



Resilience Challenges in Service-Oriented Architectures

Research Requirements for Security and Dependability for Services

Workshop on

Software and Service Development, Security & Dependability

Paulo Esteves Veríssimo, *Univ. of Lisboa, Portugal*

pjv@di.fc.ul.pt, <http://www.di.fc.ul.pt/~pjv>

10-11 July 2007, Maribor



Funded by EC contract FP6-027599

Society and Policy Considerations in ICT Security

ESFORS Software and Service Development, Security & Dependability Workshop

- Continued **adoption and trust in ICT-based services** will depend largely on the **user-friendliness of such services**
- However, common people find themselves having to deal with the **well-known plagues** of viruses, spam, rootkits and phishing attacks
- Existing technologies, in order to protect from such attacks, will introduce **costly barriers to the usability** of ICT-based services, driving society away from their use
- Security technologies that deal directly with people and society must remain user-friendly while being secure
- but.....
- **SOA world casts some doubts on this objective**

Risks of the move toward Services (I)

ESFORS Software and Service Development, Security & Dependability Workshop

- service-centric view is changing the way IT infrastructure and applications will be managed and delivered
 - services will be shared between many consumers, and offered by a multitude of providers
 - components will obey different and independent security policies, increasing the risks
 - components may be owned and operated by different and possibly many organisations
 - many different participants dealing directly with one another

Risks of the move toward Services (II)

ESFORS Software and Service Development, Security & Dependability Workshop

- in such a scenario
 - confidentiality, integrity, availability, and QoS requirements will increase
 - or at least become more visible in service-level agreem. (SLAs)
- but with the traditional approach:
 - SW and services continue to be offered on “best effort” basis
 - we will end up buried under an unmanageable number of SLAs
- **fulfilling SLAS**, i.e. rendering correct and acceptable services **will become very difficult**

Risks of the move toward Services (III)

ESFORS Software and Service Development, Security & Dependability Workshop

- the most basic reliability theory tells us that:
 - failures will be more frequent if we pursue the current “best effort” approach
- SLAs will fail:
 - the capacity and responsibility (or lack thereof) of service providers will be brought under the spot lights
 - unsolvable conflicts will be the rule rather than the exception
- in such a deregulated and pulverised (SOA) world of components, **the fragile *trust* building of online operations risks falling apart**
- problem is how organisations can assure themselves and regulators that **they have appropriate control over their IT**

SLAs in the scene (I)

ESFORS Software and Service Development, Security & Dependability Workshop

- Why do we talk about SLA ?
- Because **SLA will be a crucial component of SOA**
- SOA decoupling and decentralisation will demand that components respond for their trustworthiness and/or QoS

SLAs in the scene (II)

ESFORS Software and Service Development, Security & Dependability Workshop

- an SLA is a contract, it implies trust between the parts:
 - service user trusting service provider
 - provider should have the means to fulfil it (trustworthiness)
 - user should believe the former has those means (trust)
- even with the stable, centralised and visible notion of provider there is some uncertainty
 - in what contributes to fulfilling the end SLA
 - in whom to blame when things go wrong
- usual situation:
 - user is imposed a more superficial predicate, that ‘the provider will fulfil the SLA’, regardless of the means
 - details about these means are frequently considered proprietary
 - not available to the user even if it wanted to assess them

Imagine a scenario (I)

ESFORS Software and Service Development, Security & Dependability Workshop

- application service provider (ASP) signs SLA with several clients
 - ASP must guarantee QoS as seen by Internet users
 - ASP must guarantee security and/or dependability both of user access and of the information stored/manipulated in the servers
- clients may be end clients or in turn be service providers
- in this case they may themselves sign specific SLAs with their end users
 - ASP should guarantee that its data centre fulfils what is agreed
 - ASP contracts an SLA with the Internet service provider (ISP)
 - ISP in turn contracts with raw cable or wireless providers (CSP)

Imagine a scenario (II)

ESFORS Software and Service Development, Security & Dependability Workshop

- it is difficult to formally and technically provide guarantees about the capacity of the infrastructure and supported services to meet SLAs
- user trust is more of a question of faith, largely based on political/social terms, such as **reputation** (standing in market), **insurance** (endorsing responsibility) or **inevitability** (monopoly, public administr) of provider
 - provider says “Trust us, you know us!” or “Trust us, you have no other option!”
- ASP contract with end user depends on properties of infrastructural services transparent to the former (isolation, protection/detection)
 - ASP is the visible tip of the iceberg

Imagine a scenario (III)

ESFORS Software and Service Development, Security & Dependability Workshop

- current business practice ends up relying more on muscle (the aforementioned **unilateral trust constructions**) and legal advisors than on technical arguments and mechanisms
- one might argue that this situation is **unsatisfactory to the users but rewarding to the providers**. IS IT?
- in fact, this is not true
- we have just seen that providers are normally users to other providers, and thus the problem has repercussions throughout value chain

Trusting SLAs in an SOA context

ESFORS Software and Service Development, Security & Dependability Workshop

- unfortunately, the situation will become unsatisfactory, if not unsustainable, to all stakeholders, in an SOA context, if nothing is done to improve the situation
- in a service-oriented architecture (SOA) world, this can only get worse, and as such, **requires methodical research on the methods, architectures and mechanisms to deal with the problem**

Trusting SLAs in an SOA context

ESFORS Software and Service Development, Security & Dependability Workshop

- This brings us back to the crucial problem:
 - users are *imposed* trust on the services they buy,
 - whereas they should be given *evidence* that allows *building trust*
- evidence is akin to *trustworthiness* of the *services* and obviously, of the *infrastructure* supporting them
 - service providers must provide evidence they can fulfil the SLAs
 - capacity should be auditable by regulators and other authorities
 - user should be given means to build trust
 - (either by directly assessing the capacity of the providers it contracts, and/or by a transitive relation with regulating bodies it trusts, and which (the latter) can assess the providers' capacities.)

Research Challenges (I)

ESFORS Software and Service Development, Security & Dependability Workshop

- In an SOA context, all these are research challenges, and the problem has several facets:
- how users and other stakeholders should obtain static guarantees about the capacity of providers
 - current assurance standards being felt insufficient for SOA;
- how organisations should assure themselves and regulators that they have appropriate control over their IT to keep it dynamically within correct parameters
 - current management practices being felt insufficient for SOA;
- how systems should enforce and assess the individual trustworthiness of components at run-time, and include them in trusted computations
 - get desired degree of resilience against faults, attacks and intrusions

Research Challenges (II)

ESFORS Software and Service Development, Security & Dependability Workshop

- we need a much closer link between
 - *trust* on the applications as seen by users,
 - and *trustworthiness* of the infrastructure and supporting components
- In essence, this all boils down to
 - study of the *technical* (system mechanisms) and *legal* (standards and regulations) means of guaranteeing an accurate relation “trust a service running on S to the extent of S’s trustworthiness”.
- This is believed to be a key factor of success of business in an SOA world

Research Challenges (III)

ESFORS Software and Service Development, Security & Dependability Workshop

- Foundation for a trusted infrastructure:
 - components that have security built-in from the start and not bolted on as an afterthought
 - trustworthiness (dep&sec) is required of the infrastructure entities on which to place trust
 - however, too many designs rely on assumptions that are not substantiated, potentially putting systems at risk
- Meeting these assumptions is a complex task:
 - as computer systems become more modular, open, and geographically dispersed;
 - needs proper design and architecting principles;
 - becomes overwhelmingly involved when simultaneous resilience against accidental and malicious threats is sought

Conclusion

ESFORS Software and Service Development, Security & Dependability Workshop

- ICT-based society needs to provide trustable services
 - i.e. services that are **trusted** because justifiably they rely on **trustworthy** components and **trusted** infrastructure
- Untrusted services may nevertheless be deployed due to market pressure and:
 - be perceived with suspicion by large mass of users;
 - information will be managed by a restricted group of "experts", increasing info-exclusion;
 - may be mismanaged, prompting for cyber-crime, e-frauds, cyber terrorism and sabotage