

Protecting content: the new challenges during production

Eric DIEHL

VP media & security technologies



A little help by my friends

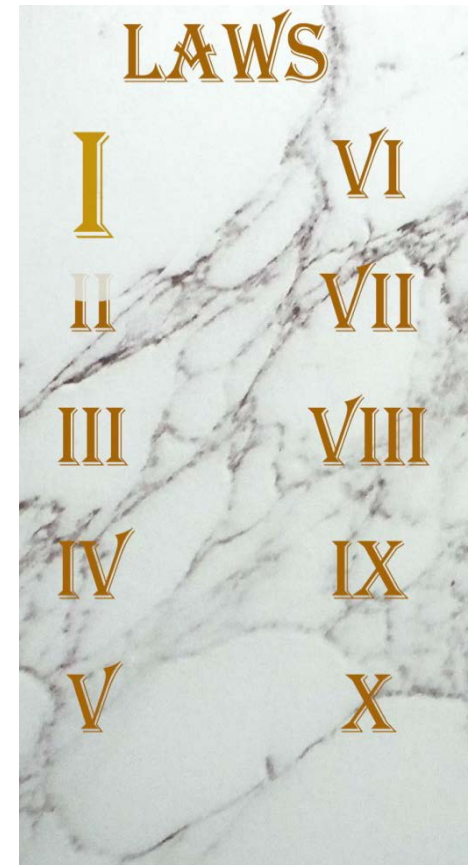
Ten laws for security

Selected over 20 years of practice

Used every day

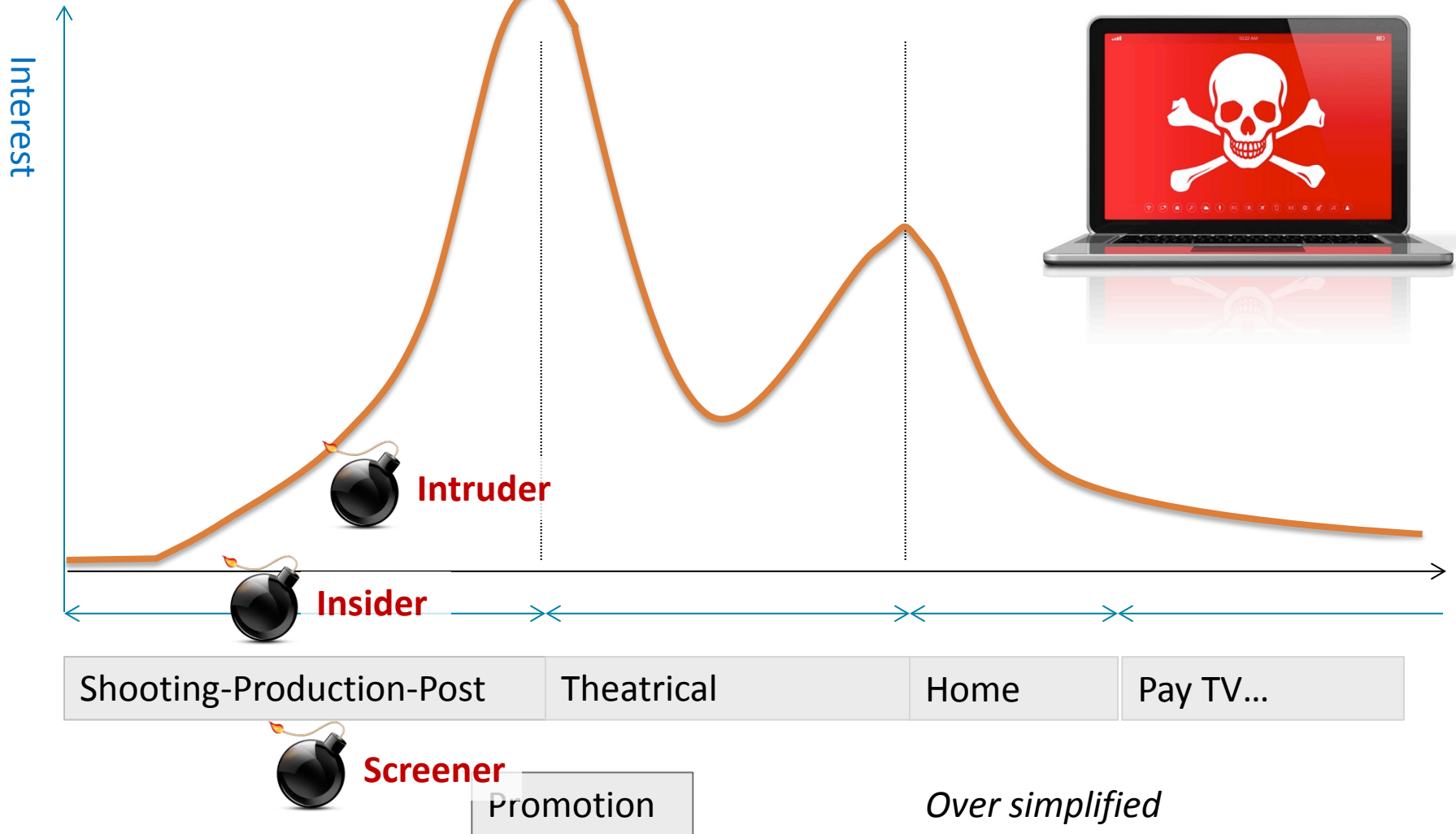
Available at <https://eric-diehl.com/ten-laws/>

- Law 1: Attackers will always find their way
- ...
- Law 10: Security is not a product but a process



Why protecting during production?

The pirate interest curve



Myth: why should I do it?

My environment is secure

- Law 1: Attackers will always find their way

We are among trusted people

- Law 4: Trust no one
- Law 7: You are the weakest link

An unfinished movie has no interest

- There were already some severe leaks

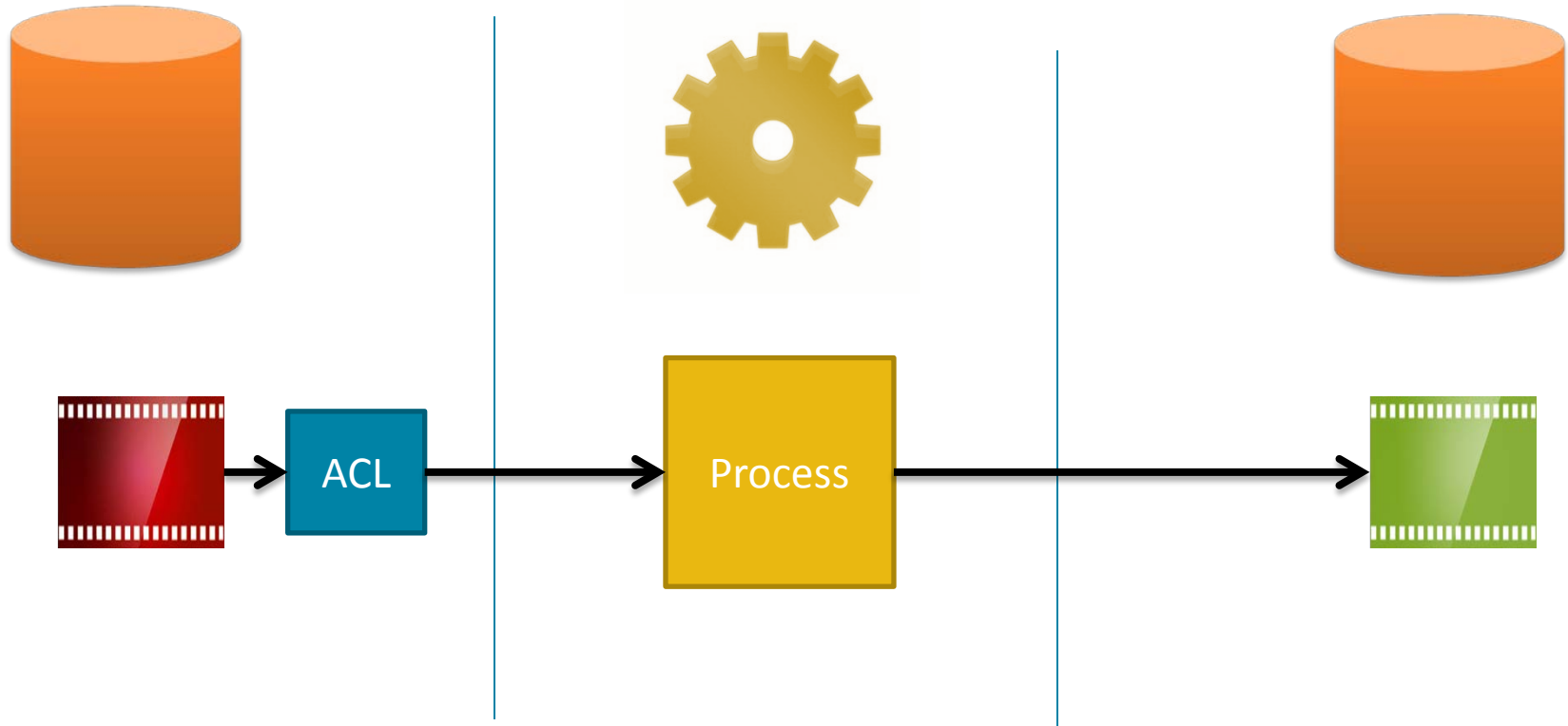


Encrypt, encrypt, encrypt

A long journey to ultimate encryption

1- Access Control

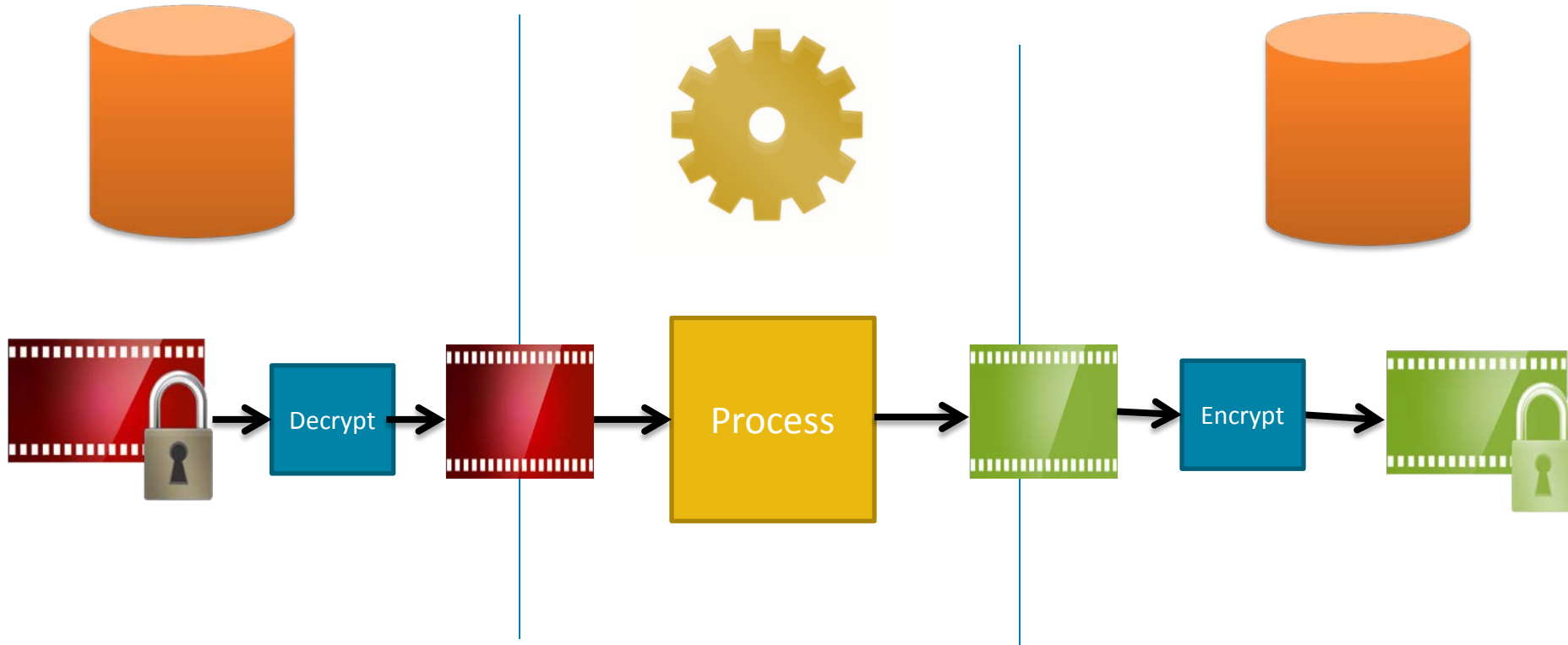
- Not optimal
- Law 1: attackers will always find their way



A long journey to ultimate encryption

2- Encryption at rest

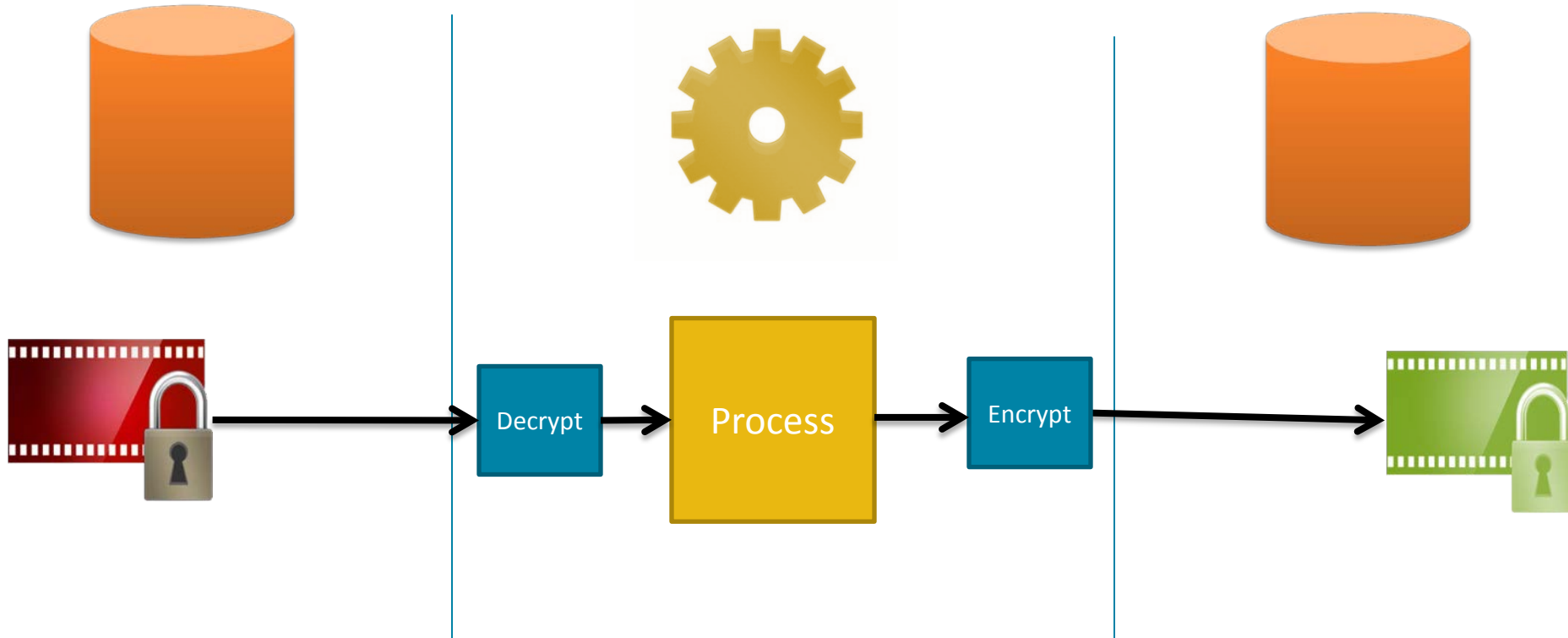
☐ Today



A long journey to ultimate encryption

3- Encryption-aware application

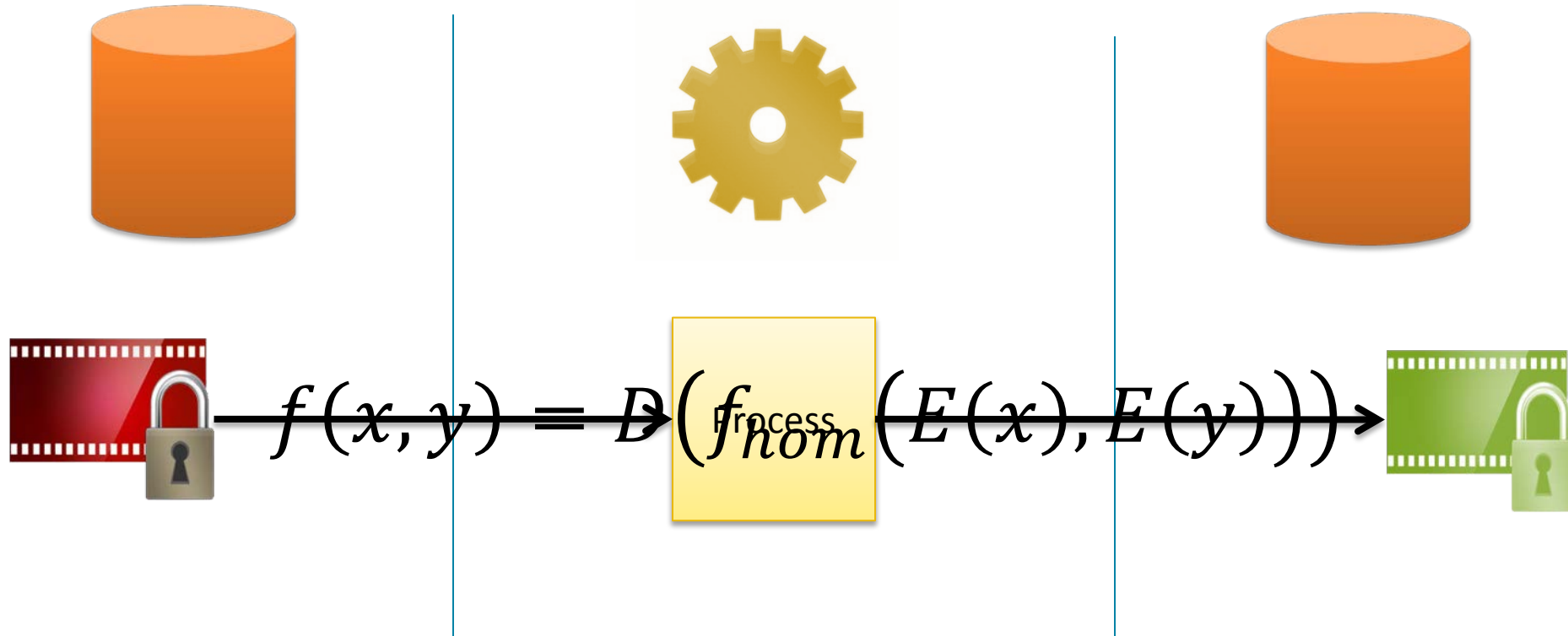
☐ Tomorrow



A long journey to ultimate encryption

4- Homomorphic encryption application

- The (far) future



Where are the problems?

Choice of encryption

- Easy: AES 128-bit
 - ❖ 256-bit is not useful

Key management

- Who can access the key?
- How is the key protected?

Promising trends in key management

- White-box cryptography
- Multi-party encryption

Law 3: No security by obscurity



Some myths

Encryption takes too long

- ❑ Wrong: modern symmetric cryptography is fast

OK, but my files are too large

- ❑ Wrong: Fast Software Encryption
 - ❖ Not AES
 - ❖ Stream ciphers designed for speed

Let's write our own implementation

- ❑ Bad idea: writing secure implementation of cryptography is an art



It is all about trust

Trust

Trust is confident reliance by one party on the behavior of other parties

Trusting what?

- Hardware
- Operating system and VM
- Administrators
- Access control
- Users



Can I trust the cloud?



Chadi Diehl ©

Your data center is
like your home

- How it can be accessed
- Who is inside

Can I trust the cloud?



Public cloud is like
an hotel

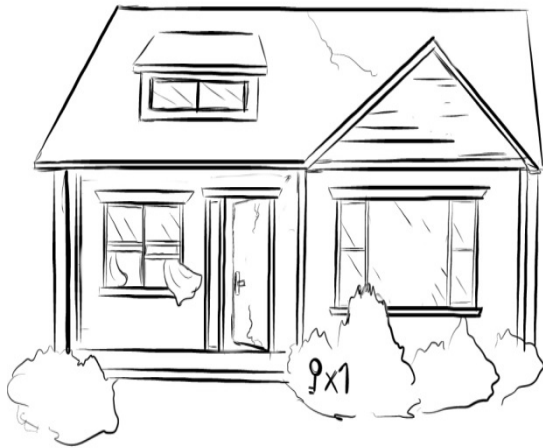
- Trust the concierge
- Lock your door
- Don't trust the
neighbor room

Can I trust the cloud?

All houses are not
equally secure



















© Chadi DIEHL



© Chadi Diehl

Trust in cloud deployments

	Data Center	Private cloud	Community Cloud	Public Cloud
Trust in Hardware				
Trust in OS/VM				
Trust in Admin				
Trust in Access				

Content at rest in the cloud

Encryption at server side and Key managed by cloud provider

- Easy to implement
- Strong trust in cloud provider

Encryption at server side and Key managed by content provider

- Trust only the quality of the implementation
- Responsibility of the key handling

Encryption at client side

- No security assumption on the cloud
- Content provider has to be knowledgeable

What choice?

- What is your level of paranoia?
- Are you fluent in cryptography and security?

You are the weakest link

Every access has to be authenticated

Law 7: You are the weakest link

Login/password is here for some time

- Weak passwords
- Reused passwords
- Reduced number of successive trials is not a solution
 - ❖ Rainbow tables

Help your employees

- Provide a password manager
 - ❖ Enforce a minimal length for the master password
 - ❖ Train and explain the benefits
 - ❖ It may even reduce operation IT cost



Every access has to be authenticated

Law 7: You are the weakest link

Administrators have the keys of the realm

All administrative tasks should request two-factor authentication

- SMS based
- U2F physical token
- Biometrics

Review regularly the administrative accounts and their access log

- And all other accounts



Every access has to be authenticated

Servers and processes are also “users”

- Mutual authentication
- White list

https, sftp, ssh

- Exclusively secure protocols
- Latest versions
 - ❖ SSL 3.0 is dead!!!

Role based

Conclusions

Conclusions

Encrypt, authenticate, and monitor

Adapt your solution to your skillset

We have a long journey to become highly secure

Cloud will require more scrutiny due to a larger attack surface

- Best practices
- Learning curve

Thank you for your attention
Any questions?

This document is for background informational purposes only. Some points may, for example, be simplified. No guarantees, implied or otherwise, are intended.