Examination of Cloud + Encryption

May 2017

Paul Rich

prich@microsoft.com

My creds:

- https://www.linkedin.com/in/parich/
- Into my nineteenth year at Microsoft, the last twelve in Office 365
- Served from 1990-1994 in the United States Navy (crypto specialty)
- Prior experience in health care, insurance, commercial printing
- Little League umpire
- White water river guide
- Swift water rescue technician
- Married to attorney
- Soloed private aircraft
- Navigated nuclear-powered attack submarine
- Director of non-profit scientific research team
- Produced one pop-rock album that got radio play inside and outside the US
- Four kids: 28, 17, 9, 7

Disclaimer: imperfect, with perfectionist streak. Prone to monologues.

Our goals for this event

- ~~Learn about Office 365~~
- Improve your credibility, cover your ass
  - **Make good choices *without becoming an encryption expert***
- Solve the right problem, save lots of grief
  - **Help our organization and customers make better decisions where encryption is suggested, worshiped, imposed, or opposed**
- Relationships

Cloud-reluctant customers say

- I don’t know if Office 365 can meet my regulatory and compliance obligations
- I need transparency and control of my data before I can trust cloud services
- I want encryption key ownership

Fraternal Twins

What do these all have in common?

Taxes and tariffs
Health care
Primary education
Roads and bridges
Sports team and stadium locations
Air travel
Encryption

Bottom Line

- If you can’t articulate the problem, any solution is premature
- If you want SaaS, privacy is a legal, not technical, matter
- Encryption keys are dangerous little critters
- Contracts are king
- Regulations rarely play a role in dictating more than “encrypt”

Can you clearly describe a business problem you are trying to solve?

Hint: If it doesn't answer "why" then it is probably not the real business problem.

Teen: **I want a car**.

Why?

- Empowerment
- Flexibility
- Independence
- Ability to transport others
- Mobility
- Meet my job/school obligations

El Chapo

Psychobabble…qu’est-ce que c’est!?!

- E@R? IaaS? BYOK? PaaS? CYOK? SaaS? HYOK? Huh!?! What does all this mean?

The Subtle Art of Acronym

- IaaS – Infrastructure as a Service
  - What is *infrastructure*?
    - Power – electricity
    - Ping – network connectivity
    - Compute - processor
- PaaS – Platform as a Service
  - What is *platform*?
    - Database
    - Web server
    - Message queue
- SaaS – Software as a Service
  - What is *software*?
    - An application that requires no further programming
    - Enables fun (XBOX, Netflix) or productivity (Adobe, Office 365, G-Suite)

- E@R – recently come into common use; acromoticon for ***e****ncryption* ***at r****est*

What is implied in IaaS, PaaS, SaaS

- The missing letter
  - “C”
  - “Cloud”
- “Cloud” implies what?
  - “Not on my property”
  - “Out there on the Intertubes somewhere”
  - “That’s someone else’s problem”
- What is a “private cloud”?
  - “On my tubes”
  - “I own it. It’s my problem.”
  - “Not Google, Amazon, Microsoft, etc.”

- **B/CYOK** is when you **B**ring **Y**our **O**wn **K**ey to the cloud service and *the cloud service uses that key in the process of encrypting your data*
  - *The cloud service is a participant in the key chain and performs the encryption and decryption of customer data*
  - *You **C**ontrol **Y**our **O**wn **K**ey, cloud controls other keys*
  - *Cloud services can compute over customer data*
  - *SaaS features work*

- **HYOK** is when you **H**old **Y**our **O**wn **K**ey and *your own systems use that key to encrypt data that is then stored in a cloud service*
  - *The cloud service cannot perform encryption or decryption of customer data*
  - *Cloud services cannot compute over HYOK-protected data*
  - *SaaS features largely or entirely broken*

Beware of “ownership”

- Ownership does not mean exclusive use
  - ***Think about title to your car or the copyright on the song you sold on iTunes***

- “BYOK” (Bring Your Own Key) means *providing a key that you own for use with a cloud service*
  - ***It does not imply ownership of all keys used to encrypt your data***

Scenarios with B/CYOK and HYOK

- **B/CYOK** may help customers **meet compliance requirements** and may also enable additional service-specific functionality
  - Service **features function** as expected
  - B/CYOK could enable a customer to **"go dark" following service exit**
- **HYOK** enables scenarios where **customers' data is opaque to the cloud** service provider
  - With few exceptions, **HYOK disables SaaS functionality**
  - Used when **customer does not need SaaS features**

How did this get so misunderstood?

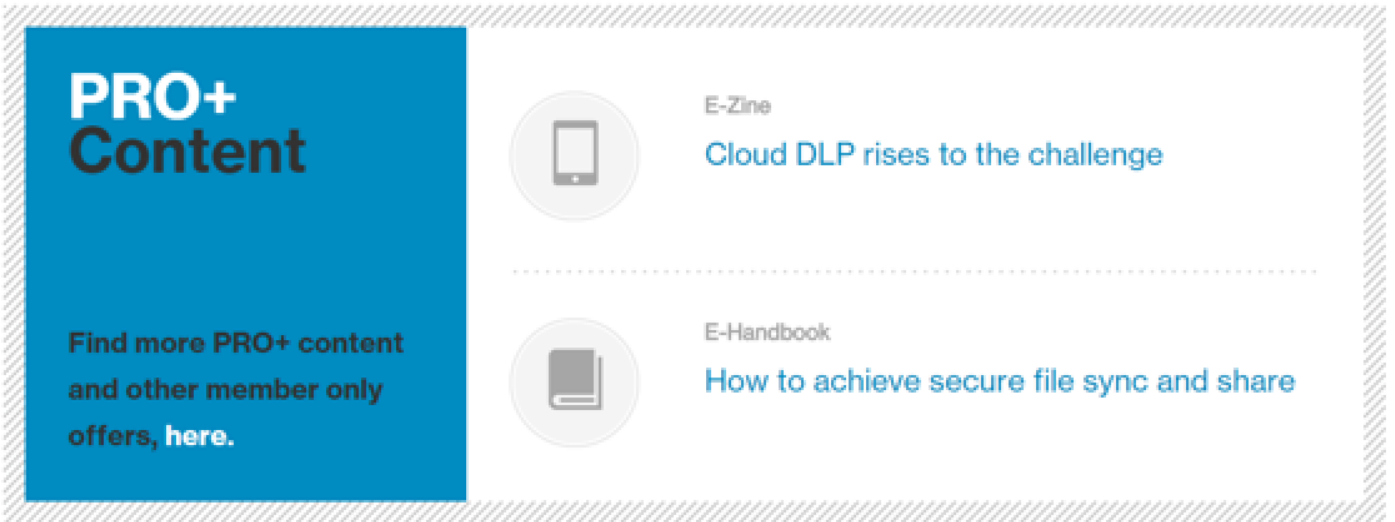
It’s very difficult for a short article to describe encryption systems without over-simplifying and enabling very broad interpretation and conclusions. Encryption is much more nuanced and complex than can be described in a few words, and attempts to do so inevitably lead to gaps in understanding. Unfortunately, sometimes technology vendors and journalists use vague or misleading statements that can be very seductive.

Let’s look at some examples.

http://searchcloudsecurity.techtarget.com/news/2240240111/Box-introduces-BYOK-encryption-key-management-service

With Box's EKM, a customer's data encryption key is sent to a customer-managed SafeNet Inc. hardware security module (HSM), while all audit logs are sent from the module to the customer. Since the customer keys are no longer kept with Box, it prevents the vendor from exposing any customer keys in a potential data breach or turning them over to the government.

Sounds powerful, but what does it actually deliver?



"Box never sees the customer keys," Wacker said. "They go right to the SafeNet HSM. And if the HSM is hosted, the companies hosting the modules can't see them either."

Let's examine further to see if this is accurate.

As a result, if government agencies such as the FBI or NSA want to obtain customer data stored with Box, they have to go through the customer -- and not Box -- to get it.

http://www.slate.com/blogs/future_tense/2014/04/03/box_is_working_on_a_feature_that_would_let_companies_keep_their_own_encryption.html

> If you gave the encryption key to your collaborators, you could absolutely encrypt data before it goes to Box and then your collaborator could decrypt that data as they download it. We would then never have the unencrypted data in the process. The challenge, of course, is most average business people and enterprises are not going to go through that experience because our differentiation as a company is to take security and combine it with a very simple user experience around working with information.

Why should customers be thrilled? And how does this relate to "decrypting on the user side?" What is the prize?

Basically, what he's saying is that encrypting and decrypting on the user side would make it trickier to use Box, which is designed for ease of use. For most customers, this trade-off probably wouldn't be worth it. But enterprise customers who prize security might be thrilled to hold their own encryption keys.

Notice that Box CEO is *not saying* "We are exploring ways that in the future Box cannot respond to 3rd party data requests.

This is not a new idea for Levie or the wider data security community, though Box would be implementing it on a particularly large scale. Last September, Levie **told *Ars Technica***, "We are exploring ways that in the future our customer would be responsible for its keys, and that's something we may make available to some of the largest organizations." Back then he didn't want to provide a solid timeframe, but now he is talking about offering such a service by the end of the year.

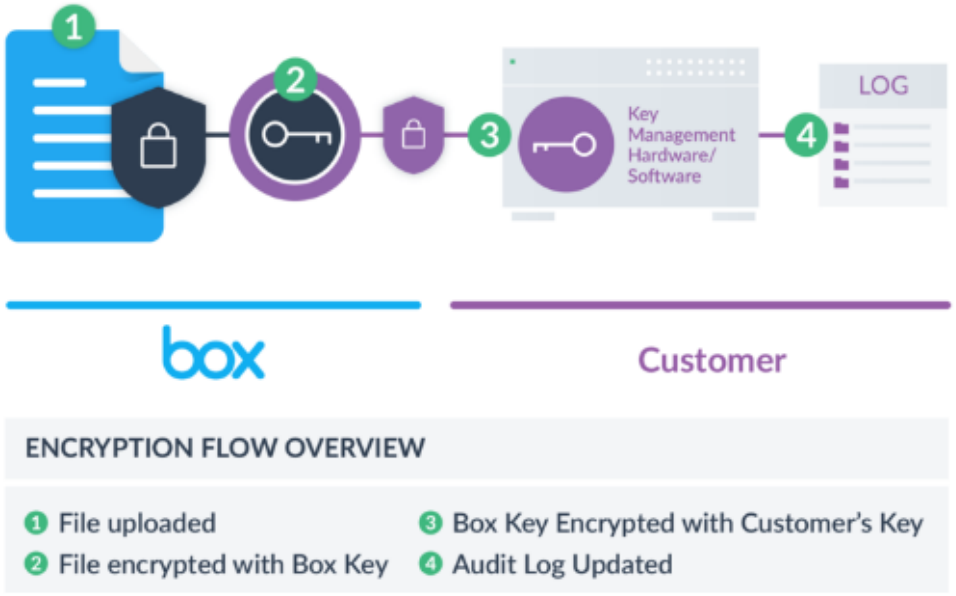
BOX “BYOK”

How Box KeySafe Works

Box partnered with Amazon Web Services to provide on-demand management of keys through AWS KMS (Key Management Services) and AWS CloudHSM—powered by Gemalto Enterprise—to support customers' needs for reliability, security and control over their sensitive content.

The Box KeySafe design uses multiple layers of encryption with the customer's key used as the outermost layer, allowing each customer to own and control the key for decrypting their files. Box KeySafe can be configured in under 30 minutes and requires very little ongoing maintenance.

READ THE DATASHEET



Note that data is encrypted with Box key upon upload.

https://blog.box.com/blog/box-keysafe/

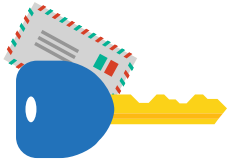
An example of SaaS and encryption dynamics

1. Mr. Intertubes the mailman delivers mail addressed to you to your cloud email service

2. A cloud email protection service analyzes contents to protect you from viruses and malware

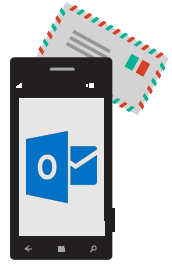
3. Your cloud email service analyzes email to execute tenant-defined rules (e.g. legal hold, archiving)

4. The message is delivered to your mailbox; the cloud service encrypts the contents



5. The cloud email service writes the encrypted message to storage

6. User requests email (browser, Outlook, etc.)



7. Your cloud email service decrypts the item, sends to client

8.

Examination: Fact or Myth?

- *Regulations mandate that I own my encryption keys.*
- *Encryption allows me to control all access to my data.*
- *BYOK prevents cloud personnel from accessing my data.*
- Letting your cloud provider manage your encryption key "*is similar to locking the door to your automobile and leaving the key in the door.*[1]"
- "*To ensure the safekeeping of encrypted data in the cloud, make sure you, not your cloud provider, maintain control of the encryption keys. If your provider requires you to hand over your keys, find another cloud service.*[2]"
- "*Would you give your keys to your home to someone you don't know?*"

1. http://www.networkworld.com/article/2986269/security/5-myths-about-data-encryption.html
2. http://www.wired.com/insights/2013/05/9-biggest-data-encryption-myths-busted-2/

“Regulations mandate that I own my encryption key”

Almost always FALSE

- Only a single known instance of a commercial regulatory body that specifies encryption key ownership*
  - **Compliance is self-imposed, so <u>you</u> have the power to shape this**
- Encryption key ownership is an implementation detail
  - **It’s specifying a solution, not a requirement**
    - **“Cryptographic keys must be stored in the corporation Banking and not at the cloud service provider.”***
- For most organizations, will turn out to be a headache or even a nightmare
  - **Almost universally, encryption key management is a neglected, poorly understood, underfunded and risky responsibility**

*Bank of Israel, Supervisor of Banks, memorandum 15LM2087, June 29, 2015.

“Encryption allows me to control all access to my data”

Almost always FALSE

- Encryption, on its own, can rarely be relied upon as access control
  - If I want to share with no one then encryption is potentially the best access control available
  - For any sharing of my data either the keys must be shared or access control must be used
- The control scope must match the key scope
  - Consider the USB drive with BitLocker and all your personal files
  - Consider the plumber or housecleaning or car valet service

“BYOK prevents cloud personnel from accessing my data”

False

- Key *ownership* has nothing to do with cloud personnel accessing your data
  - The ability to decrypt data is what matters
- If key ownership = key control does that change the situation?
  - Only where the design of the system provides this outcome
  - Only if the key owner can reasonably exert control to grant or revoke the ability to decrypt
  - Only if the key scope matches the desired control scope
  - Keep in mind the intersection of large numbers and human capabilities
  - What is the problem you are trying to solve?

“Giving your encryption key to the cloud provider is like locking your car and leaving the keys in the door.”

False

- Locking car and leaving keys in the door is *not locking your car* and *exposing your car to theft*. Why do we lock our car?
  - **A criminal might steal the car, or its contents**
  - **We want to control access to the inside of the car**
- Maybe meant “like giving your keys to the valet attendant”
  - **Valet attendants are human; cloud services can be built so that no humans have access to keys**
  - **Same protection against criminals, assuming valet is not criminal**
  - **Need to know if you stop sharing keys when you no longer want to allow access**

“Would you give your keys to your home to someone you don’t know?”

Div/0

- A cloud service with which you have a contract is not “someone you don’t know”
  - **Contract law is one of the oldest types of law in the world – see https://en.wikipedia.org/wiki/Contract**
  - **Good contracts have clear obligations with fraud, negligence and breach of contract liabilities**
- For most people, the use of keys to your home is not logged
  - **Cloud services may be able to provide a log of all activities performed with an encryption key**
  - **Broadening this concept, your cloud service provider should log all operational support actions that access your data**

What have we learned?

- Encryption is complex and generally not well understood
- Lots of public statements about encryption are false or very misleading
- Without knowing where data is encrypted and unencrypted, just saying "encryption" is largely meaningless
- Focus on contract commitments, access controls, and the law
- When a problem isn't clearly defined, solutions often don't meet business needs

True or False?

"Encryption key ownership provides me with protection against 3rd party subpoena"

False

It is the data decryption model that matters, not ownership of keys.

Bottom Line, revisited

- If you can’t articulate the problem, you aren’t ready for a solution
- If you want SaaS, privacy is a legal, not technical, matter
- Encryption keys are dangerous little critters
- Contracts are king
- Regulations rarely play a role in dictating more than “encrypt”
- **It’s simpler than you think, but not intuitive**

End of my content, time for…

- Questions
- Objections
- Arguments
- Soapboxing
- Speechifying
- Diatribes
- Trolling
- Drinks

Helpful References

- Salesforce announces BYOK – salesforce.com
- http://www.slate.com/blogs/future_tense/2014/04/03/box_is_working_on_a_feature_that_would_let_companies_keep_their_own_encryption.html (Q1 2014)
- BOX announces BYOK - TechTarget
- BOX KeySafe – box.com
- https://en.wikipedia.org/wiki/Cryptographic_hash_function
- https://en.wiktionary.org/wiki/homomorphism
- https://en.wikipedia.org/wiki/Homomorphic_encryption