Cloud Security Lecture

- Click to add text

Mark McGloin

Infrastructure Security Lead

IBM Bluemix team

Agenda 2

- Overview of Cloud security
  - Different security considerations across different types of cloud
  - Differences against traditional web security, e.g. IaaS model, multi-tenancy for SaaS
  - Compliance and Privacy considerations
- Infrastructure security in the cloud
  - Operational security
  - Datacentre and network security
- Vulnerabilities and Attack vectors
  - Overview of some best practices and processes – SaaS specific?
  - Owasp Vulnerabilities. Denial of Service
  - Iaas and PasS Vulnerabilities
- Usable Security
- Identity and Access Management
  - Single Sign On
  - 3rd party authentication/authorization, e.g. oauth
  - Other Authentication/authorization related protocols

Overview of Cloud Security

- Different Cloud models
- Security considerations in the cloud: multi-tenancy, onboarding,
- Differences vs traditional I.T. Security: Security out of org's control
- Details of different security considerations in each deployment model, e.g. patches for IaaS

Various Cloud deployment models

Software as a service (SaaS)

Platform as a service (PaaS)

Infrastructure as a service (IaaS)

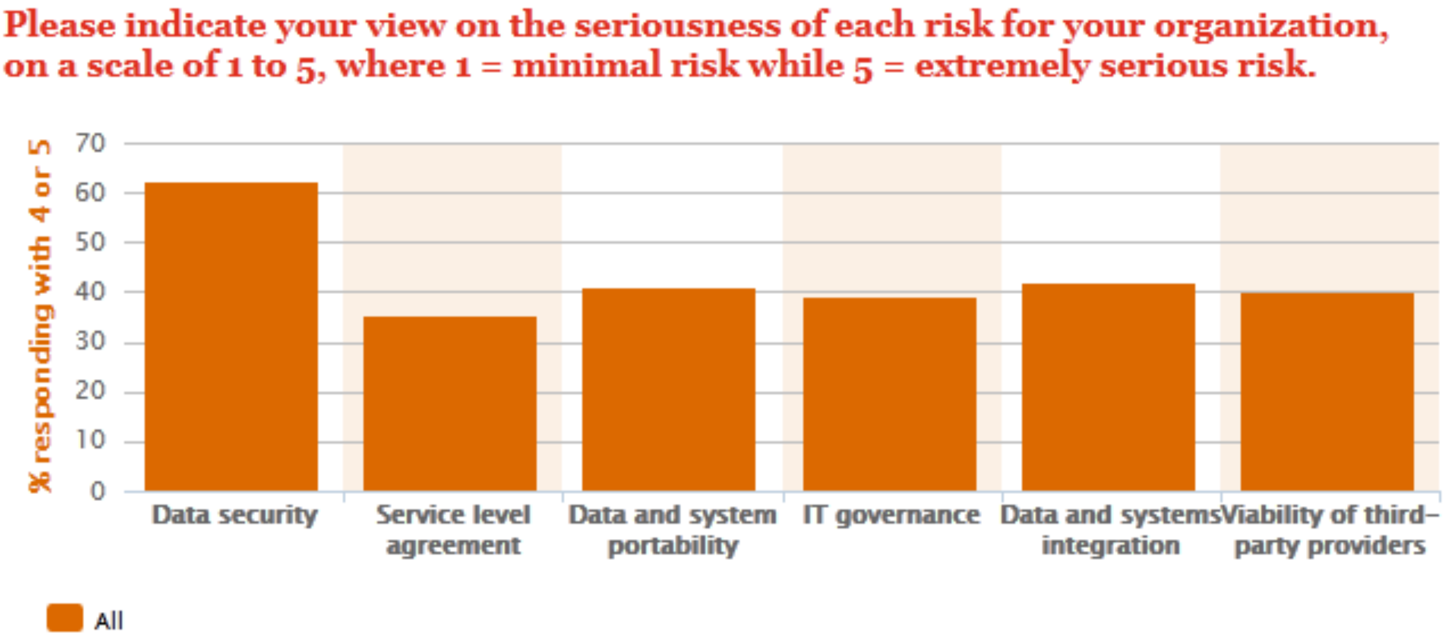
Public cloud

Private cloud

Hybrid cloud

Cloud Adoption

- PwC: Top barriers to cloud adption:



- Security a big barrier. Need to build story and allay fears

Cloud Security Considerations

- Security Infrastructure protection against threats and vulnerabilities
  - e.g. network intrusion detection, xss vulnerabilities
- Protection of data and resources
  - Is data secure in multi-tenant env. Data Leakage. What about Cloud provider employees accessing data?
- Compliance and Risk management
  - Organisations still responsible for I.T governance and legal compliance, e.g. Sorbannes Oxley
- Identity and Access Management
  - How will cloud provider identify my employees and provide proper authorization controls
- Privacy and Data Protection laws
  - German data laws prevent movement of Employee data outside Germany
- Managing security incidents
  - Process required for security professionals to register incidents and provider to act on them swiftly

Comparison against traditional I.T. Security concerns

- Multi-tenancy
- data and workload isolation
- Multiple identities
- Lack of control over security policy
- Lack of control over security patches
- Protection of backup data
- Lack of visibility to logs

Compliance standards

Many different compliance standards that need to be considered depending on solution or industry or customer.

Some examples:

- HIPPA: Healthcare specific regarding protecting patient medical info. Requirements around hardware, storage and network configuration not being shared dictate that a private cloud is the only way to truly comply
- SAS70, SSAE etc: Auditing standards. Really just ensure that you follow your own written processes but starting requirement for many enterprise organisations moving to cloud
- FISMA: U.S. Government encryption standards that are required if providing solution for any U.S. Public body (and many private ones)

Privacy and Cloud

Privacy laws vary around the world. Some examples

- Italy: More stringent laws on privacy and password strength
  - If providing SaaS solution, may need to consider privacy laws in target countries and ensuring compliance with them all
- Germany: Can't move employee data outside the country
  - Upshot is that not all data may be applicable for storage in cloud or cloud providers need to ensure data stored locally.
- U.S. Patriot Act: US law gives the government certain rights to access information as part of anti-terrorism investigations without informing you.
  - Reality is that similar laws exist in all nations.

Number of factors to consider when moving to cloud:

- Your organisation may not have control over the jurisdiction that your data resides in. Also applicable for data in motion but less of a concern
- As a Cloud Provider, you may need to provide data centres in different regions or provide technical solutions to assist customers comply with laws

Infrastructure security in the cloud

- Physical Datacentre security
- Encryption and Network Security
- Comply with best practices for reliability
- Operational Security and Processes for people

Data Center Security

- Personnel Authorization
  - Access requires current business requirement and revoked when business need ends
  - List of individuals with access re-validated quarterly
- Access Monitoring
  - Biometric controls at all physical access points
  - slab-to-slab barriers
  - man traps, motion sensors, alarms, and video

- Access Logging
  - Logs are periodically reviewed
- Security personnel
  - Manned 365 days a year, 24 hours a day
- High Availability
  - Redundant power and network connectivity

Network and Infrastructure Defenses

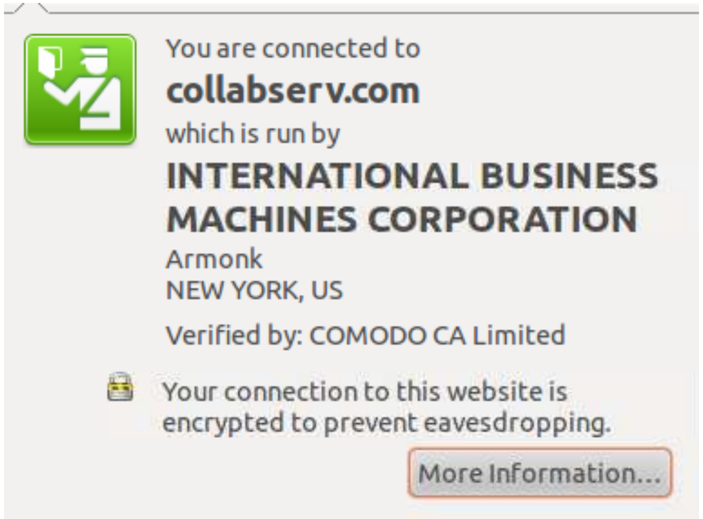
- High availability for all servers
- Protection
  - Layered firewall infrastructure protection
  - Operational remote access via secured VPN and redundant network
- Zones
  - All authenticated access in DMZ zone before user hits protected zone
- Detection
  - Deploy network and application intrusion detection/protection
  - Real time anti-virus and malware detection
  - Anti-spam protection on all incoming emails
  - Audit logs for logging and analysis of security related events

Encryption of data in transit and at rest

Encrypt all traffic entering and leaving Data Center

- Enforce SLL on all web traffic, e.g. 80 redirects to port 443
- SSL ciphers below 128 bits should be disabled
- Extended Validation (EV) certifcates for web browser traffic (more expensive)
- Opportunistic TLS for SMTP traffic entering and leaving

Minimum of 128 bit AES encryption of data at rest, e.g. Files and email folders



You are connected to

collabserv.com

which is run by

INTERNATIONAL BUSINESS MACHINES CORPORATION

Armonk
NEW YORK, US

Verified by: COMODO CA Limited

Your connection to this website is encrypted to prevent eavesdropping.

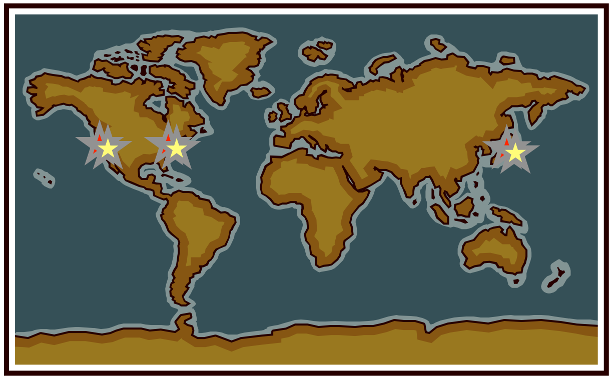
Disaster Recovery and System Backups

- Need failover sites in case of natural or man made disasters. Primary and disaster recovery data center

- Disaster recovery tested regularly, e.g. a minimum of twice yearly

- No service degradation; disaster recovery sites should be full duplicates of the primary sites

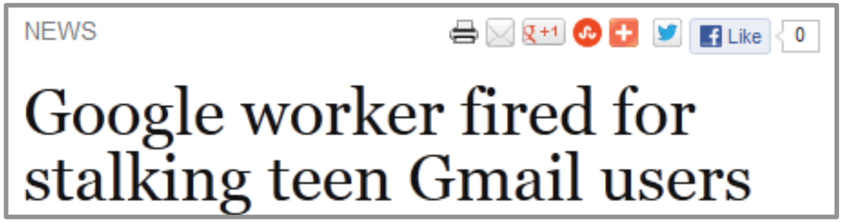
- Full system backups provide additional assurance
  - System backups encrypted with AES 128 bit
  - System backups kept off site for 30 days



Process for People

- Formal change management process for all changes to the production environment
- Separation of duty matrix to cover all operational and development personel
  - Segregation of activities and personnel with access to the code base and access to the operational configuration and data
  - Processes and tools to ensure that support and debugging information shared across that boundary does not carry private and sensitive information
- Privileged operational use requests reviewed against the separation of duties matrix
  - Should require management approval
  - Access monitored and logs reviewed regularly

Who secures against the operational team?



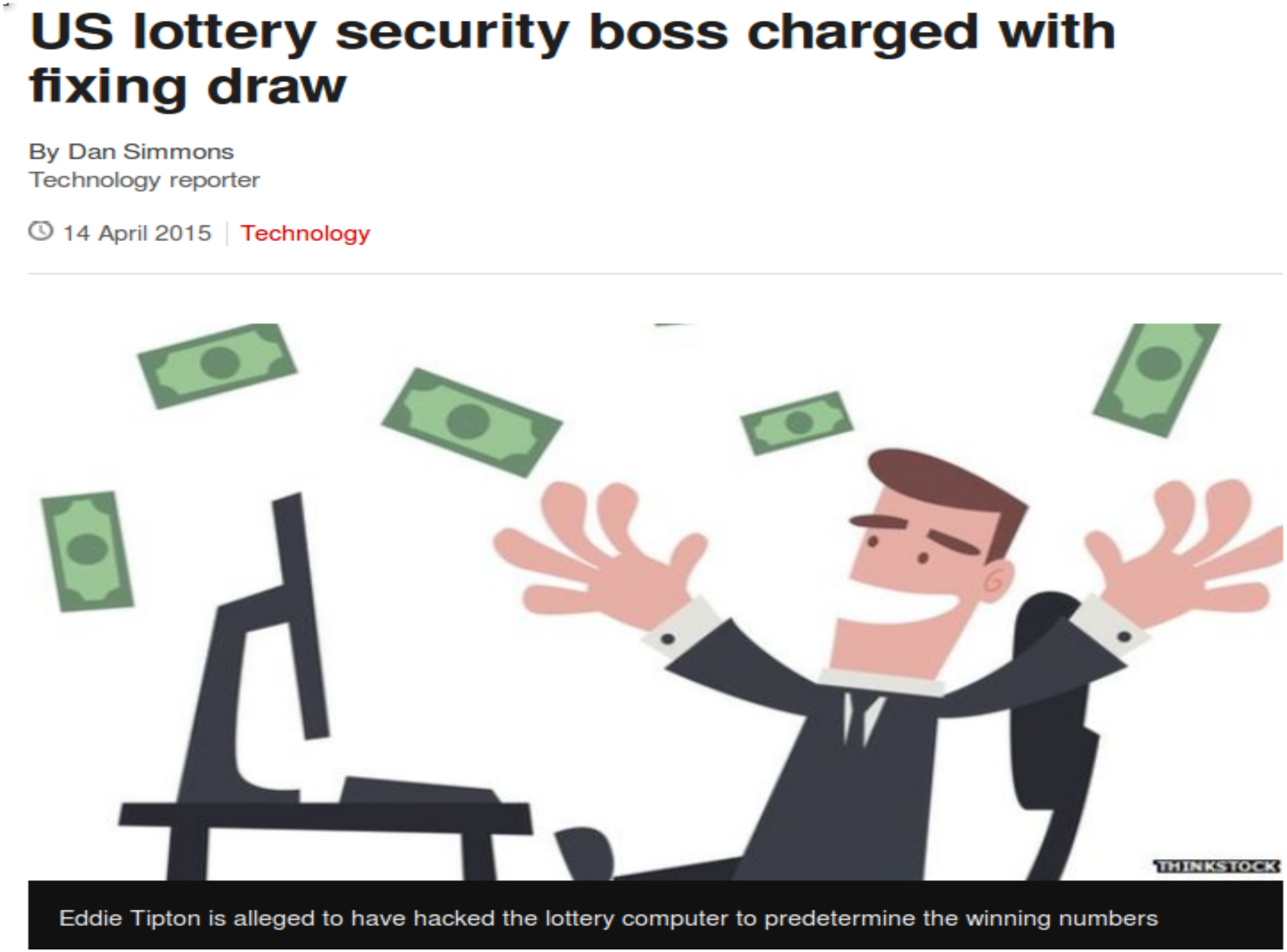
NEWS

Google worker fired for stalking teen Gmail users

Top Threats to Cloud Computing, Version 1.0

Threat #3: Malicious Insiders

French hacker who leaked Twitter documents to TechCrunch is busted



US lottery security boss charged with fixing draw

By Dan Simmons
Technology reporter

14 April 2015 | Technology

THINKSTOCK

Eddie Tipton is alleged to have hacked the lottery computer to predetermine the winning numbers

Security measures against Administrators

SaaS Protections

- Not all data may be suitable for cloud, e.g. Employee records
- Crytopgraphy: Encryption of resources before uploading. Distribution of keys issues for persons to decrypt shared data
- SoD measures and logging and detection (as discussed earlier)

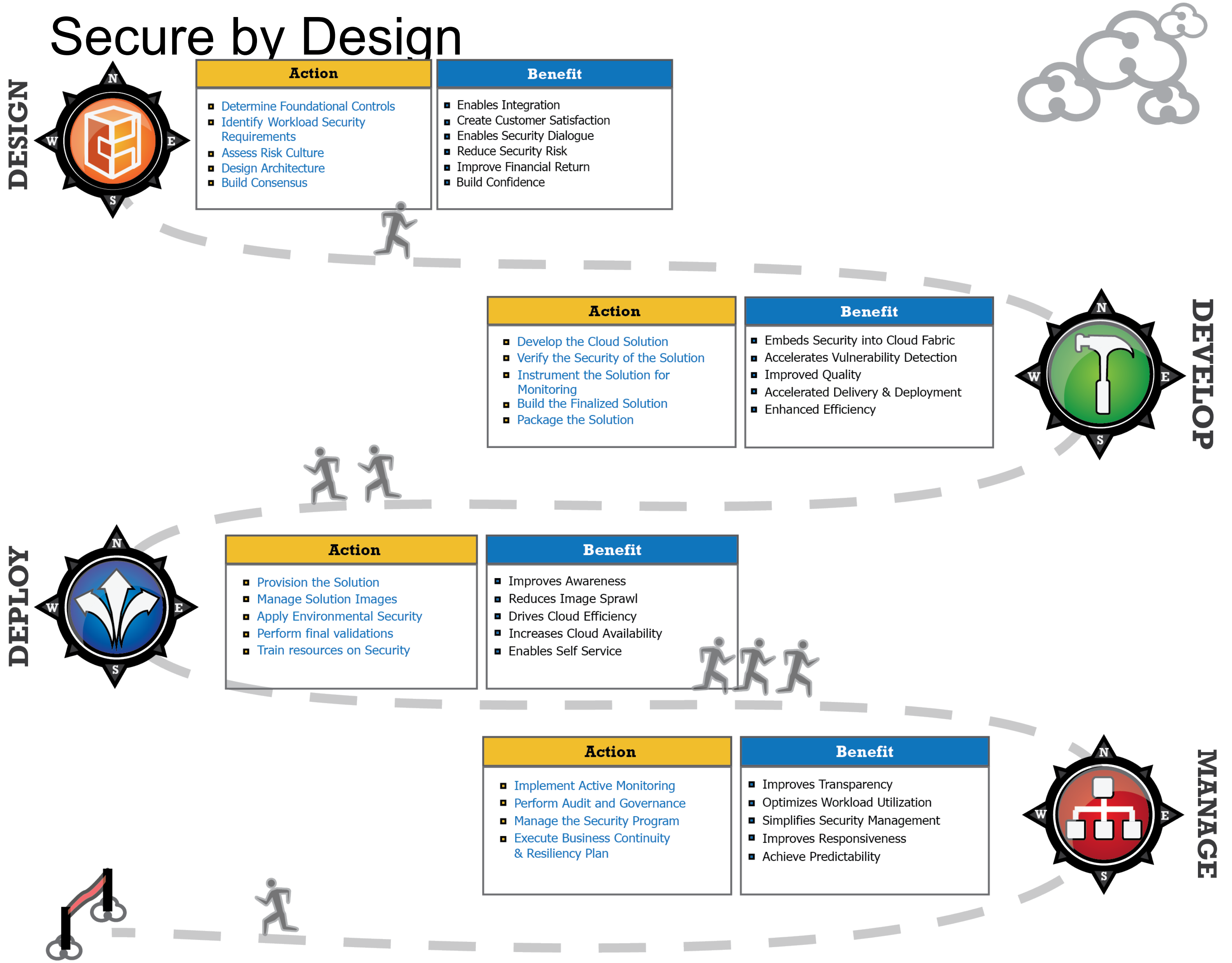
IaaS Protections

- Excluding private clouds, some level of access needed on physical server or to move/manage Vms
- Encrypted connections: Isolate customer VMs through customer secure shell (SSH) keys and server passwords
- Prevent VM dump. Use trust configuration to ensure certain hypervisor and software config enabled

Vulnerability Management

- Security by Design and processes
- Cloud Vulnerabilities
- Considering the end user

Secure by Design



DESIGN

Action

- Determine Foundational Controls
- Identify Workload Security Requirements
- Assess Risk Culture
- Design Architecture
- Build Consensus

Benefit

- Enables Integration
- Create Customer Satisfaction
- Enables Security Dialogue
- Reduce Security Risk
- Improve Financial Return
- Build Confidence

DEVELOP

Action

- Develop the Cloud Solution
- Verify the Security of the Solution
- Instrument the Solution for Monitoring
- Build the Finalized Solution
- Package the Solution

Benefit

- Embeds Security into Cloud Fabric
- Accelerates Vulnerability Detection
- Improved Quality
- Accelerated Delivery & Deployment
- Enhanced Efficiency

DEPLOY

Action

- Provision the Solution
- Manage Solution Images
- Apply Environmental Security
- Perform final validations
- Train resources on Security

Benefit

- Improves Awareness
- Reduces Image Sprawl
- Drives Cloud Efficiency
- Increases Cloud Availability
- Enables Self Service

MANAGE

Action

- Implement Active Monitoring
- Perform Audit and Governance
- Manage the Security Program
- Execute Business Continuity & Resiliency Plan

Benefit

- Improves Transparency
- Optimizes Workload Utilization
- Simplifies Security Management
- Improves Responsiveness
- Achieve Predictability

Security as a Quality

Security Checklist against every release

- Topics: authentication, identification, access control, encryption, auditing, integrity, deployment, user experience, mobile access, spam, privacy, multi tenancy, sessions, caching, coding, cookies, and testing

Security compliance

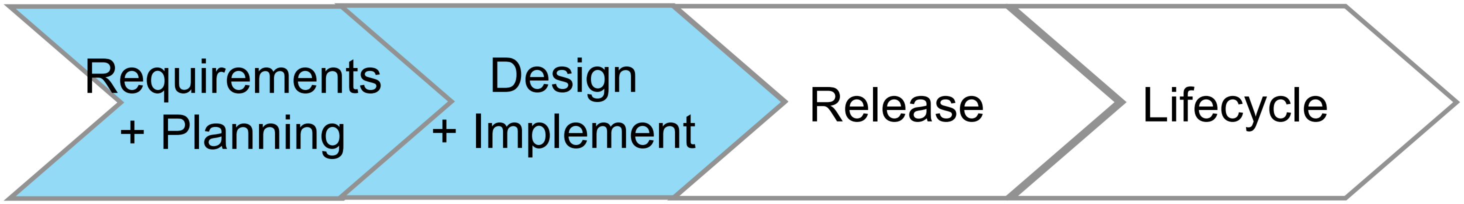
- Health checks should be performed regularly, using scripts and centralized security tools

Security Reviews

- Security reviews for any stories with security implications

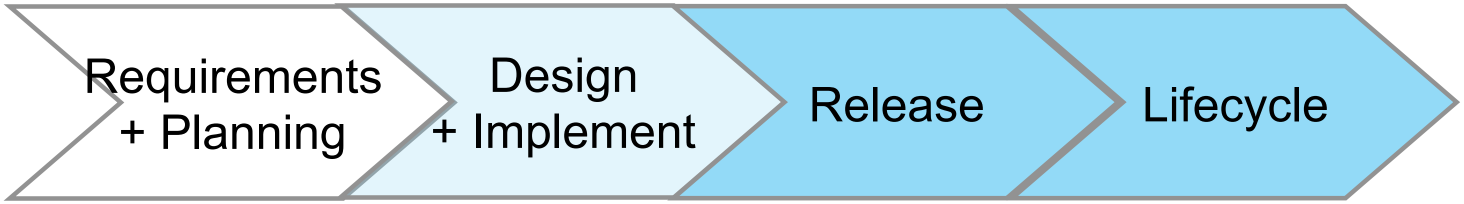
Design and coding practices

- Best practices to defend against vulnerabilities including XSS, CSRF, SQL injection

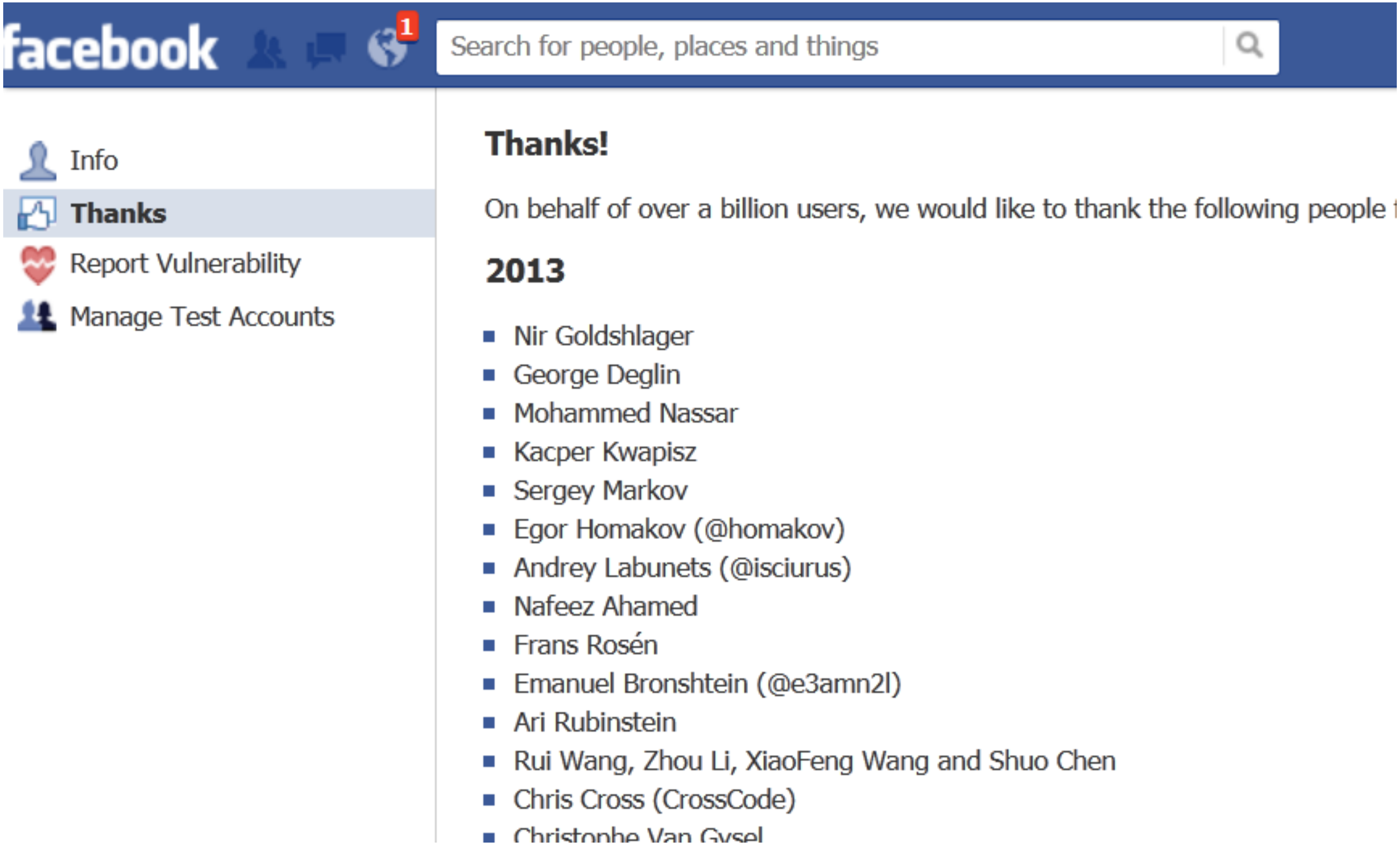


Security as a Quality

- Periodic vulnerability scanning of network and servers
- Automated testing of all applications and components on every iteration and every release, e.g. IBM Rational® AppScan®
- Manual ethical hacking. Automated tools will not catch everything and poor at some tasks, e.g. Persistent xss attacks
- Vulnerability Reviews
  - Review of status of all vulnerability related defects before deployment
- Incident management process engaged to investigate and determine appropriate actions for security events



Incident Reporting



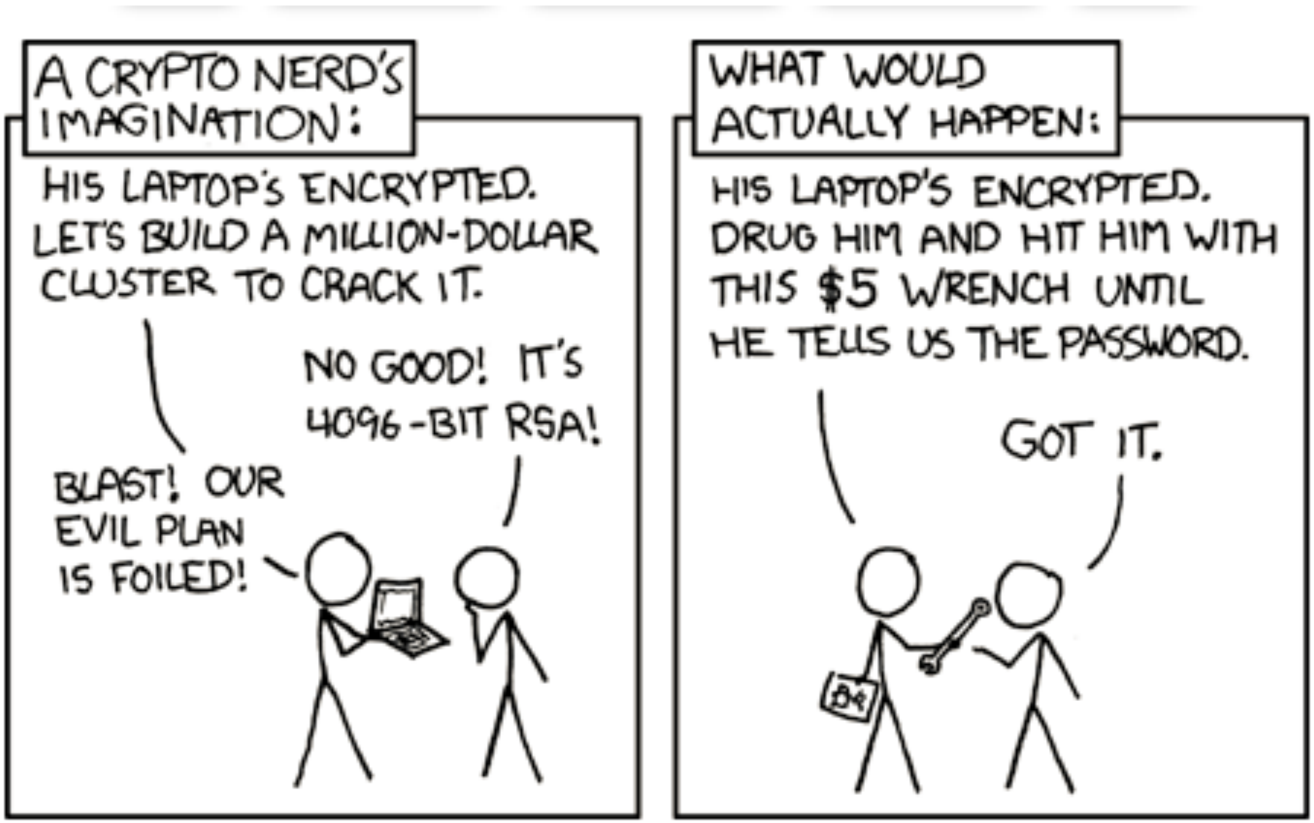
Thanks!

On behalf of over a billion users, we would like to thank the following people

2013

- Nir Goldshlager
- George Deglin
- Mohammed Nassar
- Kacper Kwapisz
- Sergey Markov
- Egor Homakov (@homakov)
- Andrey Labunets (@isciurus)
- Nafeez Ahamed
- Frans Rosén
- Emanuel Bronshtein (@e3amn2l)
- Ari Rubinstein
- Rui Wang, Zhou Li, XiaoFeng Wang and Shuo Chen
- Chris Cross (CrossCode)
- Christophe Van Gysel

Many different attack vectors in Cloud


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
B4

Cloud Vulnerabilities

Many excellent resources to check current vulnerabilities:

- Open Web Application Security Project (OWASP) Top 10
- NIST publications
- IBM X-Force Report

Some differences in concerns across different types of cloud deployments:

- For web applications, same considerations regardless of hosting yourself or in cloud
- SaaS: Need to ensure saas provider secure
- PaaS/IaaS: Phyical and network needs to be secure

Example Vulnerabilities – Not all cloud specific!

Vulnerability	Protection
SQL Injection: Attacker runs own sql	Paramaterized queries
XSS: Attacker exploits no escaping of input paramaters to run script in user's browser, e.g. Send sessionId to attacker	Escape all untrusted data
Broken authentication and session management	Use hardened and centralised authentication system. Step up auth
Indirect Object Reference: Attacker changes a parameter to object the attacker isn't authorized for.	Map indirect to direct values on server. Access control checks.
Insecure API Access: Attacker exploits flaws in api access possibly through partner application	Use trusted security protocols
Malware: Attacker exploits public cloud to distribute malware	Detection software
Password protection: Weak password policy and flawed password reset	Consider user in password policy.
Security Patches: Attacker exploits unpatched security vulnerabilities	Ensure patches applied in provider

Cloud Vulnerability Examples

Obama Twitter Account

- Attacker observed Obama (and other celebrities). Noted things like sayings Obama liked, such as name of his dog bo.
- Guess twitter account password based on that

Sony Playstation Attack

- 77 Million user accounts compromised
- A lot of user data was unencrypted
- Main criticism of Sony was lack of transparency and delay informing users

Attack on HBGary

- CEO Aaron Barr stated he would reveal Anonymous member.
- A custom written CMS application was exploited and the usernames/passwords were dumped from the users table.
- The passwords were hashed with MD5 but not salted so simple rainbow tables cracked some of the passwords.
- One non C-level accounts cracked had SSH non-root access to support.hbgary.com.
- This was elevated to root access using a known local privilege-escalation vulnerability for which written exploits were already available. Gigabytes of research info removed
- The CEO and COO had passwords were six lower-case letters and two numbers.
- Same passwords were used in Google, Twitter, and LinkedIn. Now the attackers had access to the CMS plus other applications like email.
- The CEO's was the admin for their Google Apps Mail services. By resetting users passwords, could gain access.
- One of those accounts, "Greg Hoglund", disclosed two potential root account passwords to a rootkit.com server but ssh as root not allowed. Also revealed that a Nokia employee had SSH access to that server.
- Social Engineering attack: Attacker impersonated "Greg Hoglund" and corresponded with the Nokia employee to get ssh onto server
- Once on server was able to elevate to root.

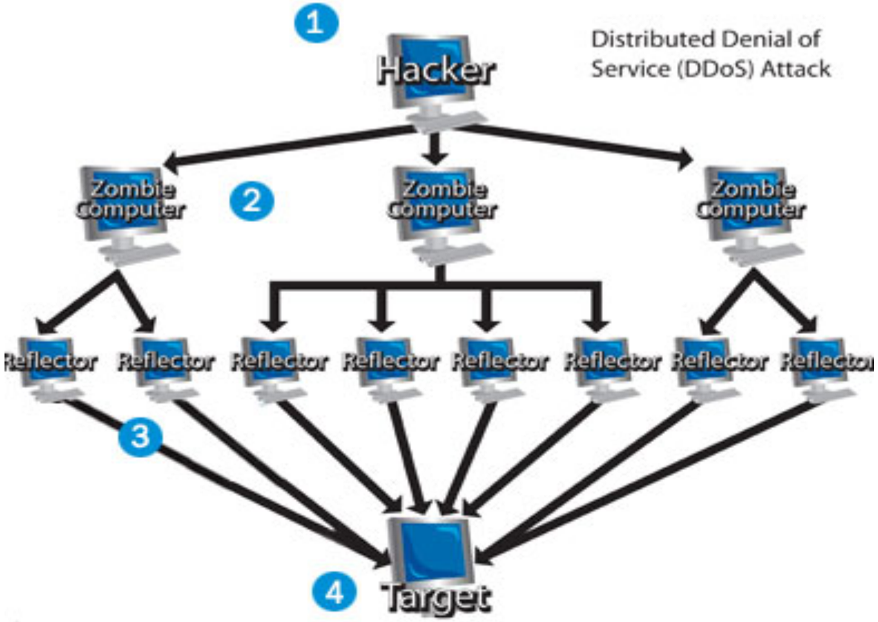
Denial of Service (DoS)

Prevent users accessing service by consuming all resources. Can happen at many levels, e.g. network or application

Types : syn flood, slow read attack, resource consumption, smurf attack

Distributed DoS : Attack from many sources, e.g. via botnet

% Machines botnet???



Extremely difficult to prevent

Cybercrime as a service

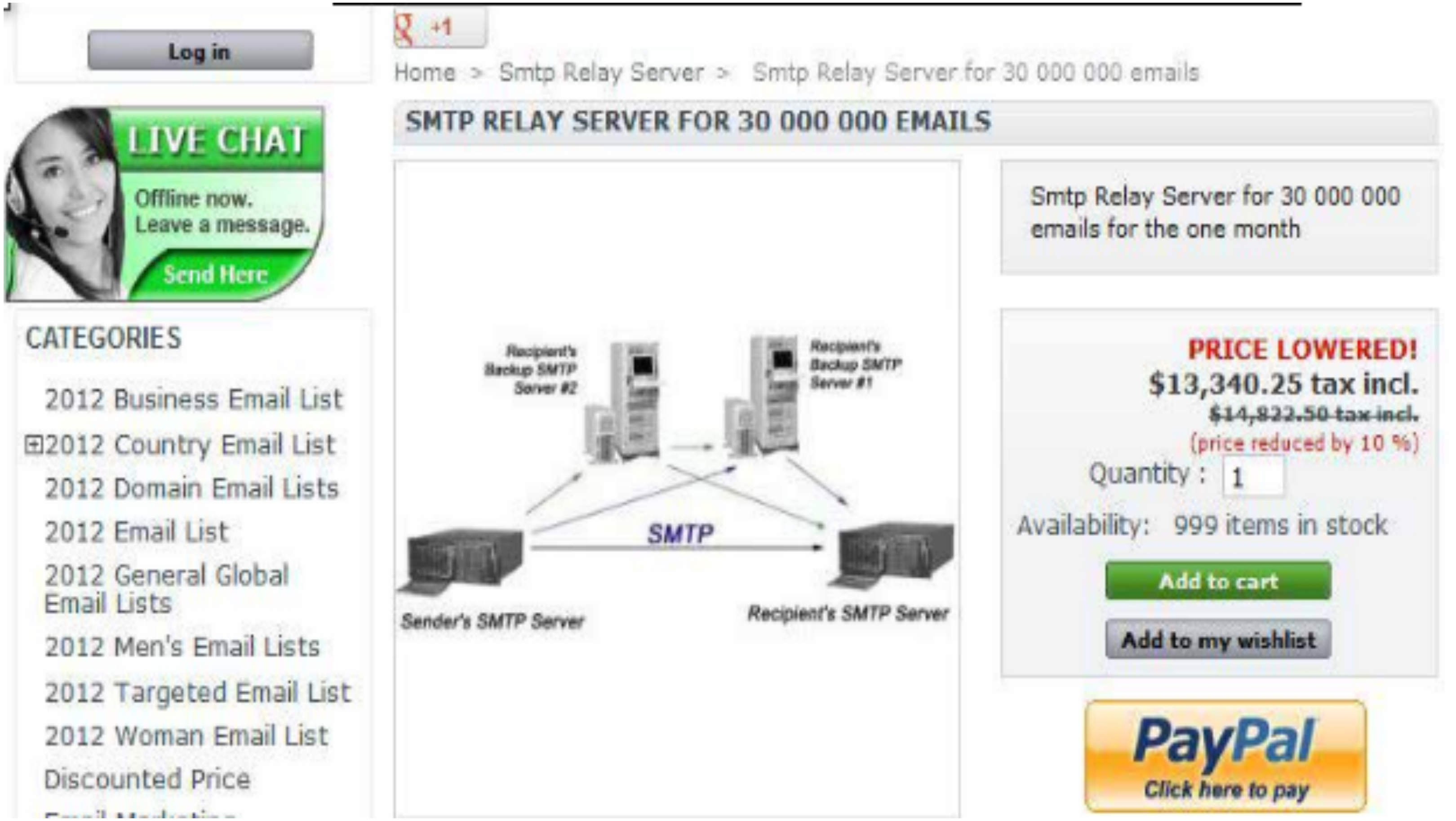
Rent a botnet of machines for illegal activities

DDoS for as little as 4.99 dollars to take down a website

Lizard Squad

DDoS attack tool, which is now available starting at $5.99 per month

Cybercrime as a service



+1

Log in

Home > Smtp Relay Server > Smtp Relay Server for 30 000 000 emails

SMTP RELAY SERVER FOR 30 000 000 EMAILS

LIVE CHAT

Offline now.
Leave a message.

Send Here

CATEGORIES

- 2012 Business Email List
- ⊞2012 Country Email List
- 2012 Domain Email Lists
- 2012 Email List
- 2012 General Global Email Lists
- 2012 Men's Email Lists
- 2012 Targeted Email List
- 2012 Woman Email List
- Discounted Price

Recipient's Backup SMTP Server #2
Recipient's Backup SMTP Server #1
SMTP
Sender's SMTP Server
Recipient's SMTP Server

Smtp Relay Server for 30 000 000 emails for the one month

PRICE LOWERED!

$13,340.25 tax incl.

~~$14,822.50 tax incl.~~

(price reduced by 10 %)

Quantity : 1

Availability: 999 items in stock

Add to cart

Add to my wishlist

PayPal
Click here to pay

IaaS and PaaS: Some specific security considerations

Applications and Organisations hosted in the cloud are all running in the same physical environment even though logical environment is separated

Potential risk to each other. Some characteristics required to protect that

- Isolation of tenant data and work space (memory)
- Isolation of tenant execution characteristics (performance, availability)
- Tenant-aware security, management, reporting
- Isolation of tenant customizations and extensions to business logic

Other IaaS/PaaS Attack Vectors

Exploiting VMs vulnerabilities or lack of security to access physical storage and network

Container or application server vulnerabilities: e.g. php server without security tightened

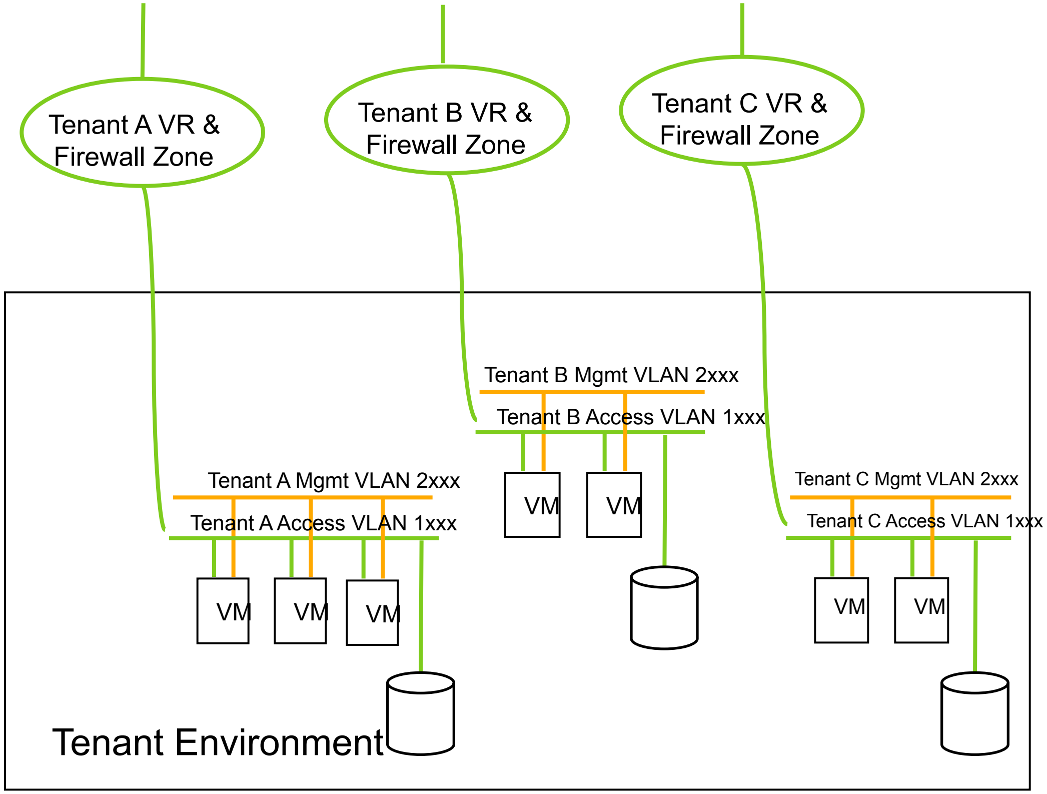
Port scanning used to detect network vulnerabilities

Attacks from Cloud customers against Internet resources, for example spamming or phishing

Separate VPN per Customer

Provides additional layer of network isolation

Provides for encryption of data over internet


Tenant A VR & Firewall Zone
Tenant B VR & Firewall Zone
Tenant C VR & Firewall Zone
Tenant B Mgmt VLAN 2xxx
Tenant B Access VLAN 1xxx
VM
VM
Tenant A Mgmt VLAN 2xxx
Tenant A Access VLAN 1xxx
VM
VM
VM
Tenant C Mgmt VLAN 2xxx
Tenant C Access VLAN 1xxx
VM
VM
Tenant Environment

May not provide encryption between Vms in the data center though

VM Security considerations

Applications and organisations are running in their own VM on shared physical hardware owned by Cloud provider. Some potential threats:

- Attempts to break out of the virtualized environment through ‘poisoned’ data, buffer overflows or other exception conditions
- Communication between different virtual machines or between a virtual machine and the host through shared disks, virtual switches, or virtual local area networks (VLANs) and a shared I/O or cache.
- Generic drivers that emulate hardware.
- Vulnerabilities in the hypervisor that allow the execution of arbitrary code on the host with the privileges of the hypervisor that allow an attacker to control all virtual machines and the host itself.
- Virtual machine-based root kits that allow for modification of the hypervisor system calls to the host operating system to run malicious code.
- An exploit, known as virtual machine escape, where a program in one virtual machine is given unrestricted access to the host through shared resources.

Hosting threats

Attackers can use Clouds to host botnets

Can use it as mechanism to spread malware

Providers need to constantly monitor network as difficult to put mechanisms in place to prevent in first place

Usable Security

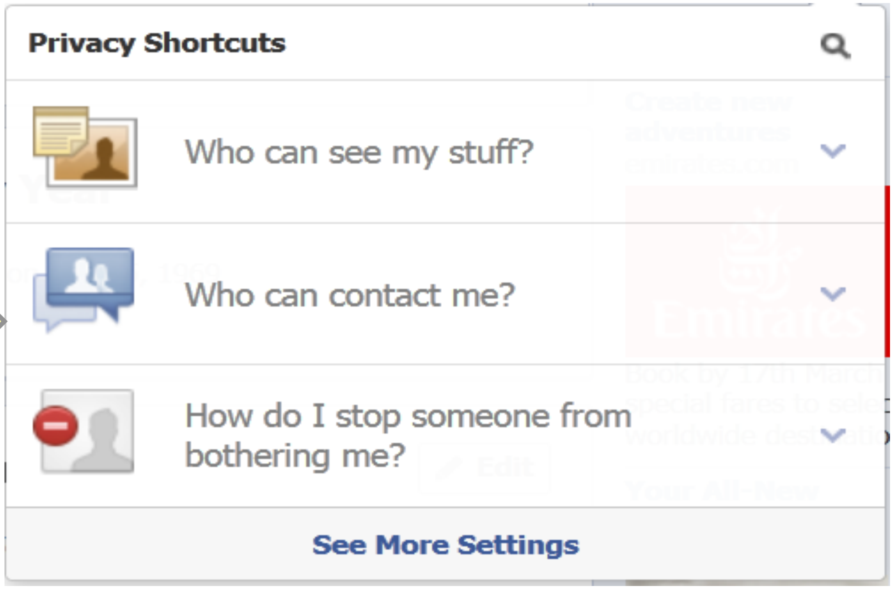
- Consider the users
- Transparent security

Security and Usability. Together.

- Ensure users considered to provide useful security
- Provide useful and usable security within the context of working with colleagues, partners, and customers
- Transparency of security ensures security awareness and assurance, for both end users and administrators
- Provide user control of collaboration and sharing
- Provide administrative control of user options
- Safe defaults reduce potential exposures
- Provide visibility on extending the organizational boundaries into the cloud

Security Transparency

- Provide full information to users on the security deployed
- For example, information on where they can be found within social network systems
- Provide Administrators with log and other information to allow them to make informed decisions on the security of their users



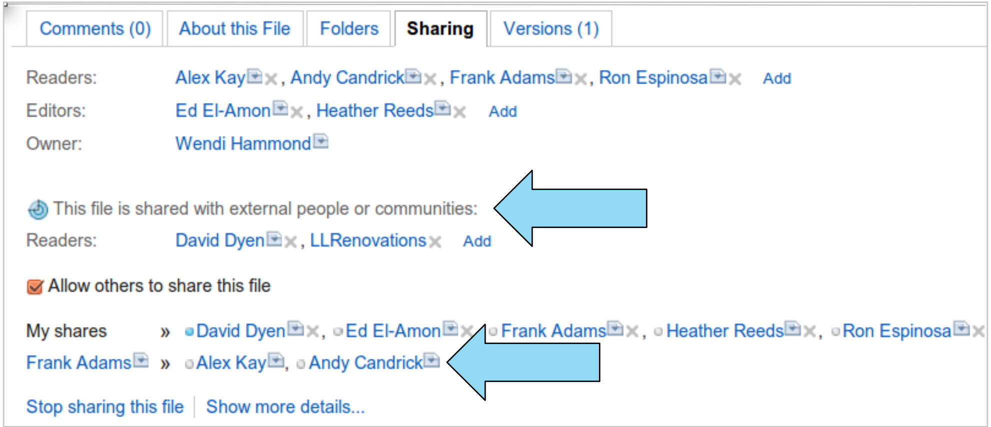
Privacy Shortcuts

Who can see my stuff?

Who can contact me?

How do I stop someone from bothering me?

See More Settings



Comments (0) | About this File | Folders | **Sharing** | Versions (1)

Readers: Alex Kay, Andy Candrick, Frank Adams, Ron Espinosa Add

Editors: Ed El-Amon, Heather Reeds Add

Owner: Wendi Hammond

This file is shared with external people or communities:

Readers: David Dyen, LLRenovations Add

☑ Allow others to share this file

My shares » David Dyen, Ed El-Amon, Frank Adams, Heather Reeds, Ron Espinosa

Frank Adams » Alex Kay, Andy Candrick

Stop sharing this file | Show more details...

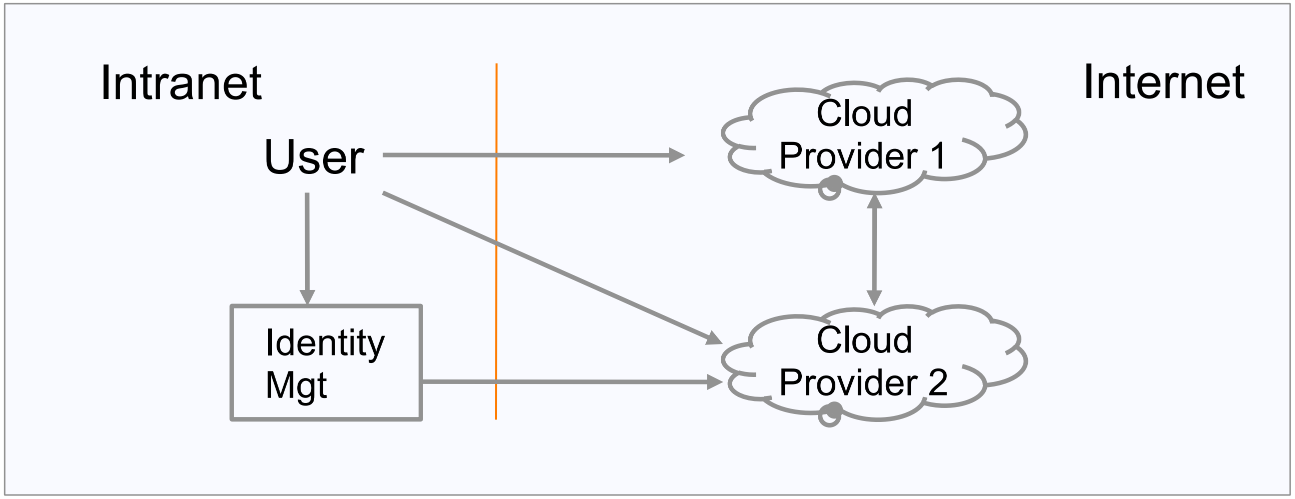
- Another example is visibility on sharing across organisational boundaires.
- Smartcloud example where I have visibility on where my files shared

Identity and Access Management

- Managing Identities in Cloud
- Federating Identity and Single Sign On
- Providing 3rd party access

Managing Identities in Cloud

- Some challenges in moving users identities to cloud



- Bulk configuration of those identities vs On-demand configuration/mapping of identity
- Various alternatives exist such as federating identity vs creating new identities in cloud providers
- SSO or partner access between cloud providers
- Third party providers exist to bridge the gap, e.g. Ping Identity, CastIron

General Identity Management considerations

- Initial identity verification, federated identities: Decide which makes sense
- Password complexity rules, expiration period, password reuse
- User roles defined with access entitlements: Some users should have less privileged access based on role
- System access granted, periodically reviewed, and revoked based on business need
- Access is logged, accountability maintained: Required to trace for any anomalies
- Identify and resolve separation of duties conflicts:
- Strong authentication and encryption of remote administration
- Monitor privileged access: Should ensure business need for this and access regularly

Different Approaches for providing Cloud identity

Users get new Identity for each Cloud Provider

Users login to their intranet and identity passed to cloud provider (federated identity)

User identity passed between Cloud providers

User provides other services with access to Cloud Provider resources

- e.g. Flickr photos shared with facebook account.

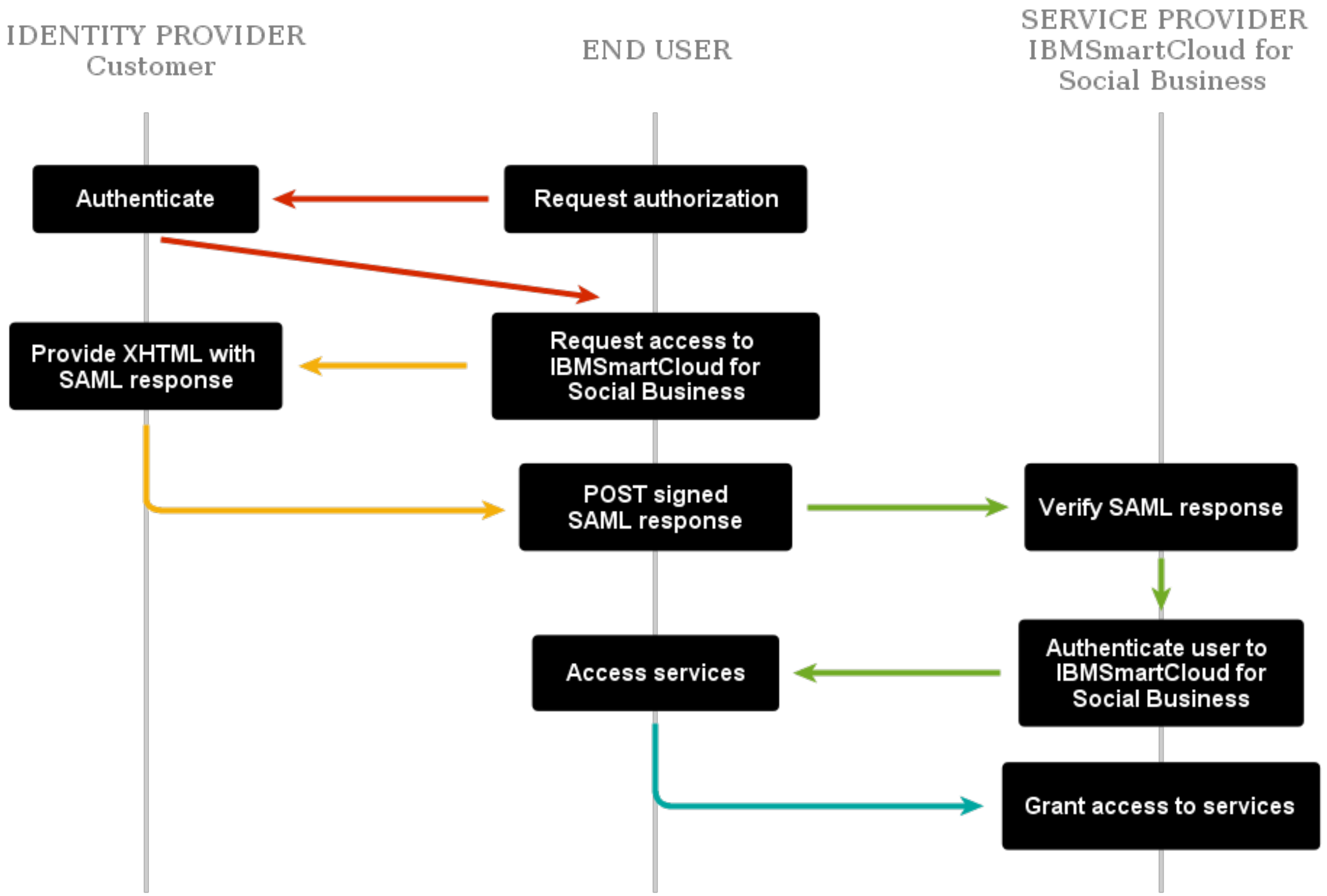
Federated authentication and Organisations

- Users from Organisation use existing intranet web passwords
- Keep your passwords behind your corporate firewall
- Manage your own password requirements
- Manage your own change intervals
- Manage your own re-use requirements
- Never send a password
  - Also designed to prevent crackers from guessing your passwords
- Because SAML is a public standard, you can use any SAML 1.1 or SAML 2.0 compliant identity provider
  - e.g. Microsoft's ADFS 2.0, OpenSAML

Federated Authentication: SAML Protocol

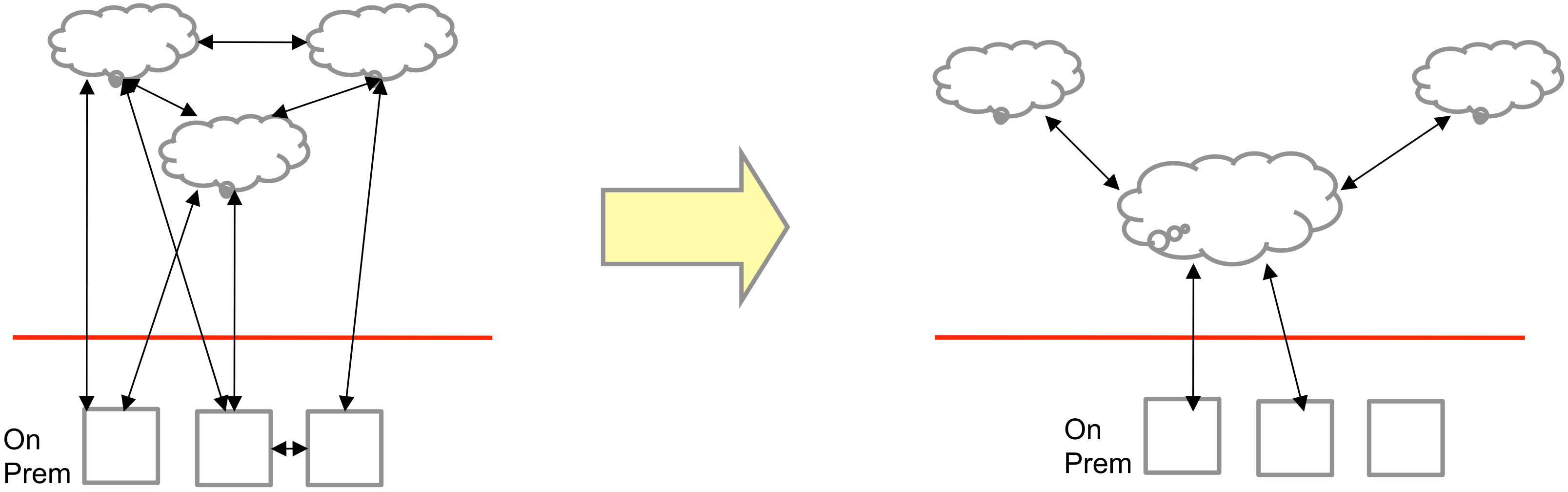
- XML-based open standard data format for exchanging authentication and authorization data between parties
- One party (Identity Provider) 'asserts' the identity of a user (principal) to the other party (Service Provider)
  - User identity: May include details on how user authenticated at IdP
  - Attributes such as role that user has.
  - Authorization statements such as permissions the user can have at the SP
- IdP signs the assertion to verify authenticity to SP. Partnership needs to be established between IdP and SP to pass credentials used to sign assertions
- OpenID is an alternative standard. Users create accounts with preferred OpenID identity providers, and use those accounts to sign onto website accepting OpenID. Main difference is loose web of Identity Providers. Organisations preference is saml standard as stronger verification of Identity Provider

Federated Authentication flow with IBM Smartcloud



Mapping Identity and integration between Cloud Providers

- Overhead in Organisations integrating with new Cloud providers or on-premises apps or Cloud Providers to Cloud Providers



- Certain providers can provide glue to reduce that many to many relationship, e.g. IBM Cast Iron or Ping Identity

Sharing access to Cloud Provider resources

Many examples where you want to provide a 3rd party with access to your resources stored in the cloud

- Share flickr photos with friends on facebook
- Provide printing service with access to flickr photos
- On premises application accessing organisation files stored in cloud

Need to provide access in secure manner using your identity

- Authentication credentials need to be passed somehow to 3rd party
- Only that 3rd party should have access to scoped resources, e.g. Only photos

Access generally required for period of time

- Don't want to involve user in providing access every time

Sharing Access: Different Approaches

Basic Authentication

- Provide your Cloud Provider username/password to 3rd party
- Undesirable to have 3rd party knowing your credentials
- More potential for those credentials to be phished or sniffed or stolen

Various Providers used proprietry protocols to improve security

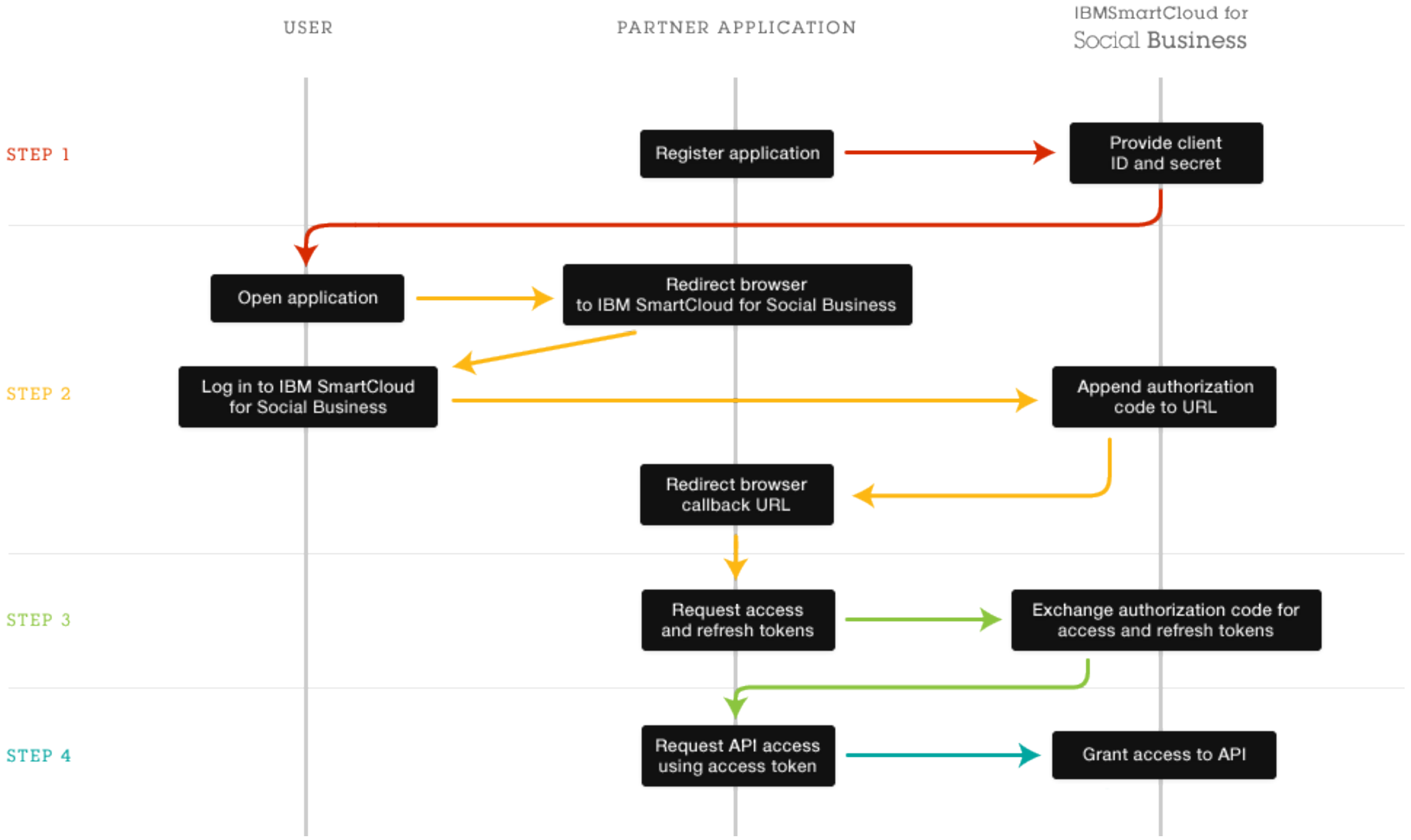
– Google AuthSub: Used Google's Authorization Proxy service to provide token

- Flickr Auth: Utiliise registered callback url based on api key and delivered token to that registered callback url

Oauth: Collaboration between providers and orgs to standardise 3rd party access

- Defacto standard for providing 3rd party access
- 3rd party does not know your cloud provider credentials

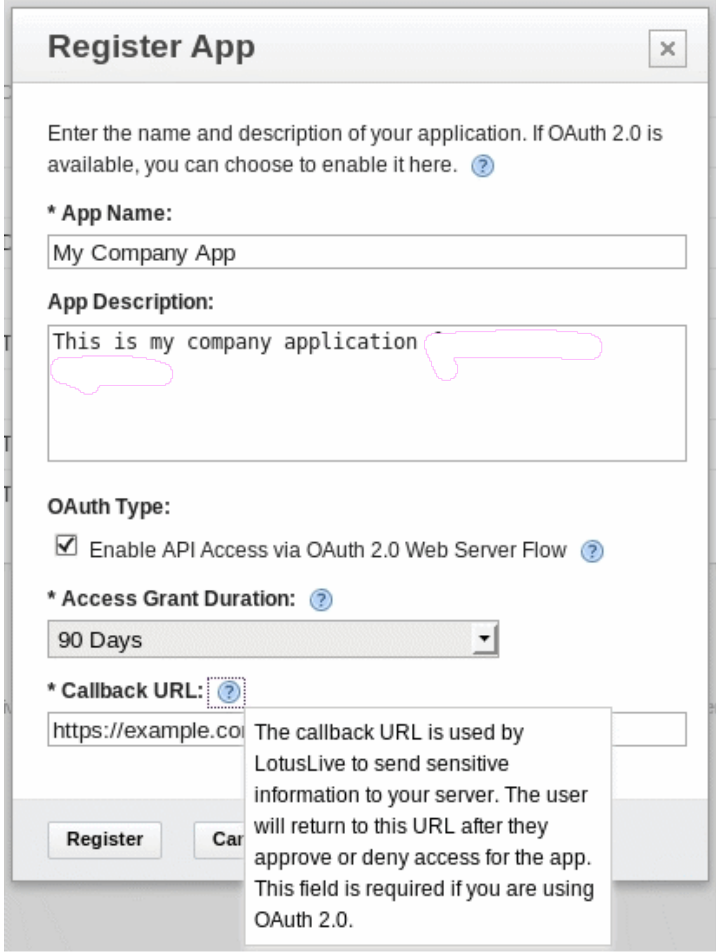
Sharing Access: Oauth details


USER
PARTNER APPLICATION
IBMSmartCloud for Social Business
STEP 1
Register application
Provide client ID and secret
Open application
Redirect browser to IBM SmartCloud for Social Business
STEP 2
Log in to IBM SmartCloud for Social Business
Append authorization code to URL
Redirect browser callback URL
STEP 3
Request access and refresh tokens
Exchange authorization code for access and refresh tokens
STEP 4
Request API access using access token
Grant access to API

Sign in with Facebook

- Use Oauth to provide access to your Faceboook Identity

Sharing Resources: Oauth and on-premises applications



Register App

×

Enter the name and description of your application. If OAuth 2.0 is available, you can choose to enable it here. ?

* App Name:

My Company App

App Description:

This is my company application

OAuth Type:

☑ Enable API Access via OAuth 2.0 Web Server Flow ?

* Access Grant Duration: ?

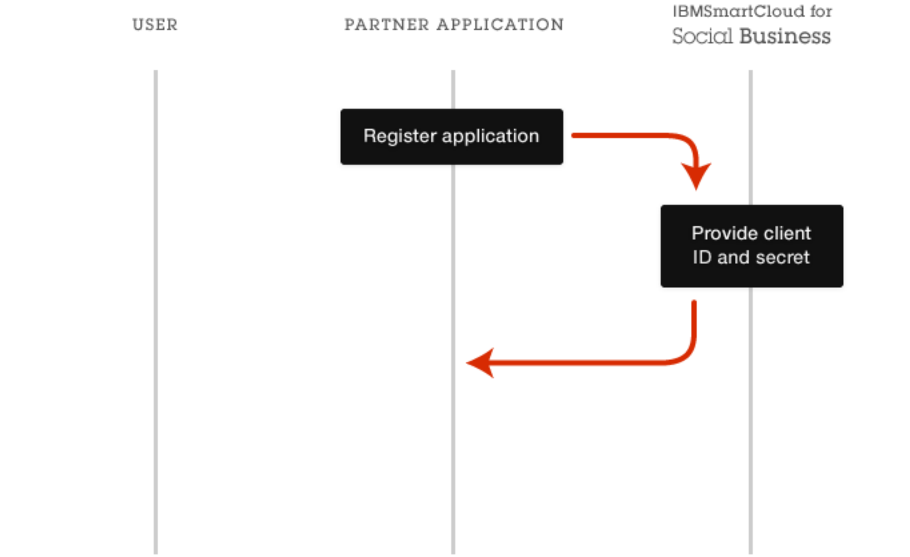
90 Days

* Callback URL: ?

https://example.co

The callback URL is used by LotusLive to send sensitive information to your server. The user will return to this URL after they approve or deny access for the app. This field is required if you are using OAuth 2.0.

STEP 1: Register Your Application

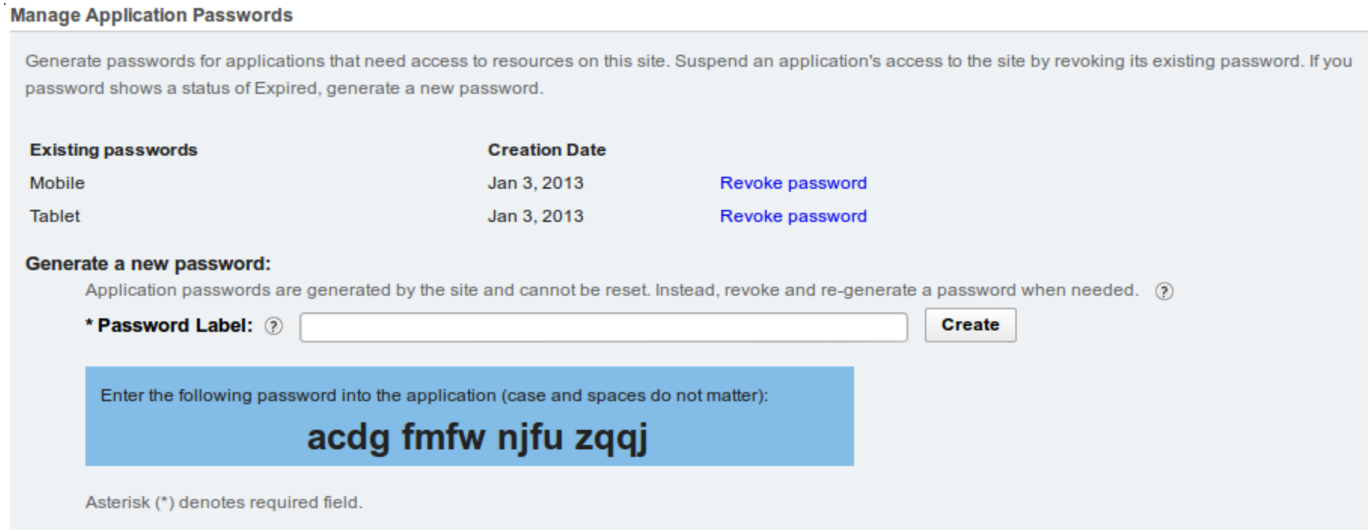


USER
PARTNER APPLICATION
IBMSmartCloud for Social Business
Register application
Provide client ID and secret

Just one example of Oauth usage
Bridges gap from on-premises apps to Cloud Provider

Application specific passwords

Application specific passwords: Provide alternative means to grant access to rich client or mobile app without using actual Cloud Provider credentials
Create a secondary password that application uses. If that password stolen, can simply disable it. Ensure can't access whole account with that password!!!!



Manage Application Passwords

Generate passwords for applications that need access to resources on this site. Suspend an application's access to the site by revoking its existing password. If you password shows a status of Expired, generate a new password.

Existing passwords	Creation Date	
Mobile	Jan 3, 2013	Revoke password
Tablet	Jan 3, 2013	Revoke password

Generate a new password:

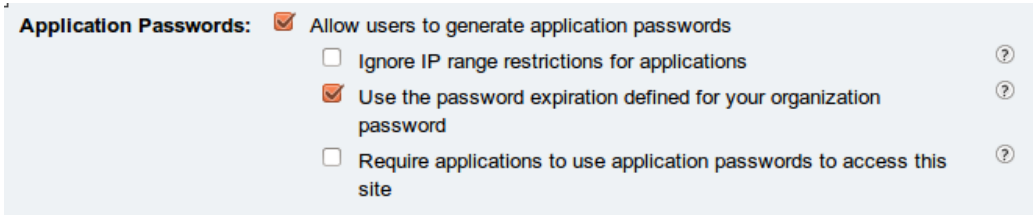
Application passwords are generated by the site and cannot be reset. Instead, revoke and re-generate a password when needed.

*** Password Label:** Create

Enter the following password into the application (case and spaces do not matter):

acdg fmfw njfu zqqj

Asterisk (*) denotes required field.



Application Passwords: ☑ Allow users to generate application passwords

☐ Ignore IP range restrictions for applications

☑ Use the password expiration defined for your organization password

☐ Require applications to use application passwords to access this site

Q&A