



云计算技术与工程

云计算安全

徐敏贤

副研究员

云计算研究中心

中国科学院深圳先进技术研究院

<http://www.minxianxu.info/vcc>

青海长云暗雪山，孤城遥望玉门关。黄沙百战穿金甲，不破楼兰终不还。
——（唐）王昌龄

Security Memes



ACK: The contents of this lecture are derived from Prof. Richard Sinnott @ Unimelb

Orwellian Nightmare...



<https://www.dsparkanalytics.com.au/>

<http://www.pedestrian.melbourne.vic.gov.au/>

Twitter tracking...

Digital Security (in the e-World)

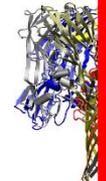


Resources

Access Control

Privileges

User Communities



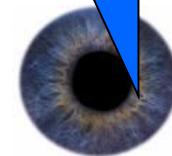
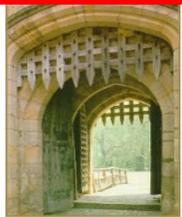
Site autonomy
Manageability

Scalable
Fine grained
Dynamic

Ease of use
Single sign-on



AGGTATAGCGCGCGGATATATA
AAATGTACGTACGGGCUCTTATA
CGGGCGGATATATAGCGGCGG



Why is security so important?



- If systems (**Grids/Clouds/outourced infrastructure!**) are not secure
 - Large communities will not engage
 - medical community, industry, financial community ...
 - or rather they will only use their own internal resources
 - private clouds!
 - Expensive (impossible?) to repeat some experiments
 - Huge machines running large simulations for several years
 - Legal and ethical issues possible to be violated with all sorts of consequences
 - e.g. data protection act violations and fines incurred
 - Amazon Web Services, Sydney
 - Trust (more later!) is easily lost and hard to re-establish



ENTERPRISE.IT, FEATURED, NEWS - Written by Renal LeMay on Tuesday, November 13, 2012 10:25 - 19 Comments

Finally, Amazon launches Sydney datacentre

Tags: amazon web services, cloud computing, cloud storage, datacentre, ec2, elastic compute cloud, halfbrick, s3, sydney

Protecting Data from Unauthorised Access by Rogue Vendor Employees

- b. **Vetting of vendor's employees.** What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy? Examples include thorough police background checks, as well as citizenship checks, security clearances and psychological assessments especially for employees with administrative privileges or other access to customer data. For example, in September 2010 a major vendor acknowledged sacking an employee for allegedly deliberately violating the privacy of users by inappropriately reading their electronic communications during a timeframe of several months.

http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

The Challenge of Security



■ Grids and Clouds (IaaS) allow users to compile codes that do stuff on physical/virtual machines

- In the Grid world a rich blend of facilities co-existed (were accessible/integrated!) which had “issues”
 - Highly secure supercomputing facilities compromised by single user PCs/laptops
 - Glasgow experience!
 - Need security technologies that scales to meet wide variety of applications
 - from highly secure medical information data sets through to particle physics/public genome data sets
- Using services for processing of patient data through to “needle in haystack” searching of physics experiments



■ Should try to develop generic security solutions

- Avoid all application areas re-inventing their own (incompatible/inoperable) solutions



The Challenge of Security ...ctd



- Clouds allow scenarios that stretch inter-organisational security
 - Policies that restrict access to and usage of resources based on pre-identified users, resources
 - Groups/tenancy...
 - But what if new resources added, new users added, old users go...?
 - Over-subscription issues
 - User management (per user, per team, per organisation, per country...)
 - What if organisations decide to change policies governing access to and usage of resources, or bring their data back inside of their firewall?
 - Really not replicated somewhere else?



Clear history: Google told to wipe your past off the net in landmark court ruling

- What if you share a tenancy with a noisy neighbour!
 - I/O demanding applications
 - You hopefully never experienced this, but early NeCTAR RC/NSP had performance issues!
- The multi-faceted challenges of "life beyond the organisational firewall"?



Prelude to Security



■ What do we mean by security anyway?

■ Secure from whom?

- From sys-admin?
- From rogue employee?
- ...



■ Secure against what?

- Security is never black and white but is a grey landscape where the context determines the accuracy of how secure a system is
 - e.g. secure as given by a set of security requirements



■ Secure for how long?

- *"I recommend overwriting a deleted file seven times: the first time with all ones, the second time with all zeros, and five times with a cryptographically secure pseudo-random sequence. Recent developments at the National Institute of Standards and Technology with electron-tunnelling microscopes suggest even that might not be enough. Honestly, if your data is sufficiently valuable, assume that it is impossible to erase data completely off magnetic media. Burn or shred the media it's cheaper to buy media new than to lose your secrets...."*
 - *-Applied Cryptography*



Prelude to Security ...ctd



- Note that security technology \neq secure system
 - Ultra secure system using 2048+ bit encryption technology, packet filtering firewalls, ...
 - ... on laptop in unlocked room
 - ... on PC with password on “post-it” on screen/desk
 - ... the challenge of peta/exa-scale computers and possibility for brute force cracking
 - ...
 - Famous quote to muse over:
 - “...if you think that technology can solve your security problems then you don't know enough about the technology, and worse you don't know what your problems are...”

*Bruce Schneier,
Secrets and Lies in a Digital Networked World*



Technical Challenges of Security



■ Several key terms that associated with security

- Authentication
- Authorisation
- Audit/accounting
- Confidentiality
- Privacy
- Fabric management
- Trust

Generally speaking

AAAA

Domain specific

(name -> DOB -> DNA)

Inter-organisational and
Technological challenges

All are important but some applications/domains
have more emphasis on concepts than others

Key is to make all of this simple/transparent to users!

- Authentication is the **establishment** and propagation of a user's identity in the system
 - e.g. so site X can check that user Y is attempting to gain access to its resources
 - Note does not check what user is allowed to do, only that we know (and can check!) who they are
 - Masquerading always a danger (and realistic possibility)
 - Security guidance/balances
 - Password selection
 - **16 characters, upper/lower case and must include non-alphanumeric characters and be changed quarterly...!?!?!?**
 - Treatment of certificates
 - Local username/password?
 - 100,000+ users that come and go
 - **Centralised vs decentralised systems?**
 - **More scalable solution needed**
 - Public Key Infrastructures (PKI) underpins MANY systems
 - Based on public key cryptography

This might seem like an aside on Cloud Security but IS important and relevant...honestly!!!

Public Key Cryptography



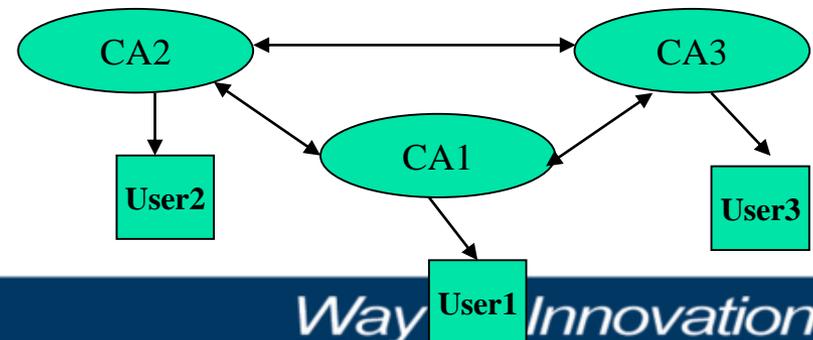
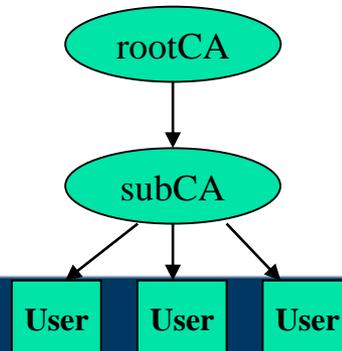
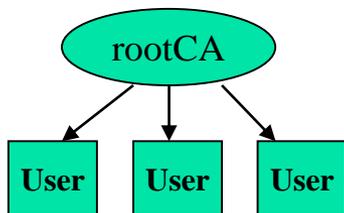
- Also called Asymmetric Cryptography
 - Two distinct keys
 - One that must be kept private
 - Private Key ... Duh! ;o)
 - One that can be made public
 - Public Key ... Double duh!
 - Two keys complementary, but essential that cannot find out value of private key from public key
 - With private keys can digitally sign messages, documents, ... and validate them with associated public keys
 - Check whether changed, useful for non-repudiation, ...
- Public Key Cryptography simplifies key management
 - Don't need to have many keys for long time
 - The longer keys are left in storage, more likelihood of their being compromised
 - Instead use Public Keys for short time and then discard
 - Public Keys can be freely distributed
 - Only Private Key needs to be kept long term and kept securely

- Mechanism connecting public key to user with corresponding private key is Public Key Certificate
 - Public key certificate contains public key and identifies the user with the corresponding private key
 - Distinguished Name (DN): CN=Richard Sinnott; OU=Dept CIS; O=UniMelb; C=AU
 - Not a new idea
 - Business card
 - My name, my association, contact details, ...
 - Can be distributed to people I want to exchange info with
 - If include public key on it, then have basic certificate, but ...
 - has to be delivered in person (or no trust!), who says I work at SIAT?, could be a forgery, I might be an impostor, what if I move to SUSTech or my phone number changes, who would have 1024-bit key on business card, ...
 - Public Key Certificates issued by trusted “Certification Authority”

Certification Authority

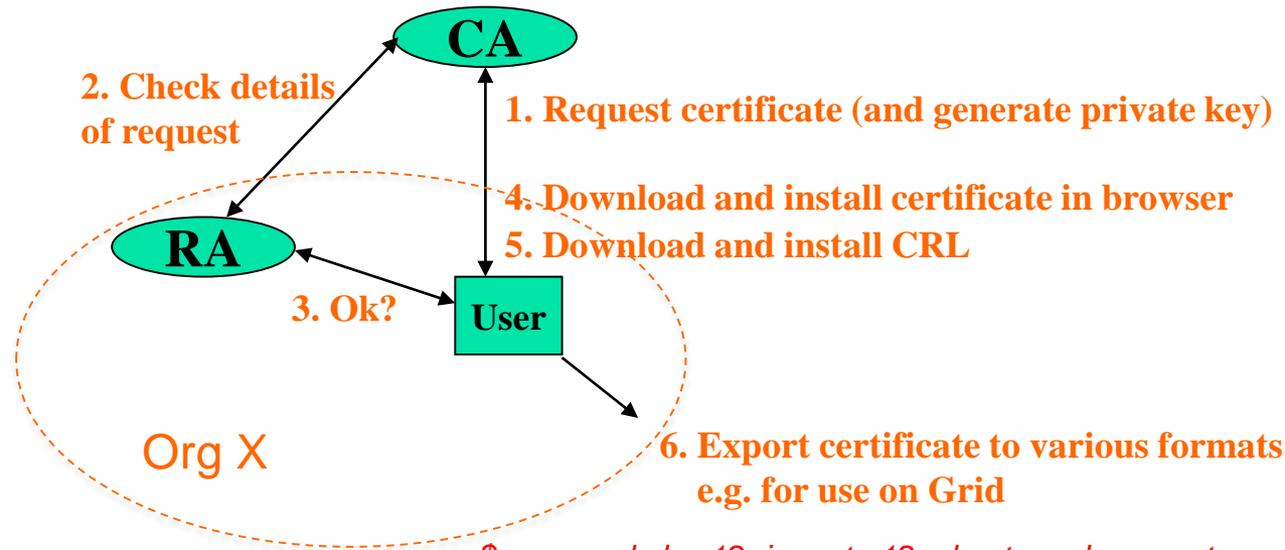


- Central component of PKI is *Certification Authority* (CA)
 - CA has numerous responsibilities
 - Policy and procedures
 - How to's, do's and don'ts of using certificates
 - Processes that should be followed by users, organisations, service providers ...(and consequence for violating them!)
 - Issuing certificates
 - Often need to delegate to local *Registration Authority*
 - Prove who you are, e.g. with passport, student card
 - Revoking certificates
 - Certificate Revocation List (CRL) for expired/compromised certificates
 - Storing, archiving
 - Keeping track of existing certificates, various other information, ...



Typical Simple CA

- Based on statically defined centralised CA with direct single hierarchy to users
- Typical scenario for getting a certificate



\$> openssl pkcs12 -in cert.p12 -clcerts -nokeys -out usercert.pem!!!!

This was/ is off-putting for end users!!!

Typically not available on Windows!!!

Root access? Local sys-admin?

Who is the RA at University/College of

"SomewhereSmall" that isn't in the e-Club?

UK e-Science Grid (~2004)



- Grid mapfile
 - DN=Rich... -> ros
 - DN=Bob... -> bob
 - ...



- EGEE Grid
 - Similar principal
 - (but role of VO)

- So what has this got to do with Cloud...?
 - IaaS – key pair!
- Cloud inter-operability begins with security!
 - There is no single, ubiquitous CA, there are many
- Your access to:
 - CSTCloud was achieved through proving your identity as a member of the SIAT
- There are many ways to prove your identity
 - UCAS Id, SIAT Id, bank credit card for Taobao, ...
 - Degrees of trust
 - But remember need for single sign-on

Prove identity once and access distributed, autonomous resources!

But...

- Does SIAT have a single way to prove identity for all their staff/students? Fired but still with VPN access?
- Does UCAS have a strong password policy? Admin/admin?
- Do we really know that it is XXX logging in from SIAT and not his student/secretary/the cleaner?
- Do I want anyone from SIAT to be able to log-in to my service (if they aren't involved in my project!?)
- Is it really MY bank card I am using on Taobao to do bad stuff?
- Relation with Cloud for IaaS vs Usage of a Cloud
 - What we really want is finer-grained security
 - Clouds don't tackle this right now
 - Typically domain/user specific (and generally a dark art!!!)

- *Authorisation* is concerned with controlling access to resources based on policy
 - Can this user invoke this service, make use of this data?
 - Complementary to authentication
 - Know it is this user, now can we restrict/enforce what they can/cannot do
 - Many different approaches for authorisation
 - Group Based Access Control (e.g. your project VMs)
 - Role Based Access Control (RBAC)
 - Identity Based Access Control (IBAC)
 - Attribute Based Access Control (ABAC)
 - ...
 - Consider the Passport vs Frequent Customer Shopping experience



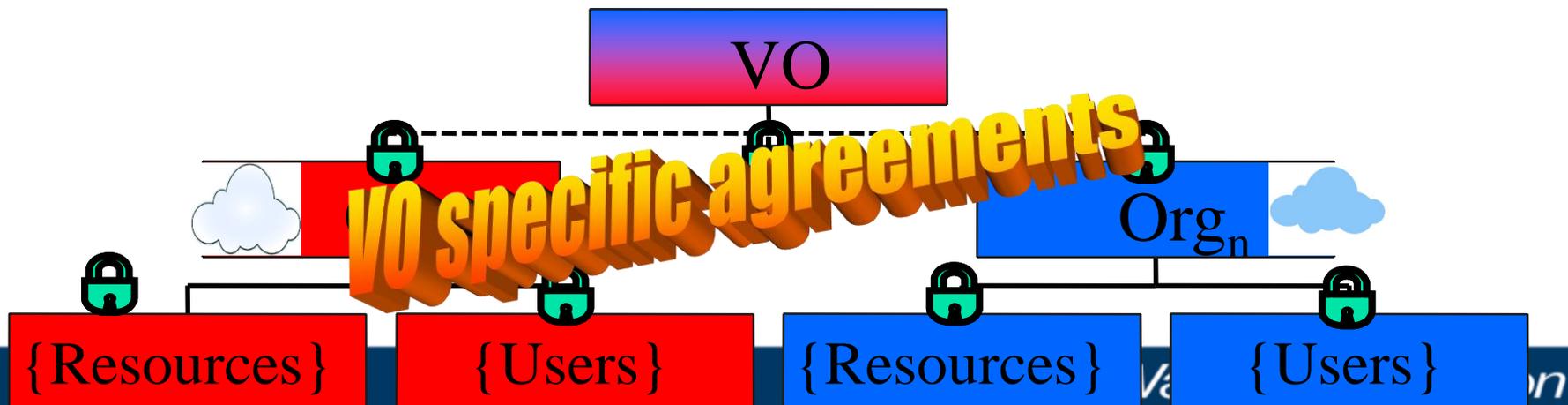
Authorisation and Clouds ?



- **Authorisation** typically applies to services/data deployed on Clouds, i.e. when they are running
 - But not only...
 - Who can install this patch, when can they do it, how many VMs will be affected if this happens...?
 - Is this virtual image free of trojans, malware etc?
 - Lots of tools to support this
 - Pakiti, Cfengine, Puppet, ...
 - Real challenge of software dependency management for complex systems
 - Amazingly (?) most users/organisations do not patch!!!
 - Side-effects, complexities, stopping jobs, restarting jobs etc

■ Authorisation

- Defining what they can do and define and enforce rules
 - Each site will have different rules/regulations
- Often realised through Virtual Organisations (VO)
 - Collection of distributed resources shared by collection of users from one or more organizations typically to work on common research goal
 - Provides conceptual framework for rules and regulations for resources to be offered/shared between VO institutions/members
 - Different domains place greater/lesser emphasis on expression and enforcement of rules and regulations (policies)



■ Many Technologies

- XACML, PERMIS, CAS, VOMS, AKENTI, VOMS, SAML, WS-*

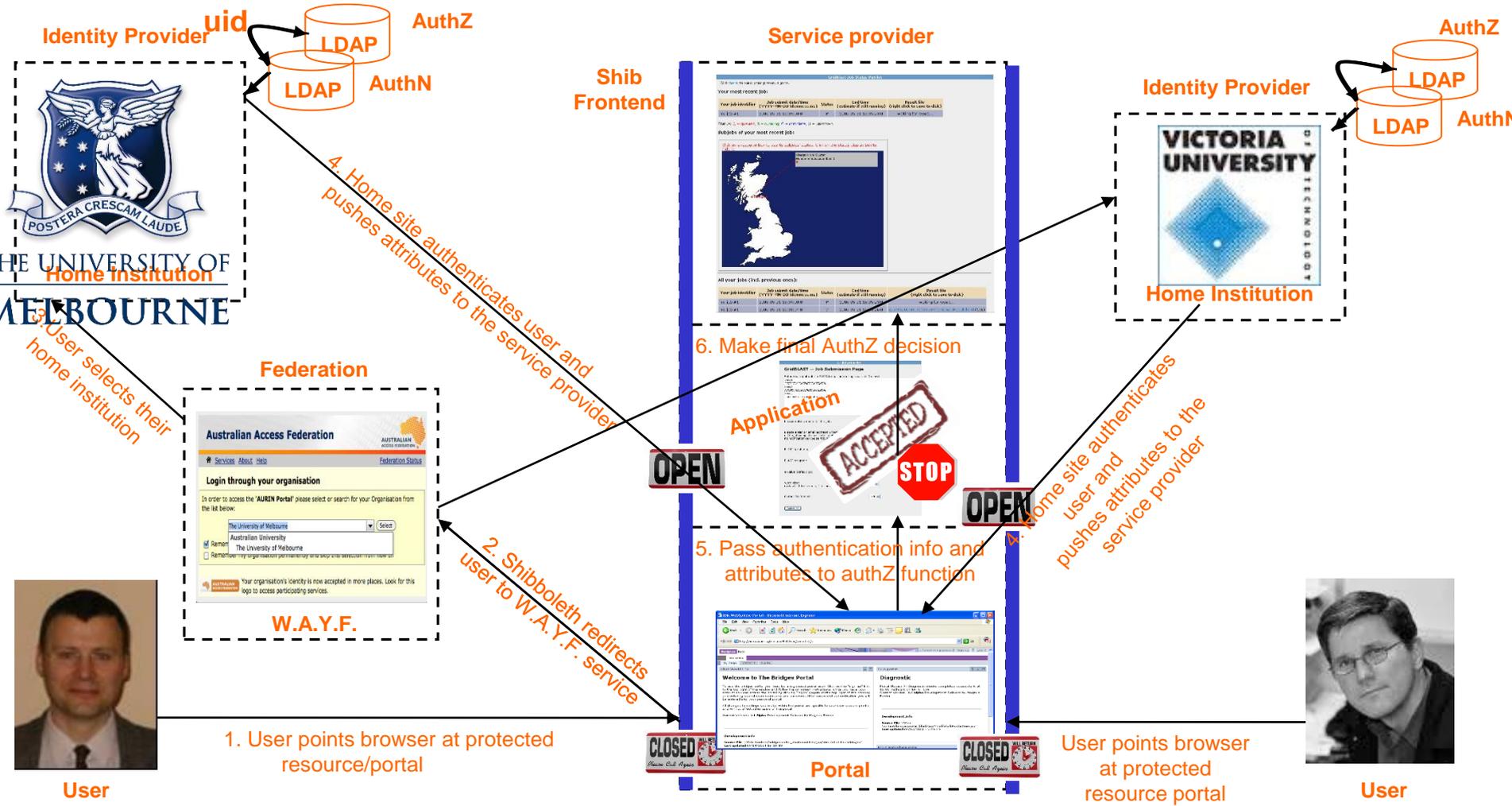
■ RBAC is typical model

- Basic idea is to define:
 - roles applicable to specific collaboration
 - roles often hierarchical
 - Role $X \geq$ Role $Y \geq$ Role Z
 - X can do everything and more than Y who can do everything and more than Z
 - actions allowed/not allowed for VO members
 - resources comprising VO infrastructure (computers, data etc)
- A policy then consists of sets of these rules
 - $\{ Role \ x \ Action \ x \ Target \}$
 - Can user with VO role X invoke service Y on resource Z?
 - Policy itself can be represented in many ways,
 - e.g. XML document, SAML, XACML, ...
 - Standards on when/where these used (PEP) and enforced (PDP)
- Policy engines consume this information to make access decisions

Should all be transparent to end users!

Reflect needs and understanding of organisations involved!

Shibboleth Augmented Authorisation



Other Cloud Security Challenges



- *Single sign-on*
 - The Grid model (and Shib model!) needed
 - Currently not solved for Cloud-based IaaS
 - Onus is on non-Cloud developers to define/support this

Other Cloud Security Challenges



■ *Auditing*

- logging, intrusion detection, auditing of security in external computer facilities
 - well established in theory and practice and for local systems
 - Less mature in Cloud environments (beyond the firewall!)
 - Tools to support generation of diagnostic trails
 - Across federations of Clouds?
 - Log/keep all information?
 - For how long?
 - ...

Other Cloud Security Challenges



- *Deletion (and encryption!!!)*
 - Data deletion with no direct hard disk
 - Many tools and utilities don't work!
 - Scale of data
 - Securely deleting a few Mb easy enough
 - Try to delete a few Tb+?

Other Cloud Security Challenges



- *Liability*
 - <http://aws.amazon.com/agreement/>

11. Limitations of Liability.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

Other Cloud Security Challenges



■ *Licensing*

- Many license models
 - Per user
 - Per server
 - Per organisation
 - Floating licenses
 - Fixed to machines
 - ...
- Challenges with the Cloud delivery model
- (Where can jobs realistically run...!)

■ *Workflows*

- Many workflow tools for combining SoA services/data flows
 - Taverna, Pegasus, Galaxy, Kepler, Nimrod, OMS, ...
- Many workflows models
 - Orchestration (centralised definition/enactment),
 - Choreography (decentralised)
- Serious challenges of
 - defining,
 - enforcing,
 - sharing,
 - enacting
- security-oriented workflows

Other Cloud Security Challenges



■ *The Ever Changing Technical/Legal Landscape*



Overview of Cloud Computing Security Considerations

17. This section provides a non-exhaustive list of cloud computing security considerations. Each security consideration listed has a reference to the associated paragraph in this document that contains more detailed information about the security consideration. Placing a cross instead of a tick beside any of the following security considerations does not necessarily mean that cloud computing cannot be used, it simply means that the security consideration requires additional contemplation to determine if the associated risk is acceptable. Cloud computing security considerations include:

- My data or functionality to be moved to the cloud is not business critical (19a).
- I have reviewed the vendor's business continuity and disaster recovery plan (19b).
- I will maintain an up to date backup copy of my data (19c).
- My data or business functionality will be replicated with a second vendor (19d).
- The network connection between me and the vendor's network is adequate (19e).
- The Service Level Agreement (SLA) guarantees adequate system availability (19f).
- Scheduled outages are acceptable both in duration and time of day (19g).
- Scheduled outages affect the guaranteed percentage of system availability (19h).
- I would receive adequate compensation for a breach of the SLA or contract (19i).
- Redundancy mechanisms and offsite backups prevent data corruption or loss (19j).
- If I accidentally delete a file or other data, the vendor can quickly restore it (19k).
- I can increase my use of the vendor's computing resources at short notice (19l).
- I can easily move my data to another vendor or inhouse (19m).
- I can easily move my standardised application to another vendor or inhouse (19m).
- My choice of cloud sharing model aligns with my risk tolerance (20a).
- My data is not too sensitive to store or process in the cloud (20b).
- I can meet the legislative obligations to protect and manage my data (20c).
- I know and accept the privacy laws of countries that have access to my data (20d).
- Strong encryption approved by DSD protects my sensitive data at all times (20e).
- The vendor suitably sanitises storage media storing my data at its end of life (20f).
- The vendor securely monitors the computers that store or process my data (20g).
- I can use my existing tools to monitor my use of the vendor's services (20h).
- I retain legal ownership of my data (20i).



- The vendor has a secure gateway environment (20j).
- The vendor's gateway is certified by an authoritative third party (20k).
- The vendor provides a suitable email content filtering capability (20l).
- The vendor's security posture is supported by policies and processes (20m).
- The vendor's security posture is supported by direct technical controls (20n).
- I can audit the vendor's security or access reputable third party audit reports (20o).
- The vendor supports the identity and access management system that I use (20p).
- Users access and store sensitive data only via trusted operating environments (20q).
- The vendor uses endorsed physical security products and devices (20r).
- The vendor's procurement process for software and hardware is trustworthy (20s).
- The vendor adequately separates me and my data from other customers (21a).
- Using the vendor's cloud does not weaken my network security posture (21b).
- I have the option of using computers that are dedicated to my exclusive use (21c).
- When I delete my data, the storage media is sanitised before being reused (21d).
- The vendor does not know the password or key used to decrypt my data (22a).
- The vendor performs appropriate personnel vetting and employment checks (22b).
- Actions performed by the vendor's employees are logged and reviewed (22c).
- Visitors to the vendor's data centres are positively identified and escorted (22d).
- Vendor data centres have cable management practices to identify tampering (22e).
- Vendor security considerations apply equally to the vendor's subcontractors (22f).
- The vendor is contactable and provides timely responses and support (23a).
- I have reviewed the vendor's security incident response plan (23b).
- The vendor's employees are trained to detect and handle security incidents (23c).
- The vendor will notify me of security incidents (23d).
- The vendor will assist me with security investigations and legal discovery (23e).
- I can access audit logs and other evidence to perform a forensic investigation (23f).
- I receive adequate compensation for a security breach caused by the vendor (23g).
- Storage media storing sensitive data can be adequately sanitised (23h).