collaboration of among ITSA users
- Level 2. Indirect Human-and-Human Relations
  - First-time collaborations among the users based on past data
- Level 3. Human in Communities
  - Influence among ITSA users
  - Knowledge sharing among the users
  - Matching ITSA users’ interest with applications

Direct Human-and-Human Relations

- Challenges:
  - How to quantify human factors in terms of the determinants, such as ***workload on the human, fatigue, learnability, attention, vigilance, human relations, human performance, human reliability, stress, individual differences, aging, safety, and results of decision making.***
  - How human factors affect humans themselves?

Indirect Human and Human Relations

- Example:
  - In ITSA, the providers upload their services/applications. The users search the service/application directory for the CBS and select the services/applications they need. Besides the quality of the services/applications, each user is concerned with the ***trustworthiness*** of the services.
  - Challenge: How can a user choose a ***trustworthy service***?
  - Related human factors: human relationships, stress, feedback, etc

Human in Communities

- Challenges:
  - How do the human factors from ***one person affect other persons in the community***?
  - How do the human factors ***from other persons in a community affect one person in the community***?
  - How do the human factors from ***one person in a community spread*** in the ***ITSA used by the community?***
  - …

Current State of Art

- **Incorporating human factors in developing TITSA**
  - Research has been mainly conducted by researchers in psychology and sociology, and few computer scientists and engineers.
  - Primarily focus on human-machine interactions, human-computer interactions, situation awareness, and human errors

Current State of Art (cont.)

- Automated service composition based on various formal specifications
- QoS-aware service composition in ITSA
- Tradeoffs among security and multiple QoS in ITSA
- Adaptive resource allocation in ITSA
- Design of ITSA for QoS Monitoring and adaptation
- Testing of ITSA

Current State of Art (cont.)

- **Trust estimation in SBS**
  - Flexible trust model for distributed service infrastructure (Z. Liu, University of North Carolina at Charlotte, S. Yau, Arizona State University)
  - Trusted computing platforms in web services (Nagarajan, et al, Macquarie University, Australia)
  - Trust management for context-aware service platforms (Neisse, et al, University of Twente, the Netherlands)
  - Improving trust estimation in CBS (S. Yau and P. Sun, Arizona State University)

Trust Estimation in TITSA

- **Trust management** needs to be incorporated in TITSAs to estimate service providers' trustworthiness so that users can decide whether to accept the services provided by the providers.
- Limitations of existing trust estimation approaches:
  - Only similarity of user profiles is considered
  - Based on pairwise trust relationship, which normally does not include the transitive property in the propagation of trust among service providers.

Trust Estimation in TITSA (cont.)

- Initialization
  - Initialize the trust values of all service providers of the CBS based on historic transactions using QoS profiles, collaboration and competition.
- Utilization
  - Update the trust values of the service providers in current transaction using QoS profile.
  - Update the trust values of all the other service providers using competition and collaboration.

25

Effect of QoS Profile on Trust Estimation

- If the feedback QoS profiles of a selected service is **better** than its corresponding claimed QoS profiles, then the service user can decide the service provider is **more trustworthy**, and consequently **increase** the estimated trust value of the service provider.
- Otherwise, **decrease** the estimated trust value of the service provider.

Improvement of Trust Estimation Using QoS Profiles (cont.)

- **Rule 1**. ***Competition relationship*** increases the trust values of the participants in the competition group.
  - Competition limits free-ride
  - The more time one spends, the more one is likely to trust the people in this group.
- **Rule 2**. ***Successive collaboration relationship*** increases trust.
  - When two persons collaborate well with each other, they tend to solve problems together and help to build trust between them.
- **Rule 3**. ***Transitive property of trust***.
  - Whenever one service provider’s trust value changes, the trust values of his/her neighbors will also change accordingly.
  - The trust value of a service provider is uniformly propagated to all the other service providers he intends to compete or collaborate with.

Improvement of Trust Estimation Using QoS Profiles (cont.)

- Rules 1 and 2 show the positive correlation between trust and competition or collaboration.
- Rule 3 defines how the trust values should be propagated among the whole network of CBS.
  - The propagation of the trust values of service providers is similar to PageRank (a webpage reputation estimation approach).
  - The more people who intend to compete or collaborate with a service provider, the more trustful the service provider is.

Expertise Needed to Incorporate Human Factors in Developing TCBS

- Services and cloud computing
- Software and systems engineering
- Networking, including mobile ad hoc networks, intelligent devices, and social networks
- Information assurance and security
- Cognitive science
- Psychology
- Business
- Culture
- …

Future Research: Human Factors in Developing TICBS

- Develop meaningful ***metrics*** to quantify human factors and QoS aspects of CBS, including trust, security and others useful for developing TITSA
- Develop a general ***framework with necessary techniques and tools*** to effectively incorporate a variety of relevant human factors in developing TITSA
- Validation

Future Research: Human Factors in Developing TITSA

- ***Trust Management***
  - Existing definitions of trust are based on the assumption that the user to be evaluated is the one to be evaluated ***based on the user's account,*** i.e., the relationship between the user and the user's account, referred as the ***identity trust*** of the user, is ignored, but should be considered.
  - Identity trust for mobile smart devices users is extremely difficult. Possible research issues:
    - What characteristics does identity trust have?
    - What is the relationship between identity trust and commonly understood trust?
    - What need to be done to incorporate identity trust management in mobile clouds?

Thank you