



OWASP

Open Web Application
Security Project

Viviendo en la Nube

Protegiendo los datos



Mauro Flores

OWASP Uruguay Chapter Co-Leader



Mauro.flores@owasp.org



@mauro_fcib

Top 10 Risks

R1 - Accountability
and Data Ownership

R4 - Business
Continuity and
Resiliency

R7 - Multi Tenancy
and Physical Security

R10 - Non Production
Environment
Exposure

R2 - User Identity
Federation

R5 - User Privacy
and Secondary
Usage of Data

R8 - Incidence
Analysis and
Forensic Support

R3 - Regulatory
Compliance

R6 - Service and
Data Integration

R9 - Infrastructure
Security



OWASP
Open Web Application
Security Project

R1 – De quien es la Información?

- Dependemos 100% del proveedor
- Puedo garantizar que el proveedor:
 - No los utiliza para otros fines (estadísticos, etc)
 - No se los vende a la competencia
- El único resguardo, un contrato... es suficiente?

R1 – De quien es la Información?

Es una locura tener toda la información en plano en la nube!!

Igual, deberíamos cifrar todo para estar seguro.

Muy lindo, pero si el proveedor accede a tus datos ni te enteras!



NSA - PRISM



Imposible!! El proveedor nunca lo va a hacer...además, para que le sirve?

Sos paranoico!! Tenemos un contrato que lo impide

Mauro, no jodas... si fuera por vos viviríamos todos adentro de una caja fuerte!

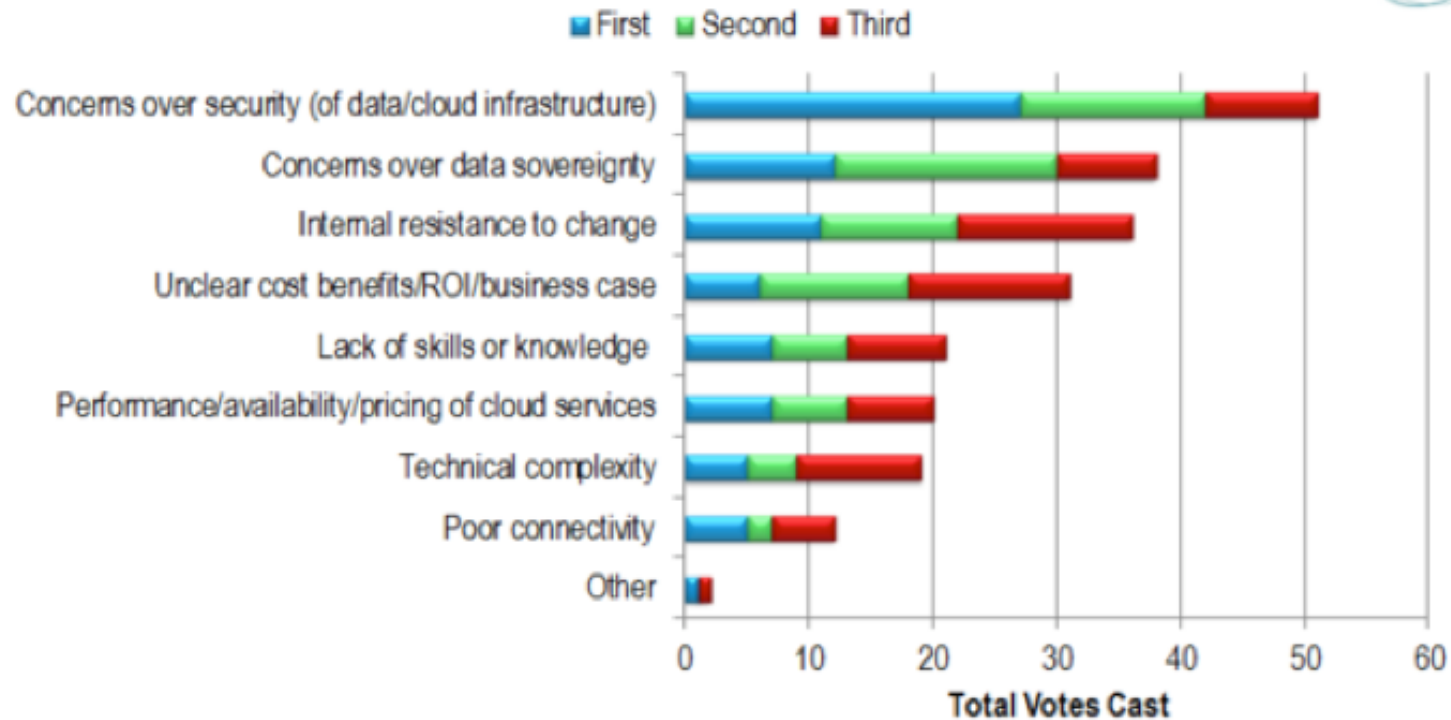
R1 – Que nos dejo PRISM?

- Desconfianza en la nube (especialmente las con base en U.S.)
 - 10% de cancelación de contratos
 - 56% no contrataría servicios en la nube en U.S.

R1 – Que nos dejo PRISM?

Which of these concerns do you think is holding back cloud adoption among enterprise customers in the markets/businesses you know best? (Vote top 3 – first, second, third)

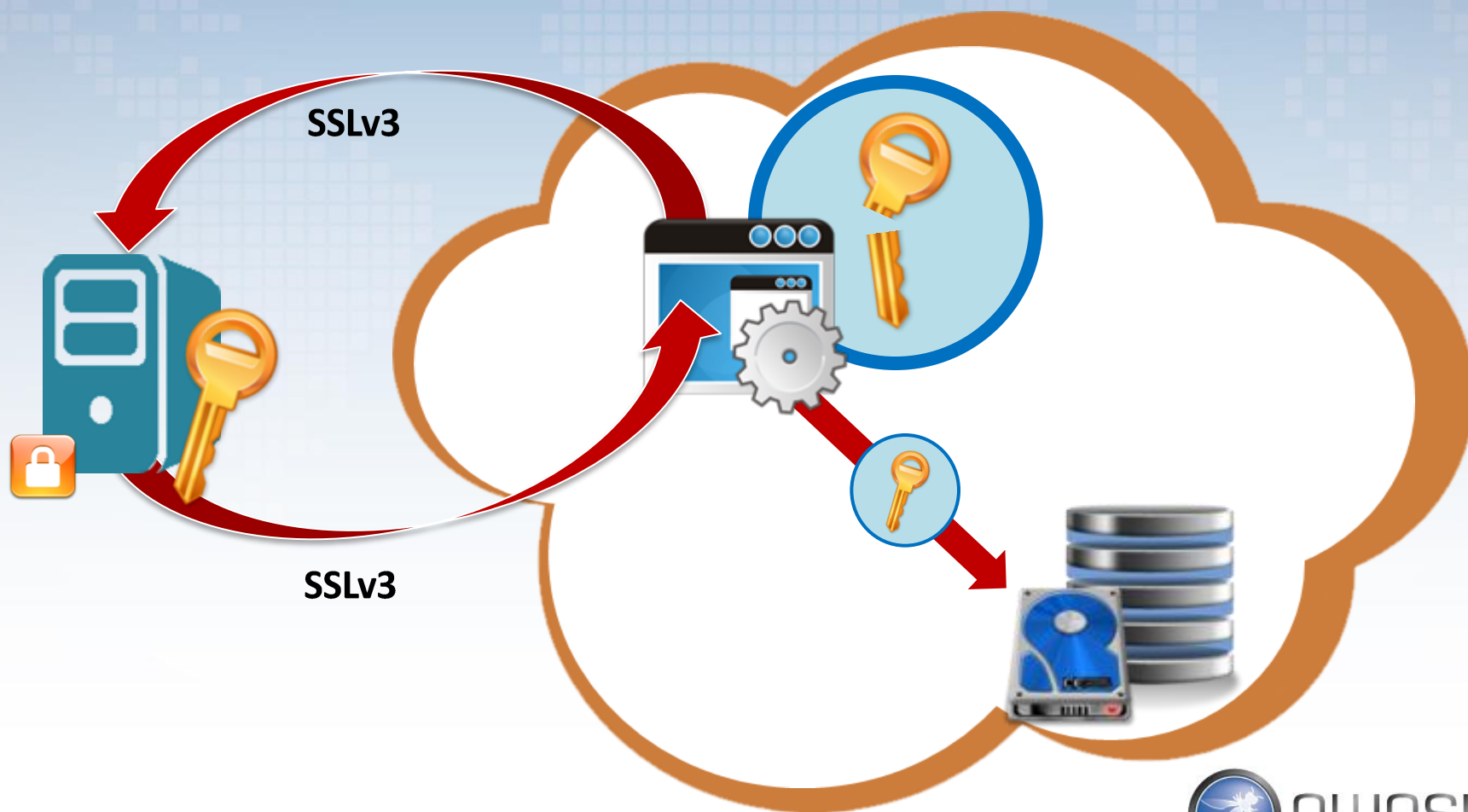
Source: Delegate Vote, New Digital Economics Executive Brainstorm, EMEA, June 2013.



R1 – Que nos dejo PRISM?

- Solo los contratos no son suficientes
- Necesitamos incluir tecnología que garantice la privacidad... y hacerlo bien!
- Debemos establecer una cadena de confianza que nazca fuera de la nube...

Protegiendo la Información



Recomendaciones

- Cifrar la información con algoritmos robustos
- No persistir las claves de cifrado
- Proteger las claves en memoria
 - No usar strings fácilmente reconocibles
 - Ofuscar o fragmentar la clave en memoria
- Utilizar múltiples claves de cifrado
 - Diferentes claves para diferentes grupos de datos



OWASP

Open Web Application
Security Project



Mauro Flores

OWASP Uruguay Chapter Co-Leader



Mauro.flores@owasp.org



@mauro_fcib

Gracias!!